The *ASK LEO!* Guide to

STAYING SAFE ON THE INTERNET

FREE EDITION!



7th Edition

askleo.com

LEO A. NOTENBOOM

The Ask Leo! Guide to Staying Safe on the Internet

Free Version

7th Edition

by

Leo A. Notenboom

https://askleo.com

ISBN: 978-1-937018-72-6

Copyright © 2026

Table of Contents

Part 1: Protect Yourself 3

It Pays to Be Skeptical 4
Just What Is Common Sense? 8
Why I Rarely Panic 14
What Do I Do If I'm Being Harassed, Bullied, or Stalked Online? 16
Stop Spreading Manure 22
Why Ask Why? 26

Part 2. Protect Your Data 29

Why Is "Back Up First" My Recommendation for Everything? 30
How to Back Up Windows 33
Is Using the Cloud Safe? 37
Backups Are Great Security 42

Part 3: Protect Your Computer 45

Eight Steps to a Secure Router 46
What Security Software Do You Recommend? 53
How Do I Remove Malware from Windows? 57
How Do I Remove PUPs and Other Unexpected Things From My Computer 62
Will Using an On-Screen Keyboard Stop Keyloggers? 65
How Do I Make Sure Windows Is Really, Completely Up to Date? 68
I Got a Pop-Up Virus Warning. Is My Computer Infected? 72
How Do I Run a Full Scan Using Windows Defender? 75

Part 4: Protect Your Laptop 79

How Do I Use an Open Wi-Fi Hotspot Safely? 80
How to Protect Data on a Laptop 85

Part 5: Protect Your Online World 88

Please Set Up and Maintain Account Recovery Information 89
12 Steps to Keep from Getting Your Account Hacked 92
How Long Should a Password Be? 98
Why Is It So Important to Have Different Passwords on Different Accounts? 103
Why Password Managers are Safer than the Alternatives 106
My Email Is Hacked. How Do I Fix It? 109
Do I Need a New Email Address if Mine Is Involved in a Breach? 116
Two-Factor Authentication: It's Not as Complicated as You Think 118

Part 6: Protect Your Privacy 122

You're Just Not That Interesting (Except When You Are): Pragmatic Privacy 123
You Can't Un-Ring a Bell: What Really Happens to Your Data When You Post Anything Online 127
Are You Giving Away Your Privacy? 131
The Biggest Risk to Your Privacy 133

Part 7: AI 137

Why I Cringe When I Hear People Are Using ChatGPT to Look Things Up 138
Faking Reality: How AI Images Are Being Used to Scam You 142

Endnotes 145

The Ask Leo! Manifesto

I believe personal technology is essential to humanity's future.

It has amazing potential to empower individuals,
but it can also frustrate and intimidate.

I want to give you *confidence*.
I want to make technology work for you.

I want to replace that *frustration* and *intimidation*
with the *amazement* and *wonder* that I feel every day.

I want it to be a *resource* rather than a *roadblock*;
a *valuable tool,* instead of a source of *irritation*.

I want personal technology to empower you,
so you can be a part of that amazing future.

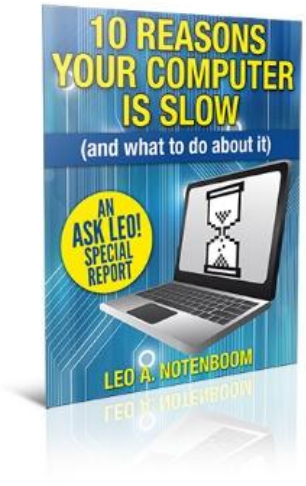
That's why *Ask Leo!* exists.



Leo A. Notenboom

https://askleo.com

First: A Freebie for You



Before we dive in, I have something more for you: my *Ask Leo!* special report, ***10 Reasons Your Computer is Slow (and what to do about it)***. This report will help you identify why your computer is slowing down, and the steps you can take to fix it.

It's yours free when you register *this* book.

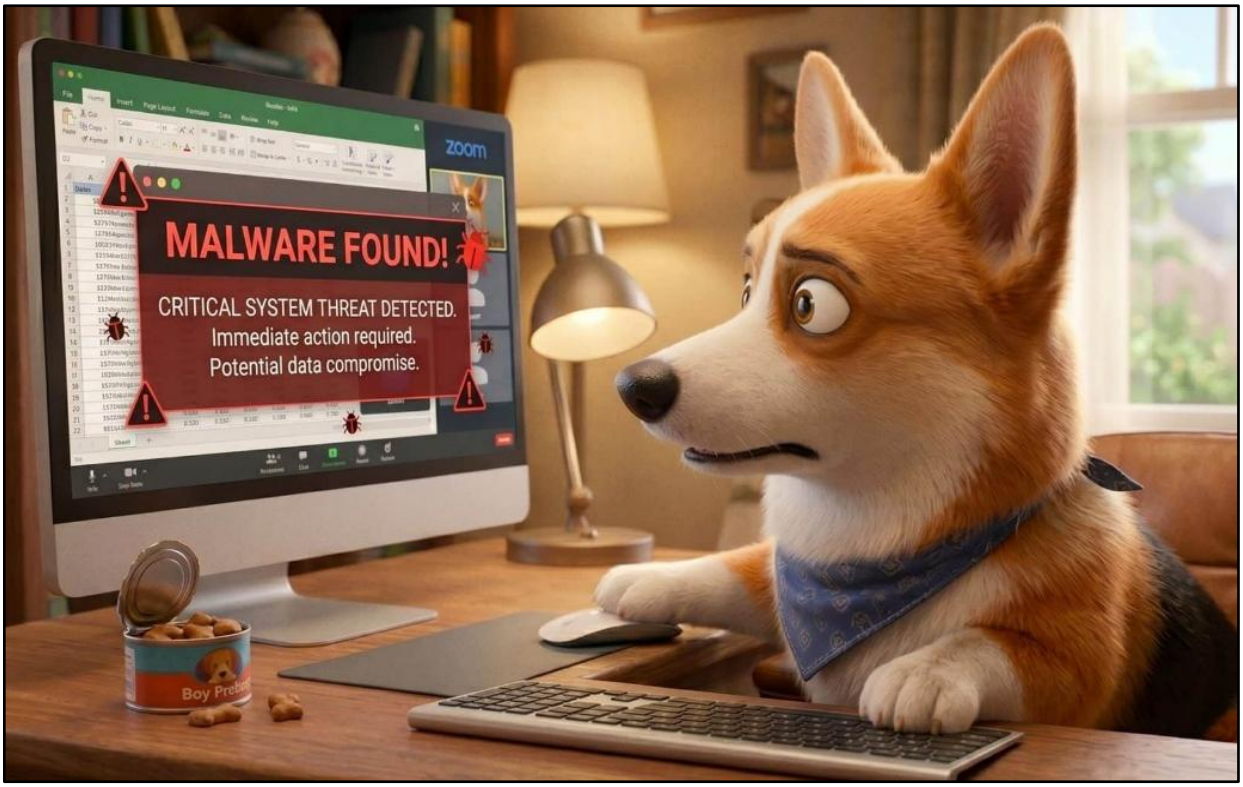
You'll receive several additional free bonuses.

- The FREE version of *The Ask Leo! Guide to Staying Safe on the Internet*. A shorter, more compact version of this book that you can share with your friends and family.
- All available digital formats of the book as direct downloads. Regardless of which version you have, you can enjoy this book on the digital device of your choice.
- Digital updates for life.
- Errata and prioritized Q&A.

You'll find the information you need to register in a chapter near the end of the book. Once you register, you'll be taken to a web page that lists all available bonuses.

Part 1: Protect Yourself

It Pays to Be Skeptical



A message pops up on your computer, warning you that malware has been detected.

What do you do?

The answer's not as clear as you might think.

In fact, no matter what you choose to do, it could be the wrong thing.

Your trust is a commodity

It's no secret that scammers actively prey on the trusting.

But it's not just scam artists who abuse our generally good nature and desire to trust. Hackers, malware authors, overly-aggressive salespeople — essentially anyone who wants something — re skilled at using your trust against your better interests.

Warning: malware detected, click to remove…

A pop-up message telling you there's malware on your machine[1] (and click here to fix it) is probably no big surprise to most people. With the constant barrage of news reports about hacks and

[1] https://askleo.com/3107

malware and the ongoing emphasis on anti-malware tools,[2] your first response on reading such a message may be to believe it.

"Malware? Well, it happens to so many people, it's no surprise that it happened to me!"

Except it might not have.

That message might be completely fake. It may be inciting you to trust it and click to take further action. And that click and "further action" could install malware, or worse.

Or it could be legitimate.

What do you do?

Unable to deliver package, details attached…

You've probably received an important-looking email telling you there's a package on its way and the details are in an attached file.[3]

Perhaps your online email provider has detected a problem with your account, and you need to check something by clicking on the conveniently provided link.[4]

I've even received email from "PayPal" indicating that access to my account had been "limited" because of suspicious activity. I needed to log in to provide additional information — once again, using the provided link.[5]

In each case, the sender wants you to trust them, and take whatever action they've recommended in their message, be it examining the contents of an attached file, clicking a provided link to their website, or even replying to the email with sensitive information.

Abusing your trust in this manner is currently one of the most effective ways to distribute malware or hack your online accounts.

And yet, each one of those scenarios could be legitimate at times.

What do you do?

I'm from Microsoft, and we've detected….

You're working on your computer one afternoon and get a phone call from someone who says they work for Microsoft. They've detected that your computer is causing many errors on the internet. They offer to walk you through some steps to show this to you, and indeed, there *do* seem to be lots of unexplained errors right there on your computer.

---

[2] https://askleo.com/3517
[3] https://askleo.com/18718
[4] https://askleo.com/132182
[5] I've actually received this scenario legitimately, which really surprised me. Of course, most are scams of some sort.

Then they offer to fix it for you[6] if you just go to a site and type in a few numbers they recite to you.

Those errors are pretty scary-looking, and you certainly don't understand them.

What do you do?

What you do: get skeptical

Skeptic: a person who has or shows doubt about something. – Merriam Webster[7]

If there were one skill I could magically impart to my *Ask Leo!* readers — hell, on the entire technology-using, internet-loving universe — it would be the skill of healthy skepticism.

I don't mean that you believe nothing and trust no one. I mean that you believe, you question, and before you trust, you learn.

Truly, being skeptical is really the only solution to the scenarios I've outlined above.

In each case, it's *critical* that you don't blindly trust the information presented to you. Question whether or not the person or company at the other end of the message has your best interests in mind. Is the story they're telling accurate? Verifiably accurate? Do you know beyond doubt that they are who they say they are?

If the answer to any of those questions is "no", or even "I'm not sure", *stop*. Stop and take additional steps make sense to confirm that what you're being told is legitimate.

It might mean some internet research, calling them back, or asking a trusted friend or resource for their opinion.

> "Skeptic: a person who has or shows doubt about something.
> -Merriam Webster

But if you aren't sure, question everything.

Be more skeptical: it's one skill that can help prevent disasters before they happen, and keep you and your technology safe.

Nullius in verba: "Take nobody's word for it."[8]

It's more than just technology

Naturally, my plea for being skeptical and that you "question everything" is about far more than just the technology you have sitting in front of you.

As I've written before,[9] an amazing amount of information we're shown each day is completely bogus — or at least nuanced and presented in such a way as to cause you to believe that things are other than they truly are.

---

[6] https://askleo.com/4164
[7] https://www.merriam-webster.com/dictionary/skeptic
[8] Nullius in verba, besides being the motto of The President, Council, and Fellows of the Royal Society of London for Improving Natural Knowledge, is a very fancy way of saying "question everything". ☺
[9] https://askleo.com/11287

Our natural tendency to believe that which supports what we already believe (known as the "echo chamber" or "confirmation bias"), makes it easy to be misled and misinformed.

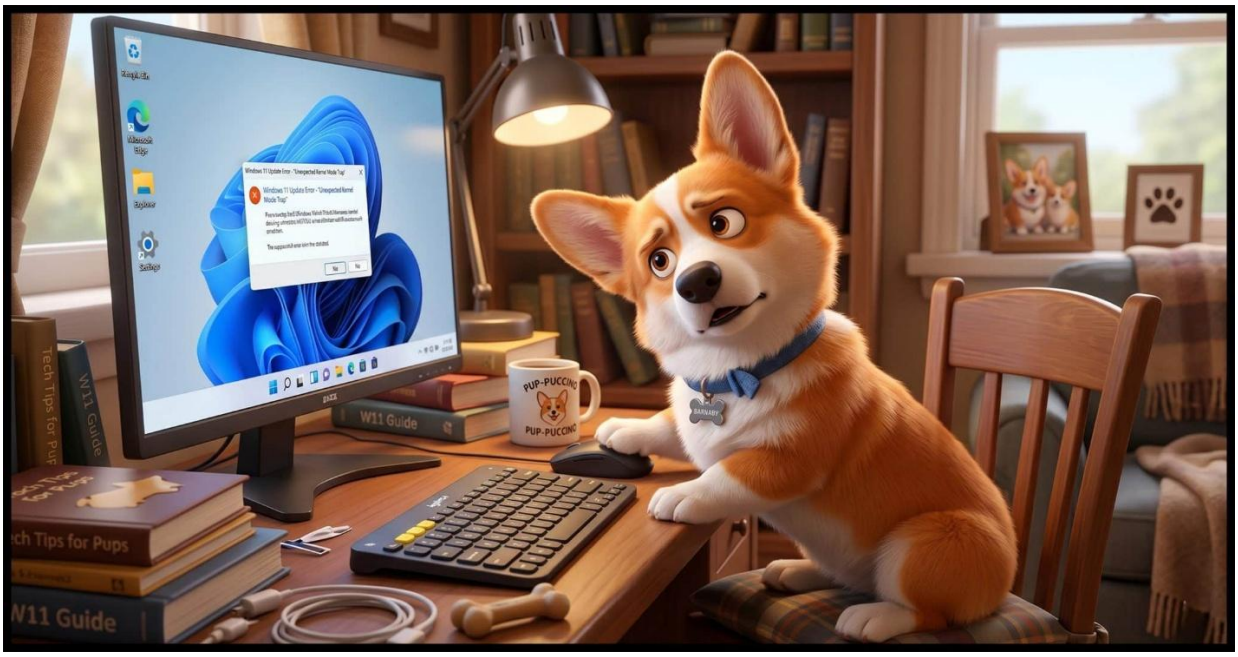
The solution remains the same:

Be skeptical.

Question everything…

…even things you already believe are true.

Just What Is Common Sense?



When it comes to internet safety, one of the most oft-cited pieces of advice computer professionals hand out is:

Use common sense.

One of the common responses is:

"Great. What does that mean?"

When it comes to technology and safety, "common sense" is important, poorly defined, and quite *un*common.

Let's see if we can define it with some familiar rules.

Common sense can be summed up in several familiar adages.

- If it sounds too good to be true, it's probably not true.
- If it ain't broke, don't fix it.
- Free is never free.
- Read what's in front of you.
- Don't believe everything you read.
- Be skeptical: question everything.
- Do your research.

If it sounds too good to be true…

Many of the security snares we fall for mask themselves by seeming irresistible.

Practical examples of offers that really are too good to be true include:

- Many "free download" advertisements
- Software that promises to speed up your computer
- Ads that include the phrase "one stupid trick to…" or variants thereof
- Click-bait headlines that include the phrase "you won't believe" or "will blow your mind" or similar

Common to most of these items, beyond the fact that the promises they make seem extreme, is that *you weren't looking for them when you found them*.

Look at any website, and you'll see advertisements. Many are legit and well-positioned, but others are little more than over-the-top attempts to get you to click or download whatever they have to offer.

Particularly when you're not looking for something, don't fall for extreme or outlandish claims. The same can be said of most shared or forwarded hoaxes and urban legends, as well as many news stories.

Common sense tells us that if it promises too much, if it sounds extreme, or if it seems astonishing, it's probably false.

If it ain't broke, don't fix it

Whether following over-inflated promises such as those I just mentioned, or out of desperation, people often do things to their computers that have nothing to do with a problem they're experiencing.

- They try to solve speed problems they don't have.
- They try to remove malware that isn't present.
- They try to update software they don't use.
- They try to fix problems that have nothing to do with their computer.

The list goes on.

I understand that each of those assumes a certain amount of knowledge. How do you know you don't have a specific problem? How do you know malware isn't present? How do you know that the problem is with the website you're visiting and has nothing to do with your computer?

That's a fair concern. But if you don't know you have a problem, why are you trying to fix it?

So turn the thinking around.

Common sense means not doing something because you *might* have a problem, but taking action because you know you have a problem, not before.

Research the problem first. Confirm you have a problem that needs fixing before you try to fix it.

(I'll talk about research shortly.)

Free is never free

The economist's old acronym is TANSTAAFL: "There ain't no such thing as a free lunch." That's exceptionally true on the internet.

Every "free" service has a cost. It may be the advertising you see, the mailing list you have to sign up for, the personal information you're sharing, or something else entirely, but there is no such thing as "free" on the internet.

People often fall into the "free" trap through advertisements of this variety: "FREE scan! Scan your computer for malware for FREE!"

Well, the *scan* is completely free. The not-so-free part? If you want to do anything about what the scan finds, you'll need to pay. It's a common sales tactic.

Less reputable programs lie to you. They warn you of malware and other scary things you don't have or that aren't issues, making it appear that giving them your money is the only way to avoid certain doom.

Which brings us to another important point.

Read what's in front of you

This frustrates me. It works like this:

- A program fails or something goes wrong.
- The user gets frustrated or confused.
- The user completely misses the fact that *the solution to the issue was included* in the error message or descriptive text.

A similar scenario:

- Someone gets an email. The first line is so outrageous that their reactions kick in right there, and they stop reading.
- As a result, they miss the text after that, which puts the statement in a clearer context, provides additional information, and eases all the outrageousness.

When something goes wrong with your computer, *take the time to read what's on the screen in front of you*. I get so many questions that could be easily dealt with had the questioner just slowed down and read the instructions in front of them.

I understand that those instructions are not always easy to understand. Honestly, I do. But sometimes they are clear enough that just taking the time to slow down and carefully read what's on your screen will help.

Which brings us to the other side of the coin.

Don't believe everything you read

I'm a firm believer that people are basically good.[10]

But that doesn't mean that everyone has your best interests in mind, particularly when it comes to the internet.

It's too easy, particularly in today's connected and information-rich world, to spread misinformation as fact. We see it all the time.

Misleading ads are only one example. Misleading ads pre-date the internet by hundreds of years. It's just that today's technology can make it difficult to distinguish snake oil from valuable and effective medication unless we're careful.

The internet can teach us how to separate overinflated claims from reality.

It can also provide us with even more misinformation.

"It's on the internet, so it must be true" is one of those statements that everyone laughs at because it's so blatantly wrong, it's laughable. Common sense tells us that because something is on the internet has no bearing on its accuracy. Yet people believe random and misleading statements from vague sources with less-than-altruistic agendas.

With information coming at you from so many random directions from both trustworthy and unreliable sources, it's critical we do not believe everything we read just because it's been formatted attractively[11] on a site that looks authoritative.

And that brings us to the most important point of all.

Above all, be skeptical

Want something that's very common sensical?

Question everything. Even me.

Never accept information at face value, particularly on the internet, and particularly from sites or individuals you've never heard of before.

Be skeptical. Ask questions. Consider the source and what that source's agenda[12] might be in spreading its message.

---

[10] That's one reason I took on heroicstories.org and run notallnewsisbad.com.

[11] Also not new. I'm fairly certain that my good grade on a paper I turned in while in college was due to the fact that I'd figured out how to use a word processor to make it look much better than it actually was.

[12] And don't kid yourself, every source has an agenda. More here: Stop spreading manure.

Over time, develop a set of resources that you trust. Naturally, I hope *Ask Leo!* will be one of them, but honestly, what matters more is that you find sites, sources, services, and individuals that you trust.

Then use those resources to help you evaluate the constant stream of information and misinformation that's heading your way.

Yes, it's a little bit of work. But it's critical.

Do your research!

Search for yourself. Learn the basics[13] of how to use a good search engine (Google, others, and AI), and how to interpret the results. **Understand the difference** between advertisements presented on the search results page and the actual results.

Look for well-known, reputable sites you recognize in those results, not just sites that happen to rank highly. Ranking highly in a search result is not an indication that the site is legitimate or trustworthy.

If you choose to look at information presented by a site you've never heard of before, remember, you've never heard of it before! Without more research, there's no way to know whether the information presented is valid, biased, or completely bogus.

Get help. If you're uncertain how to research a particular topic, there's nothing wrong in asking for help. You may have more experienced friends or family members who can help you find what you're looking for. Librarians are also valuable resources when trying to determine the validity of information you run across online.

Regardless of who's helping you, it's still important to be skeptical. When they suggest a site as a trustworthy resource, don't be afraid to ask them why they trust it.

***Look carefully for confirmation*.** There are two types of confirmation:

- Source B repeats what source A has said.
- Source B independently presents the similar information or conclusion that source A did.

The first isn't confirmation at all, it's repetition. The problem is, when enough sites and so-called sources all repeat what only one of them has said, it may feel like many sources have all come to the same conclusion. In reality, it's nothing more than a single opinion repeated over and over. This is known as the *echo chamber*.

Remember: *repetition isn't confirmation*. You want multiple sources to confirm (or deny) the issue, having arrived at their conclusions independently, using their own research.

[13] https://askleo.com/two-steps-better-search-results/

Use debunking sites. I'm a huge believer in using sites like snopes.com,[14] factcheck.org,[15], mediabiasfactcheck.com,[16] politifact.com,[17] truthorfiction.com,[18] or any of several others[19] before reacting to the latest over-the-top, can't-possibly-be-true news story, tech tip, or emailed rumor.

Many are timely and do the kind of research you want to see before getting all excited or worked up about what just landed in your inbox.

Use resource sites. There are resource sites for just about any topic. Develop a set of sites that you trust. For example, when it comes to technology, I would hope Ask Leo! is on your list. Visit the sites for which you already have a level of trust and see what they say about the issue at hand. As always, I'm not saying you need to trust them completely, but use them as part of your research to develop your own well-thought-out opinions.

The bottom line is this: if something you run across is worth the effort to take any action at all — even if it's just to forward an email — it's worth researching first. At worst, it may save you some embarrassment. At best, it could protect your computer, your identity, and even your possessions.

---

[14] No, Snopes isn't left-wing biased. Generally people claiming so are simply unhappy with the truth Snopes has uncovered. Nonetheless, if you're not happy with Snopes, look at any of the multiple debunking sites that are available these days.

[15] https://factcheck.org

[16] https://mediabiasfactcheck.com

[17] https://politifact.com

[18] https://truthorfiction.com

[19] https://www.makeuseof.com/tag/true-5-factchecking-websites/

Why I Rarely Panic



As I watched a "major" security issue unfold a few years ago, I read the media reports seeming to claim that the end of the world (or at least the internet) was upon us. I felt like I was supposed to be panicking.

I didn't, and neither the world nor the internet ended.

It's not in my nature to panic. That's just the kinda guy that I am. Panic may occasionally be called for, but usually it does more harm than good.

Yes, it was serious, but…

Don't get me wrong; the issue was serious. The potential for havoc was high. In fact, I'll even say we dodged a bullet.

But dodge it we did.

For this particular issue, server administrators had reason to be deeply concerned. Their systems were vulnerable, and the moment the news broke, their systems needed to be fixed ASAP.

As the owner of an affected server at the time, I did due diligence to ensure the servers under my control were not affected. Rather than panic, I felt more of a "better look at this right away" kind of prioritization.

The general public had even fewer options. Aside from caution when moving forward after the bug had been publicized, there was *absolutely nothing* the average consumer could do. If there was damage, it had likely already been done.

More importantly, it appears that there wasn't a lot of damage done. Servers were fixed quickly, and life moved on.

Panic and sensationalism feed the press

I use the term "press" very loosely here. At the time, you could find proclamations on the issue everywhere from individual blogs to major news media outlets.

And it all comes back to clicks.

When a story sounds sensational, more people click through to read it. That page then offers more eyeballs to the advertisers that sponsor it. As a result, there's a powerful incentive to make headlines as shocking as possible, sometimes to the extreme.

It's called "clickbait," and nothing generates clicks like feigned end-of-the-world panic.

The result is that we need to view news reporting on just about any story very skeptically. There are great, trustworthy sources out there.[20] It's just difficult to pick them out from all the noise.

Panic and sensationalism lead to bad decisions

In technology, particularly around personal computing and the internet, two themes appear consistently:

Panic leads to a sense of extreme urgency.

Extreme urgency leads to bad decisions.

I have seen people make some terrible decisions — like unnecessarily reformatting or even discarding computers, closing online accounts, and even stepping away from online activities completely — in a panicked and often ineffective response to a seemingly imminent threat.

Imminent and dangerous threats do arise — but I have yet to see one that is so serious that you can't take some time to calmly and rationally consider the ramifications.

My advice?

Be aware, but be skeptical.

Realize that many "news" and other information-delivery vehicles have an incentive to make things seem worse than they are, or to overstate the risk in one area based on the genuine risk in another.

It's unfortunate, because the press has cried wolf so many times that we're more likely to pass over a truly attention-worthy story when one comes up.

When you see a story that seems serious, and you wonder how it affects you, pause. Take a breath. Wait until the dust settles, or check in with your less panic-stricken and knowledgeable friends.

You may need to take action, but as with anything, you need to take the right action.

And reactions made out of panic are rarely right.

[20] https://askleo.com/24333

What Do I Do If I'm Being Harassed, Bullied, or Stalked Online?



Cyber-bullying, or online harassment, is a frighteningly common occurrence. Those most at risk appear to be children and people who have been in abusive relationships, but it can happen to anyone.

The questions I get most often are:

- Isn't it illegal?
- How do I find out who's responsible?
- How do I make them stop?
- How can I get back at them?

Let's tackle each of those and a couple more.

Isn't it illegal?

I need to remind you that I am neither a lawyer nor a law enforcement professional. I cannot give legal advice, and none of this should be taken as such. If you need legal advice, seek out an attorney or reach out to one of the many organizations set up to help victims of domestic violence in your area.

One problem with this question is that the answer varies — sometimes dramatically — from location to location. Some activities are illegal in some jurisdictions and acceptable in others. The only way to know which laws apply to your situation is to contact an attorney or your local law enforcement. (You'll find this to be a common refrain throughout this article.)

There are, however, a couple of generalizations or examples that might be instructive.

Sexual exploitation of children is pretty clear. While the definition of "exploitation" may be unclear in some cases, and the legal definition of "child" may vary, authorities are typically clear on its illegality.

At the other end of the spectrum, simple password theft might not be illegal. Accessing your account and reading your email without your permission might be legal. Most would consider it wrong, rude, offensive, and perhaps immoral, but depending on your local laws, it might not be an illegal offense.

What they do once they have your password may or may not be illegal. For example, hacking into your account to threaten people in your address book might be illegal, but simply annoying people in your address book may not be.

It's a large grey area. Unless things are obviously illegal, like sexual predation, you may not be able to assume what is or is not a violation of your local laws. You'll need to ask a local authority.

How do I find out who's responsible?

You don't.

This is perhaps the most common harassment-related question I get. People who are being harassed or threatened anonymously want to find out who's doing it.

The most common specific question I get relates to IP addresses.[21] People believe that once they have an IP address, they can identify the individual.[22]

No. It's nowhere near that simple.

Working on your own, your best bet is to look for all the clues relating to *the situation*. Sure, perhaps an IP address matches an IP address in an email you got from someone you know. *That's no guarantee it's the same person*, but it's a clue. So are things like who might have a problem with you in the real world, who's been causing you grief at work or in school, or who you just broke up with.

None of that can prove anything, but it can build a case you can take to the proper authorities.

You *cannot* definitively trace the source of an email (or any other internet connection) unless the offender slipped up and made it obvious in non-technical ways. But if a law has been broken, law enforcement may be able to. Some time ago, I spoke to Detective Malinda Wilson of the Seattle Police Department and the Internet Crimes Against Children task force,[23] who indicated that she had served as many as nine different warrants to follow the trail of one of her suspects.

This brings us to another point: police may not always be able to help. Detective Wilson's case likely involved a crime against a child, as that's her specialty. That's a priority, and certainly justifies the time and effort to locate the criminal and prosecute the crime.

---

[21] https://askleo.com/2132
[22] https://askleo.com/2293
[23] https://www.icactaskforce.org/

Someone hacking into your email account? That's just not as important. To quote Detective Wilson, "Often, if no crime other than the 'hacking' is done, the best advice is going to be to start over with a new account."

The abilities and resources available to your local law enforcement dictate what's possible and what's reasonable to expect when it comes to tracking down your offender.

How do I make them stop?

If you believe a crime may have been committed, contact your local law enforcement.

If the offender is in school/at work and using school/work resources, the school or workplace may have additional options. Certain forms of harassment may not be illegal, but may still be against school rules and regulations. The organization may be able to take action on your behalf and likely have a better picture of what warrants involving law enforcement.

In lieu of support from law enforcement or other authorities, your options are limited. Some ideas include:

- If you're receiving harassing email at a particular email address, close that account and open a new one.
- If your email account has been stolen and you no longer have access to it, create a new account and let your contacts know to ignore the old one.
- If you're getting harassing chat messages, close the account and begin a new one.

Yes, all of these are the cyber-equivalent of changing your phone number to an unlisted one, or even moving to avoid harassment. As in real-world examples, make sure only people you trust have your new information.

And yes: to put it bluntly, it sucks.

But the fact is, unless some law has been broken, it's not illegal to be an annoying pain in the… neck. And even if a law has been broken, the authorities may not have the resources to assist sufficiently.

How can I get back at them?

You don't.

This, too, is a common question. People feel they have been violated, and they want to get revenge.

Consider this fact: How Do I Hack into Someone's Account?[24] is a popular Ask Leo! article. My theory is that it's mostly children attempting to figure out how to get revenge on someone who has bullied or harassed them, online or off. Many of the comments on that article, including most of the comments you don't see because they are themselves abusive and have been removed, would seem to bear this out.

[24] https://askleo.com/2590

Bypassing the authorities and attempting to exact revenge can only do more harm than good and rarely resolves anything.

At best, you'll only waste time. More likely, you'll antagonize your target into taking harsher actions against you. In the worst case, you might find yourself in violation of the law and, as a result, face harsher penalties than the person harassing you.

Don't do it. Don't even try. It's just not worth it.

Involve the authorities — law enforcement, school officials, ISPs — if you can, and let them do their jobs. If they can't help, then it's by far safest to let it go if at all possible.

How do I prevent all this in the first place?

Frequently, this is asked in the context of parents wanting to keep their children safe, but most of the rules apply to us all.

- **Be the parent**. This is by far the toughest, but it means understanding what's appropriate for your children and being aware of — perhaps even monitoring — what they're doing online. It means setting rules with consequences, sticking to them, and taking care to make sure your children understand what it means to be safe on the internet.
- **Be realistic**. Children are more likely to be affected by what I'd call "peer-to-peer bullying" than they are to be approached by an adult for illicit purposes. That does not mean that sexual predation does not happen; it clearly does. But what's much more likely is that your child will be bullied by another child. Don't ignore the latter because the former is so much more heinous and gets more press.
- **Choose strong passwords**. Yes, strong passwords are hard to remember, but that's what makes them strong. The easier they are to remember, the easier they are to guess. Most individual account theft is simply someone guessing your password, with no special technology or techniques necessary.
- **Don't share your password with anyone**. The one exception is that children should be required to share their passwords with their responsible parent(s). The scenario I see repeated over and over, with both children and adults, is this: someone shares an account password with a trusted friend, and sometime later the friendship ends. It's not infrequent that the former friend does serious damage before the account misuse is detected.
- **Don't publish personal information publicly**. Google yourself: you may be amazed at what you find. Don't publish information publicly in newsgroups, public forums, social media, and other places where anyone can see. Even the smallest bit of personal information here and there can be used by a savvy stalker. Assume your worst enemy is trying to find you and every little piece of information you leave online is helping them.
- **Don't assume you know someone you've never actually met**. On the internet, it's easy to appear to be something or someone you're not. Only once you've actually met them, or perhaps when someone else you know (i.e., someone you've met) has met them face to face, can you assume you know who you're talking to.
- **Learn the technology**. You don't have to know how a car's engine works to drive safely, but you do have to know how to drive and the rules of the road. The same is true for the

internet. Take the time to learn about your computer, the internet, and the sites and services you use most often. The better educated you are about these things, the safer you'll be.

Where can I get help?

I attended a presentation on internet safety for children, which is where I met Detective Wilson. The presentation covered some of what I've mentioned here and a lot more. If you have the opportunity to attend something similar in your area, I strongly recommend it as a starting point.

Remember, the rules and cautions apply to everyone, not just children. Adults can learn a lot about the potential risks and the steps to stay safe, even by attending a presentation aimed at keeping kids safe. If nothing else, it's a good place to ask questions, and you'll get references to the local agencies and support organizations that can help you learn more or deal with any immediate issues.

Additional resources include:

- Local law enforcement — your first place to turn if you believe a crime has been committed.
- Use the CyberTipLine[25] on the web (or at 800-843-5678 in the US) to report or learn more about preventing sexual exploitation of children. (Also includes a link to U.K.-based resources.)
- Your local ISP. I know this can be spotty depending on the service you use or the scenario involved, but your ISP can be a source not only for action but for guidance on where to go next.
- Online Resources like NetSmartz.org[26] from the National Center for Missing and Exploited Children.

On paranoia

After doing this for over two decades, I've heard from all kinds of people in all kinds of situations. The most common are those with real concerns and tangible issues confirming their situation. I also hear from what, for lack of a better term, I can only call the paranoid. It would be easy to write off perceived paranoia as being overly concerned about nothing, but that's rarely, if ever, the case. Regardless of the specifics, the concerns are, to them, very real and very frightening.

Unfortunately, almost any unexpected behavior — on a computer, mobile device, online accounts, and more — is often taken as proof that something sinister is afoot. The reality is that unexpected behavior almost always has a more mundane, less threatening explanation.

Almost always.

And that's where it gets complicated. There's always a chance that the issues are real and the concern is warranted.

[25] https://www.missingkids.org/gethelpnow/cybertipline
[26] https://www.missingkids.org/NetSmartz/home

I cannot help in these situations. My advice is always to start with trusted local help. That can be technical assistance from local resources, relying on trustworthy family or friends, or even local support organizations for the type of harassment you might be experiencing. This is almost always a case where in-person assistance is required to get to the root of any issues and perhaps engage appropriate local authorities or other sources of help as warranted.

Stay safe

The internet is a wonderful, wonderful place. I truly believe it is. It's opened doors and made so much information and opportunity available to individuals planet-wide that I can't imagine a world without it.

But it also opens up doors of opportunity for the darker elements in society. Like any tool, it becomes our responsibility to use it wisely, protecting our loved ones and ourselves.

The key is simple: education. Learn about the tools, about the opportunities available, and about your computer, its software, and its abilities.

Then pass what you've learned on to others.

Stop Spreading Manure



Supposedly, in a report a few years ago, Google blatantly admitted that you should have no expectation of privacy whatsoever when using their services. The internet went crazy. Many sources seemed to say, "How outrageous! We told you so! Google is evil!" Mainstream news outlets picked up stories from smaller publishers, and they all seemed to confirm the entire sordid mess.

Except the internet was wrong. Manure, to use a polite term, was being spread far, wide, and fast.

Everyone has an agenda

In the popular television series *House,*[27] Dr. Gregory House often says, "Everyone lies."

On the internet, a similar statement can be made: everyone has an agenda.

Every website, news organization, and person sending an email, publishing a newsletter, or posting a comment has an agenda of some sort. They have something they want you to do, think, or become.[28]

All too often, the agenda being promoted is inconsistent (for lack of a better word) with reality.

An agenda almost always colors the information presented. People highlight facts supporting a particular agenda, conveniently minimizing or ignoring facts that don't. In the worst case, people fabricate facts to support their agenda.

Yes: not everyone, but some people, lie. Perhaps more often than you think.

To be honest, we all do it. We color what we say and do with data to support what we believe, often to the exclusion of all evidence pointing out the unthinkable: that we might be wrong.

If it's on the internet, it must be...

There's an interesting and somewhat strange conflict in our culture these days.

Most people realize that "If it's on the internet, it must be true" is a sarcastic falsism that expresses just how inaccurate information on the internet can be. Just because it's published on a website somewhere (or shows up in your inbox, on Facebook, or wherever), doesn't make it true.

---

[27] http://www.imdb.com/title/tt0412142/

[28] *My* agenda is simple: I want you to be more skeptical before you believe what you see on the internet, and I want you to stop spreading misinformation. I'd love for this article to go viral and garner more Ask Leo! newsletter subscribers and site visitors, as well as improving my site's reputation with Google. I have a large agenda. Don't think for a moment that other sites, services, and individuals don't have agendas that are as large or larger.

However, I think most people *do* believe most of what they read on the internet. The same people smiling knowingly at that falsism go on to believe the strangest, most bizarre, completely false things as long as the information is presented in a seemingly credible way.

They do it without thinking and without seeing the irony in their behavior.

From what I've seen, this is getting worse.

We believe what we want to believe

A couple of terms explain why this might be.

Confirmation bias is the natural tendency we all have to believe what confirms what we already believe and dismiss what doesn't. The consequences of confirmation bias can be as simple as dismissing alternative viewpoints out of hand and as horrific as being tried and arrested for expressing beliefs that are not commonly accepted (think Galileo[29]).

The problem with confirmation bias, as Galileo so clearly illustrates, is that it often stands in the way of the truth.

Put another way, we believe what we want to believe. We believe what matches our own world view and our own agenda *whether we are right or not*.

The *echo chamber* is the tendency of information sources — most notably news media — to repeat each other. In a sense, they use each other as sources. The problem is that a story originating from a single source — true or false — can appear to have massive objective confirmation when we start hearing that same story from a variety of supposedly independent sources.

Those sources aren't independent at all; they're just repeating what they heard from each other.

And it all started from a single source ...

... a source with an agenda.

Fifty shades of gray

Things get more complicated still.

We desperately want things to be simple. We want things to be true or false, black or white, right or wrong.

Good or evil.

It's much easier to comprehend "true" and "false" than it is to deal with the potential uncertainty of "mostly true", "kind of wrong", or something in between. Unlike whether the sun circles the earth

[29] https://go.askleo.com/galileo

or the other way around, the issues that we consider, discuss, and even rant about rarely have easy, yes/no, black or white answers.

The folks who write headlines and push agendas know that thinking is hard for many of us. They know that black and white is easier, and (bonus!) much more sensational. So they pick and choose the "facts" that support black-and-white thinking at the exclusion of the significantly more nuanced truth.

About that Google privacy thing

So is your Google email account private or not?

It's not that simple. It's still not a yes-or-no answer.

And yet, in our example above:

- Organizations believed to have an anti-Google bias[30]
    - Drew a sensational black-or-white conclusion[31]
        - Based on a quote taken without complete and proper context[32]
            - Which was then bounced around the echo chamber on this site[33] and dozens of others.[34]

Even though some sites posted clarifications and/or updates, they're often did so too late (the misinformation had spread) or too little (the clarifications remained biased to the pre-existing story or overall agenda).

Email privacy, and privacy on the internet in general, is a critically important and complex concept. Services like Gmail *do* process your email to do things like filter spam or populate indexes so you can search your email quickly. Are there teams of people sitting behind computer monitors reading your email? Almost certainly not.

However, unless you encrypt your email, it is by definition fundamentally not secure. *This is nothing new* or specific to Google.

And yet, in the pursuit of clicks, page views, and furthering anti-Google sentiment, some sources pick and choose what to present and then sensationalize how they present it.

You. Must. Think.

So what's the solution?

---

[30] http://www.pcworld.com/article/204842/consumer_watchdog_fighting_google.html
[31] http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care
[32] https://thenextweb.com/news/no-google-did-not-say-that-we-cant-expect-privacy-in-gmail
[33] http://www.huffingtonpost.com/2013/08/13/gmail-privacy_n_3751971.html
[34] These three were selected at random from an (irony alert) Google News search on "Google Privacy".

You. You are the solution. You and I and everyone we know must — and I really do mean *must* — become more skeptical and demanding of our news and information sources.

You and I must *think* about what we read. We need to learn to identify the sources and the agendas those sources have that color what they present and how they present it.

We need to learn to draw our own conclusions. Whenever you accept misleading or inaccurate stories as truth, *you've been manipulated* to serve someone else's agenda. And when you pass those manipulative stories on to friends, family, and acquaintances? Well, my friend, you've just turned into a virtual manure spreader. Because manure is what it is.

Be skeptical.[35]

If something sounds outrageous — *even if it supports your beliefs* — there's a hefty chance *it's completely bogus*. Overly sensational or outrageous-sounding headlines or content are a hallmark of bogus stories.

Do a little research. Check and verify the sources; follow the trail. If they all point back to a single source (or no source at all), realize what you're looking at. One source repeated a thousand times in a thousand places doesn't make it a thousand sources.

In the past, we could count on the media to do fact- and source-checking for us, but that's clearly no longer true. In the race for media outlets to publish quickly, the effort to make sure it's accurate has apparently been left behind.[36]

Collateral damage: legitimate news and important issues

One of the truly sad casualties of all the misinformation on the internet is how difficult it has become to find the truth, and how difficult it is for accurate, important news and information to get the attention it deserves.

It's all lost in the noise: covered in manure.

The non-profit world has a term: *donor fatigue*. This applies to potential contributors who, while supportive of a cause or organization, get tired of being asked for money, time, or whatever else.

The same is true here.

Call it *manure fatigue*. It is tempting to disregard anything found on the internet as likely to be bogus. Unfortunately, there are legitimate outrages, atrocities, and issues of privacy[37] that really do deserve our attention, understanding, and even action.

It just takes some skepticism and some thought to separate the wheat from the fertilizer.

---

[35] https://askleo.com/21535

[36] Not to mention that many formerly outstanding news outlets are now either explicitly or implicitly adopting politicized agendas to curry favor with various government officials.

[37] https://askleo.com/21593

Why Ask Why?



When I was helping a friend the other day with some Windows issues, a not-uncommon question came up, one that I often dread.

"Why?" As in, "Why did they do that?"

It's a common question that gets applied to computers and software of all generations and iterations. Recent versions of Windows have certainly generated a healthy share of "Why?" questions, but trust me, it's nothing new.

The problem is, asking "Why?" is most often an exercise in futility.

Don't ask out of frustration

Faced with something they don't understand, can't comprehend, or don't like, many people ask "Why?" out of frustration.

Why were decisions made the way they were? What were they thinking? The questions may be mostly a way to emphasize just how much the questioner disagrees with those decisions. They're not really looking for an answer.

That's a good thing, because most of the time, there is no answer. Expecting one — in particular, one that would allow you to make peace with whatever issue you're facing and thus be OK with it — is just going to frustrate you when no answer is available.

Searching for a *why* out of frustration is energy wasted.

To get all Zen for a moment, it is what it is.

Getting frustrated, demanding to know why, or even understanding why isn't going to change any of that. You don't have to like it, but it's probably best to accept whatever it is and make decisions accordingly.

When the why isn't the real why

One of the most frustrating answers to "Why?" is what I refer to as marketing-speak. You could even call it misleading or misdirecting marketing-speak.

This happens when the source of our frustration believes we can't handle the truth, or doesn't want to share the truth, and gives us some corporate line about why a specific change was made.

A company might say they made a change because testing revealed it was better, stronger, faster, or whatever, when in reality, the change was made to further some agenda. That agenda might be about:

- Selling more product (not something the company wants to admit publicly).
- Unifying some underlying technology (rarely a selling point).
- Laying a foundation for some future direction (that the company can't yet admit to for competitive reasons).

Whatever the reason, it's clear to those of us who use the resulting change that it's anything but better, stronger, faster, or whatever.

Once again, the reason doesn't matter. It is what it is. They did what they did for whatever reason they did it.

Live with it or seek out alternatives. In either case, move on.

Often, the answer doesn't help

Sometimes, you get lucky and find out why something is the way it is. And once you know why… you're no better off.

"Why did they change the user interface?"

"So it would be consistent across all kinds of devices."

"But I don't use other devices. Besides, it doesn't work on the device I have."

Doesn't matter. That's what they did and that's why they did it. Maybe it makes other people happy. Maybe someday it'll make you happy when you get another device. Maybe it'll never make you happy. Doesn't matter. It is what it is.

Sometimes understanding why doesn't help.

Ask "Why?" out of curiosity

I don't want to make it seem like you should never ask why. "Why?" is an important question when you're curious. When you're trying to learn how things work, the question "Why?" is often an important step to making better use of it.

A genuine "Why?" often uncovers reasons that can help you make sense of how things are connected and how things relate.

When you ask "Why?" in an attempt to learn something, it may occasionally be out of momentary frustration, but you're genuinely interested in the answer.

On the other hand, asking why out of pure frustration because you encounter something you don't like is rarely educational or helpful.

To sum up…

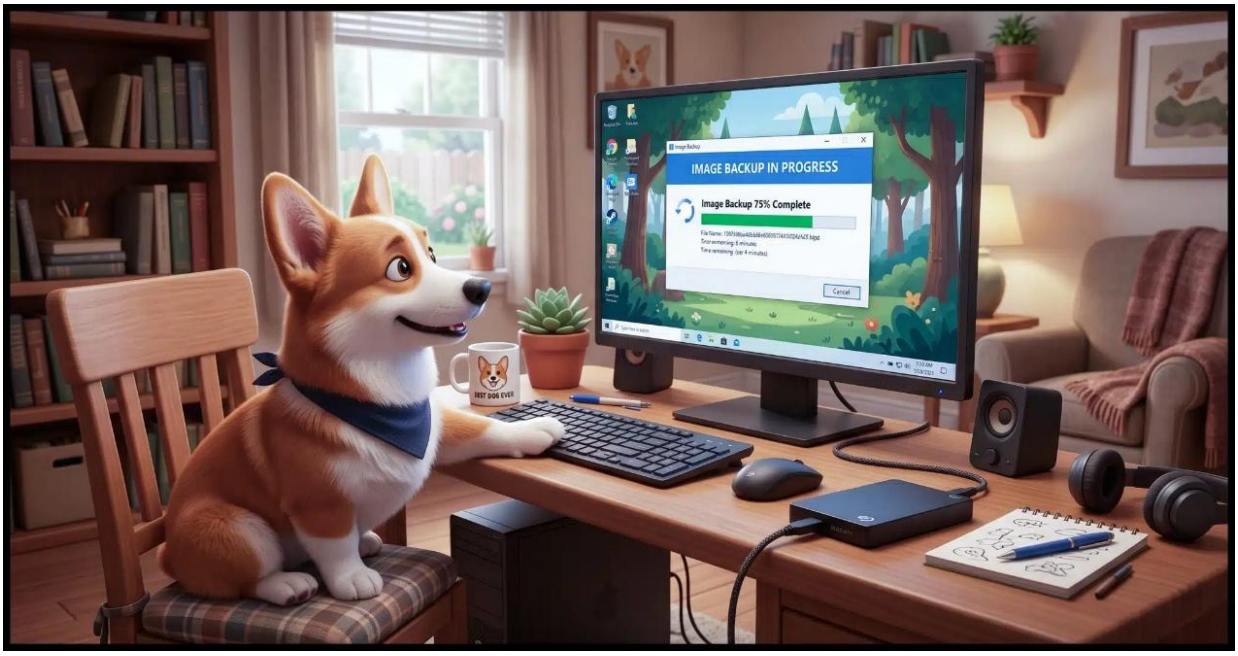
If you're genuinely curious, go ahead and ask why to learn from the answer, if an answer is available.

But if you're just frustrated, asking why is likely to frustrate you more. Don't bother. As best you can, accept what frustrates you. If that means you need to make changes — say using something else that frustrates you less — that may be a better option.

Part 2. Protect Your Data

Why Is "Back Up First" My Recommendation for Everything?

> *"In your response to the Spectre and Meltdown vulnerabilities, the first thing you recommended was to back up. Why? How does that relate to anything? How does backing up help protect me from malware and vulnerabilities?*



I harp on backing up a lot, I know. But it's on purpose.

As I've said elsewhere, nothing protects you and your data like a complete, recent backup.

Why back up first?

A complete system image backup taken prior to a change, update, or malware's arrival represents a safety net. If anything goes wrong, restoring that backup returns your computer to the state it was in prior to whatever it was that happened.

The backup I'm talking about

I want to be clear that the kind of backup I advocate is a *complete* *system image backup*.[38] That's a backup of your entire hard disk, including your operating system, installed programs, any hidden partitions, and your data.

[38] https://askleo.com/5754

Other types of backups are certainly better than nothing, but for the issues we're about to consider, it's a system image backup that will save your bacon.

Vulnerabilities make you vulnerable

Once malware gets on your machine, it can exploit vulnerabilities in software (or "bugs") and wreak havoc.

You may or may not be able to remove the malware through traditional means — for example, by using an anti-malware tool. Even then, once your security software says the malicious software has been removed, there's still no way to know with 100% accuracy that it is correct. *Malware's #1 job is to hide, and there's really no way to know your security software saw through all possible deceptions.*

Short of reinstalling your system from scratch, restoring from an image backup taken prior to malware's arrival is the only way to know for sure the malware has been removed.

So, whenever I hear the phrase *new vulnerability discovered*, I immediately think "Back up!" and use that as an opportunity to remind everyone of what I've just described.

Read-only vulnerabilities are gateways to more

Here's one way a backup can rescue you.

Some vulnerabilities only enable reading of protected memory areas. All they do is read data, so they can't damage anything, and you won't lose any data — right?

Consider the following scenario:

- Malware infects your machine.
- That malware uses some vulnerability to read otherwise protected operating system internal memory.
- What that malware finds is information that allows it to request and be granted administrative privileges on your computer.[39]
- With administrative privileges, the malware can read, write, encrypt, delete, or destroy whatever it has a mind to.

The vulnerabilities don't directly harm you; *they enable the malware's ability to harm you*.

Again, a backup protects you from the majority of that harm.

[39] While the operating system wouldn't keep the administrator password lying around in easy-to-read plain text, we can probably assume that malware poking around in the operating system's protected memory could find something it could use to this end.

Updates can cause problems

Another scenario in which backup saves your bacon is around Microsoft updates. While it's gotten better, Microsoft's track record in providing stable updates is sometimes questionable.

It's important to take all updates to protect yourself from malware that might exploit software vulnerabilities — yet the updates might "brick" your computer.

That should never happen — and it doesn't happen often — but it can.

A complete system image backup taken before the update will protect you if the update goes bad. If you find your machine unresponsive after the update, you can restore the backup image and wait for the update to be updated so it's no longer problematic.

Yes, absolutely, it's *extremely* frustrating if this happens to you. But it's important not to let the fear of updates prevent you from updating. **A complete system image backup is your fear-reducing safety net.**

It can't get any worse than this

An image backup represents a snapshot of your entire computer at a point in time — a snapshot you can revert to should anything untoward happen.

When you can always roll back to that prior snapshot of your machine, *no matter what happens from that point forward, it can't get any worse*. If it does, you revert.

That's why any time I'm faced with risk, I back up. Be it installing major updates, performing clean-up and/or repair operations, replacing or upgrading hardware, or just making changes to the work you keep on your computer, a backup is your safety net.

Do this

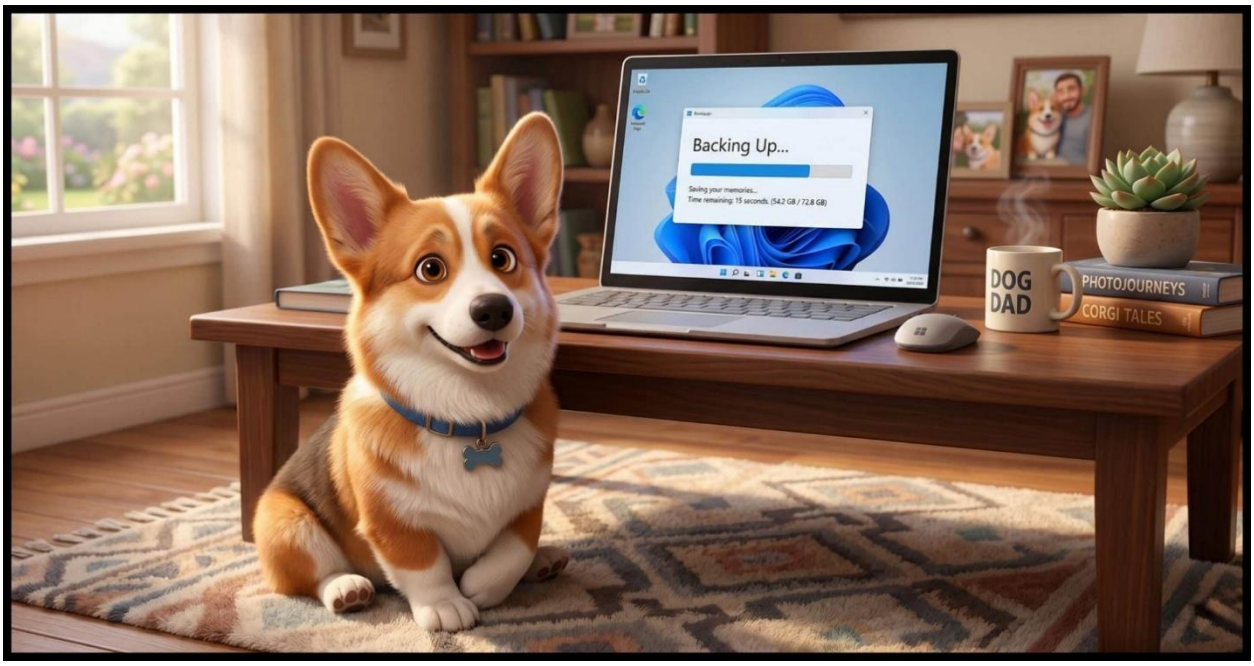
Back up.

Back up often.

Sooner or later, you'll be very, very glad you did.

And it'll always be part of my response. :-)

How to Back Up Windows



You may have heard I'm a huge fan of backing up.

Microsoft Windows includes several tools that, when used in conjunction with a third-party tool, provide a backup strategy that will protect you from almost anything that can go wrong.

Let's learn how to use those tools properly so we can get your backup strategy started.

We'll use the free edition of EaseUS Todo (there are other third-party programs that do this, but EaseUS Todo is one of my recommendations), along with File History and OneDrive, to learn eight tasks involved in a robust backup plan.

1. Make an image

Start by making an image backup of your computer. It doesn't matter if you don't know what to do with it; that'll come later. Creating an image of your computer gives you a known point to which you can always return should anything go wrong in the future.

- Creating a Backup Image Using EaseUS Todo Free[40] explains how to create an image backup of your system to an external hard disk.
- YouTube: Installing EaseUS Todo Free[41]
- YouTube: Backing up With EaseUS Todo Free[42]

[40] https://askleo.com/29600
[41] https://youtu.be=6bGF2WNcIXo
[42] https://youtu.be=GwKSt0U1G6g

This is something you'll want to do periodically and ideally automate.

2. Make a recovery disk

To recover an image — to restore your computer to operating order when something bad happens — you'll need what EaseUS calls an emergency disk.

You may also want to create a Windows recovery drive. This is a disk (a DVD or USB thumb drive) from which to boot. It includes additional tools to examine and possibly repair your system as well as the ability to reinstall Windows from scratch if needed.

- Creating an EaseUS Todo Emergency Disk[43] explains how to create a recovery disk.
- How to Create a Windows Recovery Drive[44] illustrates the process of creating a recovery drive.
- How Do I Boot From a USB Thumb Drive?[45] Make sure you can boot successfully from the recovery drives you've created.
- YouTube: Creating an EaseUS Todo Emergency Disk[46]

3. Restoring an image

Restoring an image is the process of taking a backup image you've previously created and putting it back on your computer's hard drive (which erases anything currently on that hard drive). An image restore is what you take after replacing a faulty hard drive with a new, empty one.

- Restoring an Image Using EaseUS Todo[47] shows how to restore a backup image created by EaseUS Todo.
- YouTube: Restoring an Image Using EaseUS Todo[48]

4. Restoring an individual file from an image

I rely on image backups primarily because there's no question about what's in them: everything. But sometimes you don't want to restore everything; you just want a single file, folder, or collection. You can do that from a backup image you created above.

- Restore Individual Files from a Windows Image Backup[49] shows you how. EaseUS Todo makes restoring individual files and folders from an image backup easy.
- YouTube: Restoring a File from an EaseUS Todo Image Backup[50]

---

[43] https://askleo.com/29683
[44] https://askleo.com/28233
[45] https://askleo.com/5356
[46] https://youtu.be=3fpzGxeYu-Y
[47] https://askleo.com/29825
[48] https://youtu.be=r0d23dcTBac
[49] https://askleo.com/28536
[50] https://youtu.be7jR9L9B_t48

5. Set up File History

In addition to image backups, we can utilize more "in the background" backups in the form of File History. File History sets aside space on your hard disk (ideally an external hard disk, perhaps even the same one containing your backup images) to which it writes copies of your data files periodically as they change. Using File History, you can recover a file as it was an hour ago, a week ago, or sometime in between, depending on how often files change and how much space you've set aside for backups.

- Enable File History in Windows[51] tells you how to set it all up.
- Enable File History in Windows 11[52]
- YouTube: Enable File History in Windows 11

6. Restore a file using File History

After you've had File History running for a while, you'll surely encounter a point where you want to recover a file that has been backed up.

Learn to browse what's been backed up, locate the file or files you want, and restore them.

- Restoring Files with File History[53]
- YouTube: Restoring Files with File History[54]

7. Use OneDrive for backing up

Backing up to a completely different physical location, offsite backup, has never been easier since cloud storage and synchronization tools like OneDrive.

- Using OneDrive for Nearly Continuous Backup[55] shows you how and discusses a couple of simple changes to your workflow that result in almost continuous cloud backup of all your work.
- YouTube: Using OneDrive for Nearly Continuous Backup[56]

8. Restore a file from OneDrive history

Just like File History, the day will come when you need to recover a file that's been backed up to the cloud.

[51] https://askleo.com/28383
[52] https://askleo.com/164161
[53] https://askleo.com/29116
[54] https://youtu.bejfHO6qM5WuY
[55] https://askleo.com/29368
[56] https://youtu.be=uzpAkqgWFu0

- Recover Deleted Files in OneDrive[57] points out that OneDrive has an online Recycle Bin from which you can recover deleted files.
- Recovering from Ransomware with an Online Backup[58] discusses how it can even save you from ransomware.
- YouTube: Recover Deleted Files in OneDrive[59]
- YouTube: Recovering from Ransomware with an Online Backup[60]

Don't let it happen to you

Backing up is important. I say it so often because it's so true.

I also say it because I see so much data loss and accompanying heartbreak occur when people don't realize just how important it is until it's too late.

Used together, these eight steps and three tools (image backups, File History, and OneDrive) can ensure you're appropriately backed up and need never suffer data loss again.

[57] https://askleo.com/29457
[58] https://askleo.com/29736
[59] https://youtu.be6XAkSxhy7XQ
[60] https://youtu.beuJBaLYQgOVs

Is Using the Cloud Safe?



One of the comments I received on my article on lessons learned from a fairly public online hacking[61] was very concise:

"That's why the cloud is dangerous."

I think a lot of people feel that way to varying degrees.

I strongly disagree. Using the cloud can absolutely be safe.

I also think believing the cloud is dangerous prevents you from taking advantage of the things that the cloud can do for you — things like protecting your data.

It also ignores the fact that you're already doing things "in the cloud" safely and have been for *years*.

What is "the cloud"?

I have to start by throwing away this silly, silly term, "the cloud." It's nothing more than a fancy marketing term. Ultimately, it has no real meaning.

The cloud is nothing more than services provided online over the internet.

Seriously, that's all it is.

Or you could say that the cloud is simply using someone else's computer.

[61] https://askleo.com/103465

Services that provide data storage, enable you to communicate with others, provide applications, sell you things, or answer your technical questions all happen in the cloud.

That's nothing new.

The cloud is new in name only

Most people have been using online services long before anyone thought to slap the name *cloud* on 'em.

- Do you have an online email account like Outlook.com or Gmail? You're keeping your email in the cloud.
- Do you use any kind of email? It gets from point "A" to point "B" through the cloud.
- Do you upload pictures to a photo-sharing site like Flickr, Google Pictures, or Photobucket? That's the cloud.
- Do you use any social media? Yup, they're in the cloud too.
- Do you use an online backup service? You've been backing up to the cloud.

I want to drive home the point that this thing people are calling *the cloud* is nothing new. You've been using it already — probably for years before that silly name was attached to it.

So let's jettison the name and all the baggage comes with it and call it what it really is: *online services*.

OK, fine. But is the cloud dangerous?

Or, put in less puffy terms: are online services dangerous?

No more so now than it's ever been.

In fact, I'll claim that the average online service is becoming *safer* than ever before as service providers learn from mistakes and implement industry best practices.[62]

If anything has changed at all, it's the breadth of available online services and the number of people using them.

The fact is that any tool, when misused, can be dangerous.

For example, placing sensitive information in your online email account (and *only* your online email account), and then not using proper security on that account, is *absolutely* dangerous, and always has been. It's not that online email accounts are dangerous. The danger arises from *using them improperly*.

---

[62] I don't have the data to back it up, but my feeling, based on being in this industry for as long as I have, is that by and large, service providers are getting better. The state of the art in online security is improving overall. If it seems like problems are happening more often, my sense is that it's because there are more online services now than there ever have been. My gut tells me that the number of failings as a percentage of available online services is going down.

The same is true for any online service, be it those generating the latest buzz or those you've been using for years.

We're all at the mercy of service providers

At this point, many folks point out that the security breaches that we hear about are often the fault of, or related to, a problem at the provider of the service in question.

Many are, it's true.

But you know what? *That's not new either*.

As long as there have been service providers, there have been mistakes, breaches, and policy screw-ups at service providers.

I'm not (not! not! not!) trying to excuse service providers for making mistakes or screwing up. Every fiber of their corporate being should be working to prevent security-related errors and mitigate the impact when they happen.

But the reality we have to accept is that ultimately, service providers are staffed by humans, and humans make mistakes. Saying mistakes should never happen is unrealistic.

And it's extremely poor security planning.

Besides, when it comes to security issues, we are most often our own worst enemies.

No one can protect you from you

Let's go back to the Mat Honan hack[63] for a moment, which is where that "the cloud is dangerous" comment originated.

Mat didn't lose his data because of the breaches he experienced.

Mat didn't lose his data because of problems with the online services (though there definitely were issues).

He lost his data because he wasn't backed up. Even if he had not been hacked, he was at high risk of losing everything anyway had he lost his laptop or experienced a simple hard disk failure.

Had he been backing up his data, I bet there wouldn't have even been a news story.

On top of that, the hack reached as many of his accounts as it did because *he had linked all of his accounts together*. Mat helped the hackers get to his accounts.

No, the lesson here isn't that online services are dangerous. The lesson here is that *we have to assume responsibility for our own safety*.

[63] https://askleo.com/103465

And I'll say it once again: this is not new.

How to use online services safely

Using online services safely really boils down to not much more than the guidelines we've all heard before.

All, of course, augmented by a dose of common sense.

- Back up. If it's only in one place, it's not backed up.
- Use strong passwords.[64] Set up and *keep* all account recovery information current. [65] Use extra security, such as two-factor authentication, if supported.
- Encrypt[66] sensitive data stored online.
- Understand the security ramifications of using someone else's computer or someone else using yours.
- Understand how to use internet connections provided by others securely, especially open Wi-Fi hotspots.[67]
- Don't link your important accounts together in such a way that breaching one opens the door to all of them; use different passwords[68] (and perhaps even different email addresses) for each.
- Keep your software up to date, scan for malware, and do all the other items commonly listed to keep your computer safe on the internet.[69]

All, of course, topped off with a healthy dose of common sense.[70]

Only the part about using different email addresses for different accounts is relatively new — everything else should sound familiar.

Postscript

Mat Honan, the victim of that public hacking[71] I mentioned at the beginning, published an update detailing how he's recovered from his hacking.

One quote struck me: "I'm a bigger believer in cloud services than ever before."

This is the gentleman whose experience started this very discussion. While others are quick to blame the cloud, after all is said and done, he's not one of them.

Neither am I.

---

[64] https://askleo.com/4844
[65] https://askleo.com/15584
[66] https://askleo.com/43770
[67] https://askleo.com/4790
[68] https://askleo.com/11788
[69] https://askleo.com/2374
[70] https://askleo.com/16473
[71] https://askleo.com/103465

Find his story at Mat Honan: How I Resurrected My Digital Life After an Epic Hacking.[72]

It really can be safe

There's no such thing as perfect security,[73] and that's true whether you keep your information securely locked away on your own computer in your bedroom or if you store it in the cloud. There's always something that can go wrong.

But by following basic security guidelines, there's no reason that most of the popular online services can't be used safely.

Used properly, they even *add* security by providing things like additional backups, throw-away email accounts, data replication, and more.

You do have to assume responsibility for your own security, and that includes taking reasonable precautions to prevent a problem and taking additional steps to minimize the impact should something happen.

Yes, you can avoid online services all together (just remember, that means walking away from email as well), but you'd be missing out on so many of the opportunities the internet has to offer.

Rather than asking "Is the cloud dangerous?", learn to use it safely. You'll be much better off for it.

I know I am.

Postscript

Mat Honan, the victim of that public hacking I mentioned at the beginning, published an update detailing how he's recovered from his hacking.

One relevant quote that struck me: "I'm a bigger believer in cloud services than ever before."

This is the gentleman whose experience initiated this very discussion. While others are quick to blame "the cloud", after all is said and done, he's not one of them.

Neither am I.

Find his story at Mat Honan: How I Resurrected My Digital Life After an Epic Hacking.[74]

[72] https://www.wired.com/2012/08/mat-honan-data-recovery/
[73] https://askleo.com/21748
[74] https://go.askleo.com/honanrecovery

Backups Are Great Security



We tend to think of backing up as separate from keeping our computers secure.

Nothing could be further from the truth.

To misquote the cereal commercial: backups are an important part of a healthy, secure breakfast.

Recovery from failure

Backups are a great way to ensure you're protected from hardware or software failure, or even your own mistakes.

- If your hard disk fails unexpectedly, you can restore your data from a backup image.
- If your software corrupts a file, you can restore it from a backup.
- If you accidentally delete a file, you can restore the most recent copy from your backup.

Online or offline, the drill is the same: when something goes wrong, rely on your backup to save you (or at least reduce the impact).

But wait, there's more!

Recovery from malware

Backups — specifically image backups — play a key role in your overall security.

- If malware infects your system, you can restore from a backup image taken prior to the malicious software's arrival.

- If malware corrupts a file, you can restore it from a backup.
- If malware deletes files, you can restore the most recent copies from your backup.

No protection from malware is ever 100% safe. We're all at risk. A proper backup dramatically reduces the impact of malware that does make it through.

With a full-image backup, malware becomes an annoyance instead of a disaster.

Recovery from ransomware

Ransomware is just malware.

Everything I've listed above about malware applies to ransomware.

If ransomware infects your system, you can restore from a backup image taken prior to the malicious software's arrival.

If ransomware encrypts files, you can restore the most recent copies from your backup.

Yes, it is that simple.

And yet…

"But ransomware can encrypt backups!"

People die wearing seatbelts, but that's no reason not to buckle up. While it is possible for ransomware to encrypt backups, that's no reason not to back up.

You're less likely to die wearing a seatbelt, and you're less likely to be affected by ransomware if you have good backups.

Here's why.

- Not all malware is ransomware. Your backup still protects you from those.
- Not all ransomware encrypts backups. Your backup still protects you.
- Many backup tools take steps to protect your backups from ransomware.
- Backups kept offline are out of the reach of ransomware.

Again, ransomware is just malware. Malware that is not ransomware that deletes backups has been around for a long time. Same issue. Same solution.

You're safer with a backup than without.

"So I'll disconnect my backup drive when I'm not backing up."

I recommend you do not disconnect your backup drive.

That's like saying you'll put on your seatbelt when you know you're going to be in an accident.

You just don't know.

By keeping your backup drive connected, you can automate the backup process so you don't have to think about it, much like making your seatbelt an automatic habit when you get into the car.

Having a backup process work without needing your intervention is more important than worrying about the backups themselves being encrypted by ransomware. If you have to initiate a backup to make it happen, it won't happen.

You will forget.

And you'll be left without a current backup, even when you need it for reasons other than ransomware.

Your backups are an important part of your security strategy

Adopting that mindset means:

- Automate periodic backups, ideally daily and/or continuously.
- Leave your backup drive connected. If you're worried about ransomware encrypting your backups, you can take one or both of these steps.
- Use a tool that protects your backups. Macrium Reflect's Image Guard feature is one example. There are others.
- Periodically copy your backup offline. Yes, this is a manual step that you might forget, but it's safer to forget this than to forget backing up completely.
- Use online backup services. Many, like Dropbox or OneDrive, have the equivalent of a Recycle Bin as well as additional protections for ransomware.

Above all: back up. Someday, somehow, you'll be very glad you did.

Part 3: Protect Your Computer

Eight Steps to a Secure Router

> *"I'd like to know how to clear the history of my Linksys router. I'd also like to know how I can make it more secure and protect it from hacking.*



The topic is an important one: how do you make sure you have a secure router? It's your first line of defense against automated malware attacks trying to get at your computer from the internet to install more malware.

You want to be sure there aren't any big gaping holes. Very often and by default, there are.

Here are the most important steps to a more secure router.

First, a caveat: My router versus your router

There are hundreds, if not thousands, of different routers. Different brands and models have varying capabilities, power, and, of course, cost.

Most importantly, they have different administration interfaces.

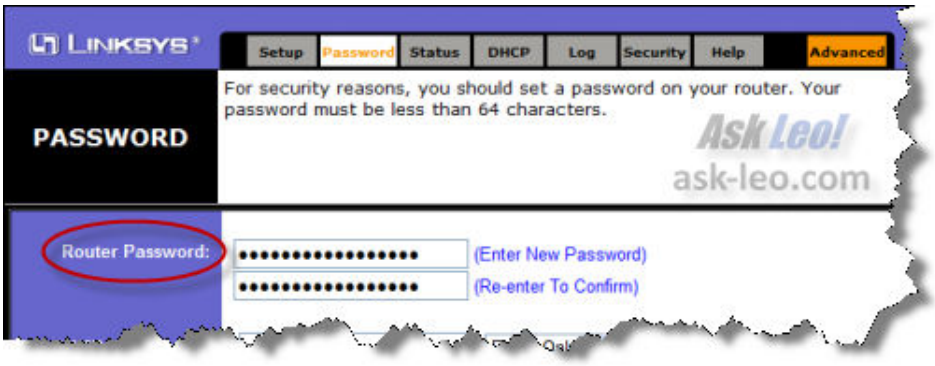
What that means is, I can't tell you exactly how to make changes to your router step-by-step. The concepts I'll cover apply to almost all consumer-grade routers, and I'll be using an old and popular LinkSys BEFSR81 router and LinkSys WAP54G access point as examples.

You'll need to "translate" the examples to the equivalent settings on your own router or access point. Make sure you have access to the documentation that came with your router or locate it online.

You may well have a single device that combines the router and wireless access point. You probably refer to it as your router, but in reality, there are two separate devices — a router that deals with network access and a wireless access point that provides your Wi-Fi connectivity — housed in a single box. In my example, they are separate devices.

1. Change the default password

If you do nothing else to secure your router, *change the default password*. Change it to be something long and strong.[75] If your router supports it, a pass*phrase* of three or more words might be ideal.



The reason for this is that it's a common gaping security hole.

For many years, almost every router and access point from the same manufacturer was shipped with the same default password. For LinkSys, if your login is a blank username and a password of "admin", as outlined in its manual, *anyone and everyone knows it.* Anyone can log in to your router and undo the security steps we're about to take.

Then, any malware that takes advantage of the default passwords on routers can make changes without your knowledge.

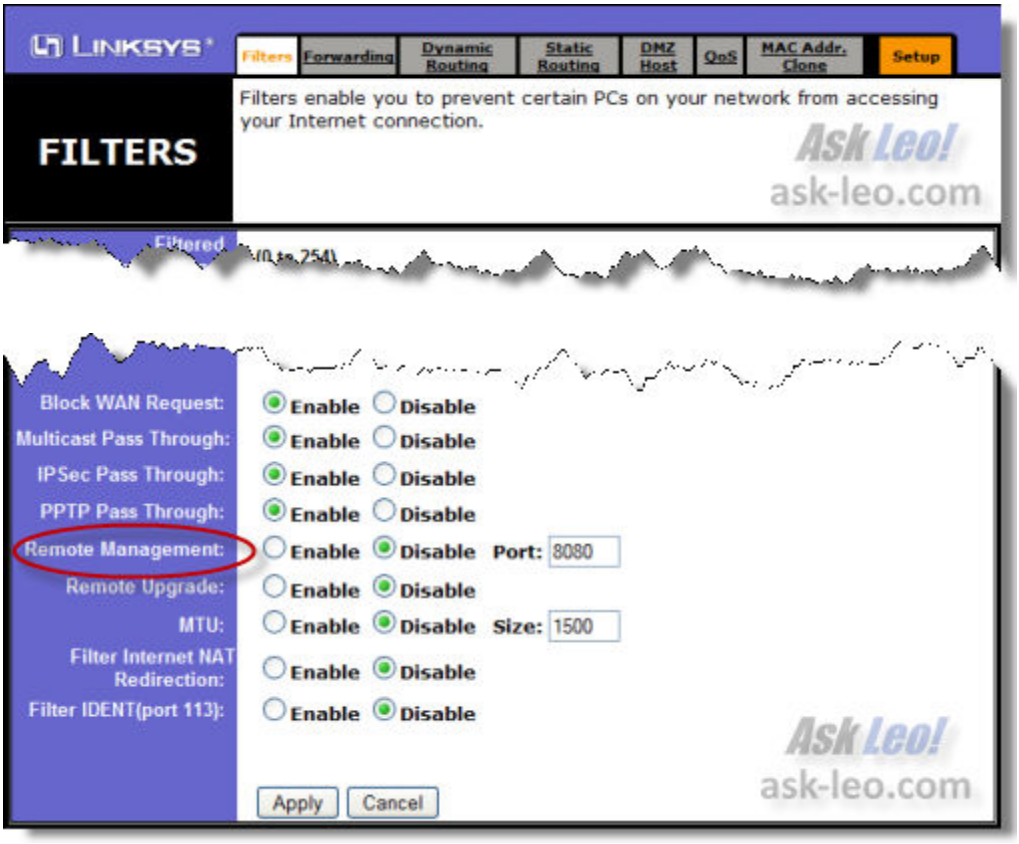
Fortunately, in recent years, most — though not all — router manufacturers have been getting smarter. If the instructions that came with your router included checking a sticker on the actual router for the admin password, and that looks like a strong password, then the security hole is significantly smaller. Now only those people who can walk up to your router and look at that sticker can get in.

I'd change the password anyway.

2. Disable remote management

Remote Management is a feature that allows your router to be administered from anywhere out on the internet.

[75] https://askleo.com/4844



While this setting (coupled with a *very* strong password) might make sense for a handful of people,[76] for most folks there's absolutely no need to administer the router from anywhere but the local machines connected to it.

Make sure the remote management setting is off.

3. Turn off Universal Plug and Play

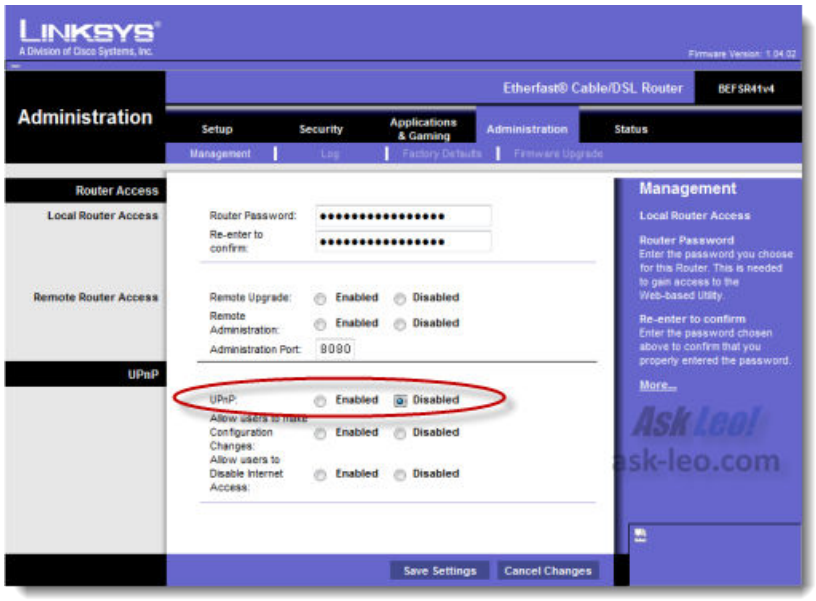
Universal Plug and Play (UPnP) is a technology that allows software running on your machine to configure services like port forwarding (a way of allowing computers outside your network to access your local computers directly) without you having to go in and administer the router manually.

It seems like a good idea, right?

Nope. Turn it off.

---

[76] Some ISPs will insist on this, but they'll also prevent you from administering your own router as well. More common is a scenario where you're responsible for supporting someone else's network – say that of a friend or family. Remote administration can be helpful in a case like that. Even so, I'd think twice about setting it up, and would insist on an exceptionally secure password if you do.

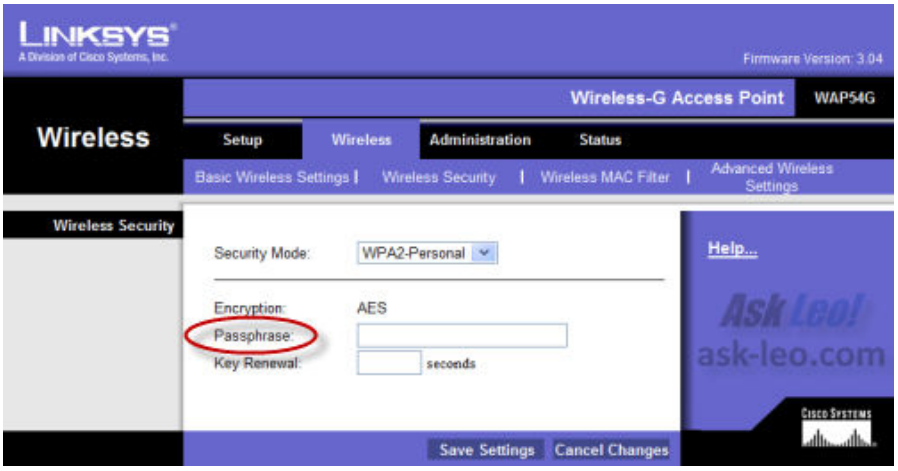


It turns out that malware can also be UPnP-aware and make malicious changes to your router without your involvement or awareness.

(Note: UPnP is unrelated to Windows "Plug and Play" hardware detection; it's just another unfortunate collision of similar names.)

4. Add a WPA2 key

It's time for another password, this time to secure and encrypt your wireless connection.



First, use **WPA2**, not WEP. WEP encryption turns out to be very easily crackable,[77] and even WPA (without the 2) has been shown to be vulnerable.

[77] It's essentially like having no encryption at all.

Second, just as you did for the router's administration password, select another good, secure key/password/passphrase (the terms are roughly interchangeable here). You only need to enter it once here and once on each device allowed to connect to your wireless network.

Having a strong WPA2 key ensures that only machines you allow on your network can see your network, traffic, and router.

5. Disable WPS

WPS, or Wi-Fi Protected Setup, doesn't live up to its name; it's not very "protected" at all.

WPS was intended to make setting up a protected Wi-Fi network easy. WPS would, with the push of a button, set up Wi-Fi encryption between the router and clients that supported it.

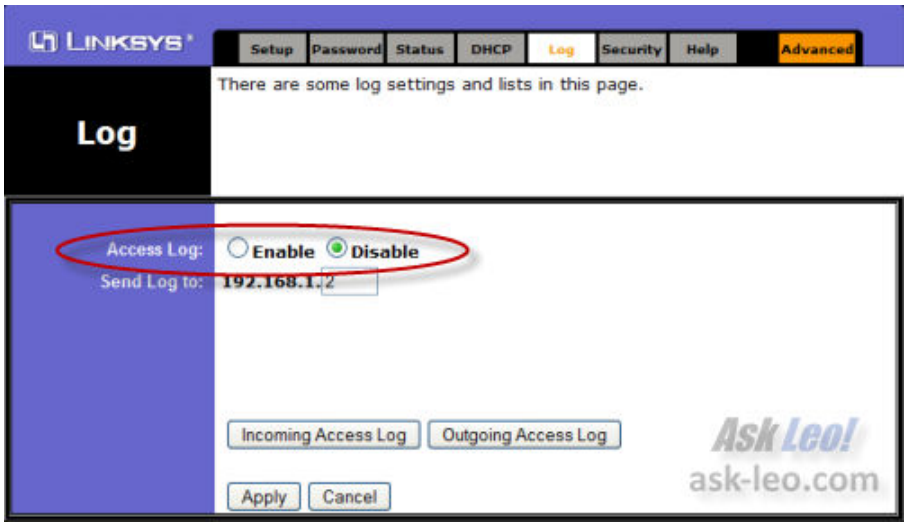
The problem with WPS is that the protocol is flawed. It is vulnerable to brute force attacks. A malicious entity within range can force their way onto your network, bypassing any encryption keys you set up.

WPS is enabled by default on many routers. Turn it off.

6. Turn off logging

This has less to do with configuring a secure router, and more to do with maintaining your privacy.

This is also about making sure logging is still turned off, since if a router supports any kind of logging at all, it'll likely be off by default.



Disable the logging, and no information will be kept on the router, or sent to any other machine. This should also clear any log the router has.

It's worth pointing out that most consumer-grade routers do not have the capacity to keep logs themselves. If they keep anything, it will be a shorter, partial log. When enabled, some offer to send the log to one of the computers on your network for storage. Disabling logging will not erase any logs stored elsewhere.

7. Secure your router physically

As we've already seen, even if the default administrative password is unique to your device, it's still visible to anyone with physical access to the router who can see the sticker on which it's printed.

In fact, your secure router may not be secure at all if anyone can just walk up to it.

All your router's security settings can be reset in a flash if someone has physical access to the device. Almost all routers have a "reset to factory defaults" mechanism (typically, holding a reset button for a certain amount of time). If someone can walk up to your router and do that, all the security settings you've just enabled may be instantly erased.

Only you can judge whether you need this extra level of physical security, but do consider it. It may be as simple as keeping the device in a locked room or closet.

8. Check for firmware updates

Routers (and access points) are just small computers dedicated to a single task: handling network traffic. Normally the software — referred to as “firmware” since it’s stored within the device’s hardware — works just fine.

Unfortunately, security vulnerabilities are sometimes discovered, and you need to update your router’s firmware to stay secure. This usually involves downloading a file for your specific router and using its administration interface to install the update. Some routers can fetch and install the update directly. Either way, the update is a manual step you need to take.

Checking to see if there’s a firmware update for your router is also a manual step. Some routers perform the check at the push of a button in the administration interface. If not, you need to visit the manufacturer’s support site, look for information pertaining to your specific model, and determine if a newer version of the firmware is available.

Two steps that aren't steps

Each time I mention this article, folks make two suggestions for Wi-Fi that do not improve security at all. In fact, they may harm security in some ways by providing a false sense of added security.

The first is MAC address filtering. I discuss this in more detail in Is MAC Address Filtering a Viable Wireless Security Option?,[78] but the bottom line is that like a cheap padlock, MAC address filtering only keeps out honest people. If someone wants to access your network, MAC address filtering is easily bypassed.

The second suggestion is to turn off SSID broadcast on wireless networks. Even when not being broadcast, the SSID is still visible and unencrypted in the packets of traffic sent to and from the router. Disabling the broadcast does nothing to prevent someone with skills from easily discovering it. I discuss this in more detail in Does Changing or Disabling the Broadcast of My Wireless SSID Make Me More Secure?[79]

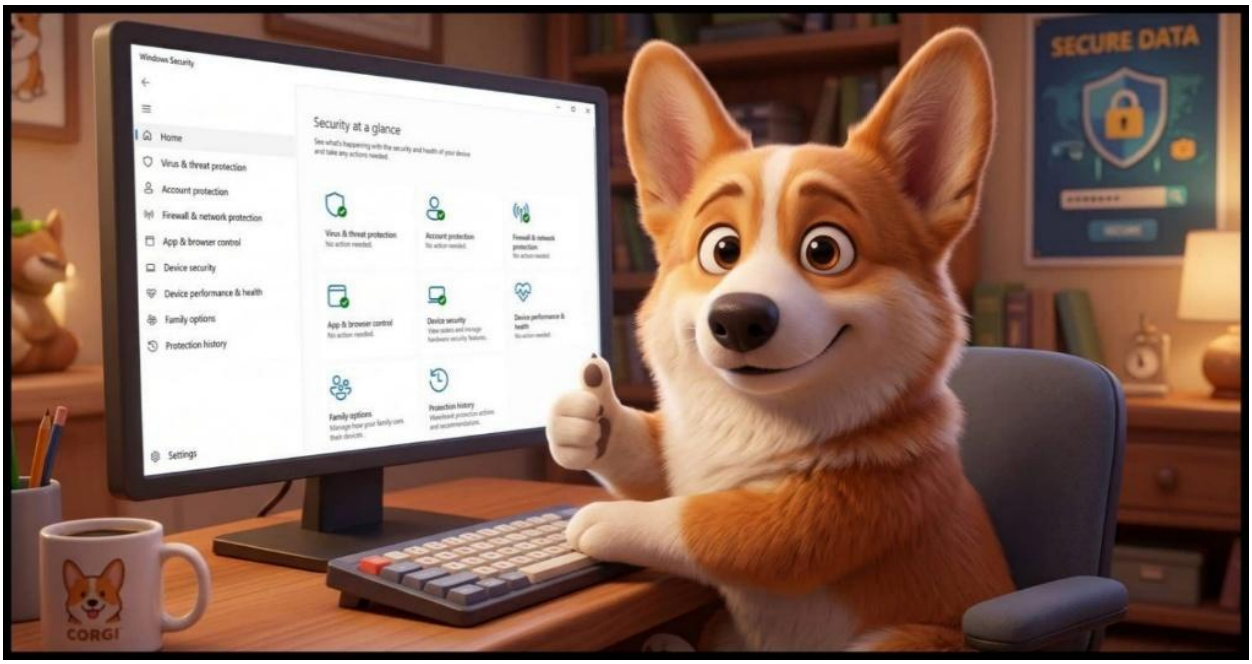
[78] https://askleo.com/4350
[79] https://askleo.com/5049

When it comes to Wi-Fi, putting a WPA2 password on the connection is currently your best security measure.[80]

[80] Router Security (https://routersecurity.org/) has a much deeper list of steps and issues to consider if you want to pursue this further.

What Security Software Do You Recommend?

> *"What security software should I use? What anti-virus is the best? How about a firewall? And what about spyware? Should I use one of the all-in-one packages that claim to do everything? Is there anything else I need?*



As you might imagine, I get questions like this all the time. As a result, I do have recommendations for security software and techniques to stay safe in various articles all over Ask Leo!

To make your life a little easier, here's a short version that sums it all up into four steps.

The short-short version

- Windows' built-in Windows Security remains my recommended security solution for most systems.
- Your router can serve as your primary firewall at home or work.
- Leave the Windows Firewall enabled unless it causes problems.
- Let Windows Update keep your computer as up to date as possible.

That's it. Good basic protection in four steps. That's it.

Basic security software: Windows Security

Windows Security — previously known as Windows Defender — comes pre-installed with Windows, and Microsoft seems to improve it with every release.

Windows Security does a fine job of detecting malware without adversely affecting system performance or nagging you for renewals, upgrades, or upsells. It just does its job quietly in the background: exactly what you want from your anti-malware tool.

The ratings game

Every so often, Windows Security comes under fire for rating lower in tests published online than other security packages. I get push-back — often angry push-back — that it remains my primary recommendation.

There are several reasons I stick to that position.

- No anti-malware tool will stop all malware.[81] Malware can and does slip by even today's highest-rated packages.
- What is "highest-rated" changes depending on the date, the test, and who's doing the testing. There is no single clear, consistent winner.
- Regardless of how the data is presented, the differences among detection rates across most current anti-malware tools is relatively small compared to other factors.

There are also some practical reasons I continue to prefer Windows Security.

- It's free.
- It's already installed; there's nothing you need to do.
- It rarely impacts system performance.
- It keeps itself up to date using Windows Update.
- It has no hidden agenda; it's not going to pester you with renewals, upgrades, or up-sells to tools you don't need.

It's not perfect, but no security tool is.

My recommendation stands. Windows Security remains a solid, free security package with minimal system impact. It should be appropriate for almost everyone.

Alternative security software and additions

I also recognize that Windows Security might not be the right solution for everyone. No single product is.

This is where I run into some difficulty trying to make recommendations. The landscape keeps changing. More than one once-free tool has moved to promoting their paid product so heavily that the free version virtually disappears. People download and install programs thinking they are free, only to discover it's a "free trial" or "free download" (if you want to keep it past a certain length of time, you're required to purchase it).

Some programs are as much a self-promotion tool as a security tool, bombarding you with sales pitches and upgrade offers to the point of getting in the way of your work.

[81] https://askleo.com/6276

Things keep changing. So, to the extent that I mention specific tools below, *caveat emptor*: "let the buyer beware". I can't honestly predict that the tools will remain recommendation-worthy.

A short list of top recommendations from around the internet include:

- Avast
- BitDefender
- ESET
- Malwarebytes
- Webroot

Note that these aren't necessarily free.

There are plenty of others as well. I've selected these because they have shown up fairly consistently in the ratings game over the years. Don't take offense if I've overlooked your favorite.

Caveats to all

I need to reiterate some important points.

- Beware of the word *free*. In most cases, a "free trial" is just that: a trial of a full-featured product eventually requiring payment. In some cases, like MalwareBytes, the "free trial" becomes a truly free version after the trial ends. In other cases, they are two separate downloads. And in other cases, there is no truly free version at all. Be sure you know which you are getting.
- Regardless of which you download, you are still likely to be faced with upgrade and upsell offers. Unless or until you know you want this, decline.
- Speaking of declining: when installing any of these, *always choose custom installation*, never the default. The default may include unrelated software you don't need or want.
- Windows Defender, the anti-malware component of Windows Security, will turn itself off if you install a third-party tool. It should turn back on if you uninstall.[82]

What else besides security software?

Besides having security software, I recommend three other essential actions to stay safe: enable a firewall, back up, and stay up to date.

A firewall

For home and business use, I recommend the use of any good NAT router as a firewall. You almost certainly already have one.

They don't have to be expensive and are one of the simplest approaches to keeping your computer safe from network-based threats. If you trust all the computers on the local network side of the

[82] This is because you should not have multiple security packages performing real-time scans at the same time.

router, there's no need for an additional software firewall[83] besides the one already present in Windows.

Back up

I *strongly* recommend you back up regularly.

In fact, I can't stress this enough. Up-to-date backups completely avoid 99% of the disasters I hear about.

Macrium Reflect[84] and EaseUS Todo[85] are the backup tools I currently use and recommend.

Stay up to date

Keep your computer — Windows *and* all the applications you run — as up to date as possible.

This happens automatically, as long as you don't take steps to disable it. Needless to say, I strongly recommend you not disable those functions, and let Windows Update keep your system as up to date.

Many of the security issues we hear about are due to individuals (and, sadly, corporations) who have not kept their operating system or applications current with the latest available patches.

And finally, Internet Safety: 7 Steps to Keeping Your Computer Safe on the Internet[86] has even more tips for keeping your computer safe.

A note about Windows 10

You can continue to use Windows 10 safely after the end of support date. See What Happens at Windows 10 End of Support?[87] for more.

Windows Security will continue to receive security database updates into 2028. See Why I Don't Expect a Windows 10 Apocalypse for details.[88]

And you may be able to sign up for the ESU — Extended Security Updates[89] — program for additional peace of mind into 2027.

If you're using a third-party security package, check with that provider's plans, but in general, most will continue to work on Windows 10 for a long time after Microsoft's official end-of-support date.

[83] https://askleo.com/3484
[84] https://askleo.com/4996
[85] https://askleo.com/29600
[86] https://askleo.com/2374
[87] https://askleo.com/145971
[88] https://askleo.com/181353
[89] https://askleo.com/175852

How Do I Remove Malware from Windows?



One question that shows up frequently in the Ask Leo! inbox is how to remove malware.

The scenarios differ, but the problem is the same: a machine has been infected with spyware, a virus, ransomware, or some other form of malware, and that machine's owner is having a tough time getting rid of it. Often, anti-malware software has been installed that "should" have taken care of it before it got to this stage.

Hopefully, that will never be you.

Let's review the steps I recommend for removing malware *and* reducing the chances of it happening again.

A word about prevention

If there's one thing I would have you take away from this article, it would be this:

Prevention is less painful than the cure.

As we'll see in a moment, the steps to remove malware can be painful and time consuming, and you run the risk of losing data. Knowing how to stay safe on the internet[90] is much, much easier in comparison.

Let's look at what to do when prevention has failed.

[90] https://askleo.com/2374

Back up

My strong recommendation is to start by taking a complete image backup of your system.

Why would you want to back up a system you know is infected with malware?

A backup taken now is an "it-can't-get-any-worse-than-this" fallback. Some of the techniques we use to remove malware run the risk of breaking things and making the situation worse. With this backup at the ready, you can always restore and start over with nothing lost. With this backup at the ready, you can always restore and start over with nothing lost. It will also allow you to carefully restore data after some of our more drastic recovery steps.

Restore a prior backup

If you've been taking regular backups, this is the most expedient step and can save a lot of time and energy.

Restore your machine completely from the most recent full system backup plus any incremental backups taken before the infection occurred. Except for learning from the experience, you're done.

Unfortunately, most people don't have this option available. Most people don't begin backing up until after they've experienced data loss or a severe malware infection. One of the lessons they learn is that **a recent backup can save them from almost any problem, including malware**.

Update the anti-malware database

If you have anti-malware software installed, make sure it's up to date. This includes more than just the software itself; *the database of malware definitions* must also be current.

Almost all anti-malware tools use databases of malware definitions. They change daily, if not more often. As a result, they must be updated regularly. If you're using the built-in Windows Security program, the database gets updated along with Windows Update.

Most programs do this automatically, but if for some reason they don't, the program will not "know" about the most recent forms of malware. Make sure your database is up to date, so it recognizes the latest threats.

Perform a full scan

Anti-malware tools regularly perform a "quick" or fast scan. That's typically sufficient for day-to-day operations.

But not today.

Fire up your anti-malware tools and run a full/advanced/complete scan of your entire system drive. If you have a single tool, that might be one run; if you use multiple tools, such as separate anti-virus and anti-spyware tools, then run a full scan with each. This may take some time, but let the tools do their job.

This also applies if your anti-malware automated scans have stopped working for some reason (that reason often being malware). If this full scan discovers something, it might be worth checking to make sure the security software is properly configured to still scan automatically.

Try another anti-malware tool

No anti-malware tool catches all malware.

I'll say it again: *there is no single tool that can catch every single piece of malware out there*. None. Some are better than others, some catch more than others, but none of them catch everything.

So using additional reputable tools is a reasonable approach.

I recommend the free[91] version of Malwarebytes' Anti-Malware[92] as the first tool to use. It has a reputation for removing some nasties other tools apparently miss. Once again, run a full scan.

Regardless of which tool you select, *stick with reputable tools.* When a machine is infected, most people tend to panic and download just about anything that claims to be an anti-malware tool. *Don't do that*. There are many less-than-reputable individuals out there ready to take advantage of your panic.

Do some research before downloading anything, or you may just make the problem worse instead of better.

Research specific removal instructions

If your anti-malware software tells you the *name* of the specific malware you're dealing with, that's good information, even if it can't remove it.

Search for that malware, and you're likely to find specific removal instructions at one or more of the major anti-malware vendor sites. These instructions can be somewhat technical and intimidating, so take your time to follow them precisely, or get a techie friend to help.

Those instructions often come with offers to remove the malware for a price. As long as it's an *option* (in other words, the manual removal instructions are also provided), then it may be a viable alternative if the company is one you trust. On the other hand, if all you're presented with is a promise and a price, move on.

Some sites offer free tools you can download to remove specific malware. Once again, *use caution*. When the tools are from reputable sources, they're a quick way to avoid some hassle. When the tools are just more malware in disguise, they'll make your problems worse.

If you download anything to help address the problem, make sure that wherever it comes from, it's an organization you know and trust.

[91] Yes, there is a truly free version. See the Malwarebytes article (https://askleo.com/5765) for details.
[92] https://askleo.com/5765

Surrender, reformat, and reinstall

There is only one sure-fire, 100% guaranteed way to remove any virus.

In fact, it's the only way to *know* that you've removed a virus. Once infected, none of the steps above are guaranteed to remove malware, *even if they report that things are clean*. Once infected, all bets are off. An infection can fool anti-malware software into thinking that everything is fine even when it's not.

There's just no way to know.

The only way to be sure you've removed all viruses is:

- **Back up**. If you haven't already, back up the entire system. You'll use this to restore your data after we're done.
- **Reformat**. Reformatting erases the entire hard disk of everything: the operating system, your programs, your data, and most important of all, all malware. This may be part of the next step, as most Windows set-up programs offer to reformat the hard drive before installing Windows.
- **Reinstall**. Yes, reinstall everything from scratch. Reinstall the operating system from your original installation media or download. Reinstall applications from their original media or downloads saved elsewhere.
- **Update**. Update everything, making sure to bring Windows completely up to date for the most current protection against all known and patched vulnerabilities. Applications, particularly your anti-malware tools, should be updated as well.
- **Restore**. Restore your data by carefully copying it from the backups you created when we started. By "carefully," I mean take care to only copy the data you need so as not to copy back the malware. There is no guarantee you won't copy the malware back, so copy only what's absolutely needed, and make sure your anti-malware tools are running and up to date.
- **Learn**. Take stock of how this happened, what you might have done to get infected in the first place, and what might have helped you recover more efficiently. Schedule a frequent system backup.

It's not your fault, but it is your responsibility

By now, I hope you can see why prevention is so much less painful than the cure.

Taking a few extra steps to keep things up to date, avoiding those cute virus-laden downloads and attachments, and learning how to stay safe[93] is much easier than the recovery process I've just outlined.

And having backups[94] can make the recovery process as close to painless as possible if you do get infected.

[93] https://askleo.com/2374
[94] https://askleo.com/6643

It's not your fault. But *it is your responsibility* to learn how to stay safe when you use your computer.

In an ideal world, we'd never have to worry about malware or bad guys fooling us into doing things we shouldn't. But you already know this isn't an ideal world; software isn't perfect and never will be. And there will always be someone out to scam the vulnerable.

Even though it's not your fault, you need to get educated and take the steps needed to stay safe.

Right or wrong, it's just a practical reality.

How Do I Remove PUPs and Other Unexpected Things From My Computer



Ending up with random software on your machine that you never wanted in the first place is annoying as all heck.

So-called PUPs (for Potentially Unwanted Programs, although there's rarely any "potentially" about it) are tools, settings, utilities, browser toolbars, extensions, and other types of software that arrive on your computer as a result of installing something else. PUPs are rarely related to what you're installing.

I'll talk a little about prevention, but first, let's walk through the steps I recommend when you realize you've been saddled with software you didn't know you'd agreed to and certainly never wanted.

Start with a backup

The steps we are about to take have a small chance of causing problems.

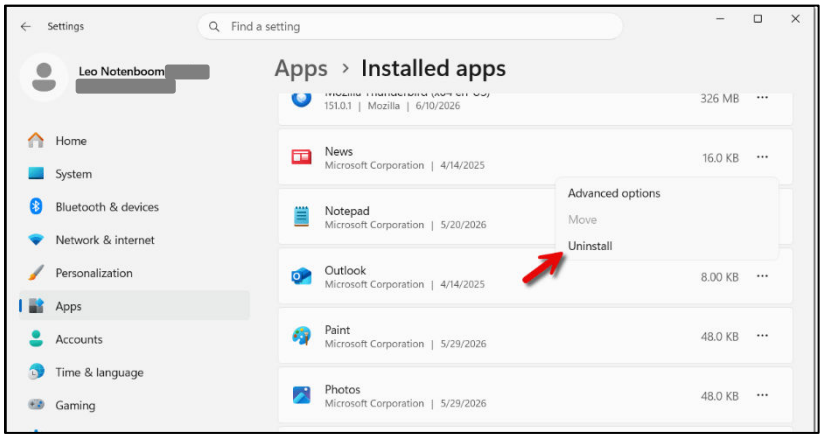
Whenever that's the case, I recommend you take a full image backup of your machine before you do anything else. That way, you'll have that backup to restore should anything below go wrong.

Uninstall the somewhat well-behaved PUPs

A number of unexpected toolbars and other applications that show up on your machine are relatively well behaved: they are somewhat easy to uninstall using official mechanisms.

Start in the Windows Settings app, and click on Apps (Windows 10), or Apps -> Installed Apps (Windows 11).

Look for the item by name. Sometimes that can be tricky, as applications are intentionally named obscurely to make them more difficult to remove, but the well-behaved items we're looking for here should be relatively clear. Look for names that include the word *toolbar* or *extension* in particular, as those are some of the browser-behavior-altering pests that often put us in this scenario.

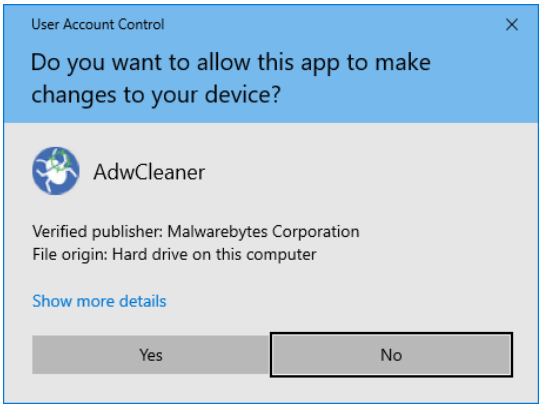


Right-click the item you want to uninstall, and click **Uninstall**.

Even if that appeared to work, take the next steps, because in many cases there will be traces left over, and sometimes those traces can reinstall the PUP.

Run Malwarebytes AdwCleaner

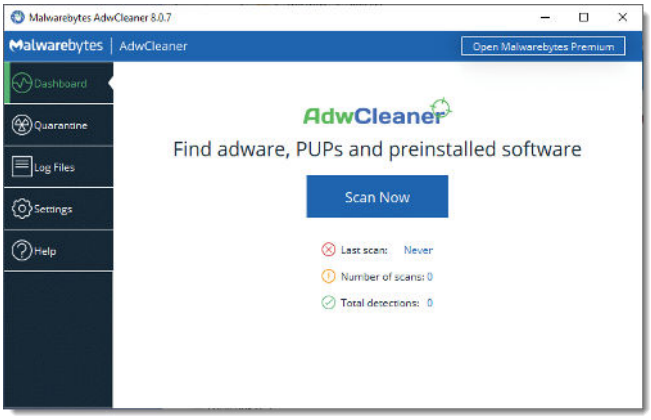
AdwCleaner was purchased by Malwarebytes in 2016 but remains a separate tool. You can download it from Malwarebytes here.[95]



AdwCleaner has no installation. Once downloaded, run it and answer **Yes** to any UAC prompt.

Click **I agree** to any licensing terms agreement. Click **Scan Now**.

Once the scan is complete, AdwCleaner will present its scan results.



If you're not certain what AdwCleaner finds, go ahead and let it clean up anything you don't recognize by clicking **Clean & Repair**. (It first warns you that all programs should be closed.)

[95] https://www.malwarebytes.com/adwcleaner

The ultimate removal

Even with the tools I've outlined, and other tools that may also be used or may come along later, there's a real possibility that the unwanted software will *still* not be completely or successfully removed. This often happens when the PUP is new and the security-software makers are still catching up to the latest tricks it might be playing.

It's worthwhile to consider restoring to a recent backup image.[96] Restoring will make these things go away *every single time*.

If you have a backup image of the machine from before the pests were installed, you can restore your machine to that image, and they're gone. No fancy tools are needed, and you needn't just hope that it works. Restoring to a prior backup works every time.

Presuming, of course, you have one.

Prevention

PUPs and related pests arrive in several different ways, but most commonly are "offered" to you when you install[97] or even update[98] something else. Often, the offer is hidden and defaults to Yes. The technical loophole is that by choosing this default (or not unchecking the appropriate box) when you install some program, you're *asking* for this other software, these PUPs, to be installed.

Don't do that.

Whenever you install any software — *even software you've purchased* — always choose the Custom or Detailed option — whatever option is *not* the default option.

Then pay close attention to every choice you're presented. If it offers you something that is not clearly related to the software you want, *uncheck it*. If it offers to change your search page, *uncheck it*. If it offers to install some toolbar, *uncheck it*.

You get the idea.

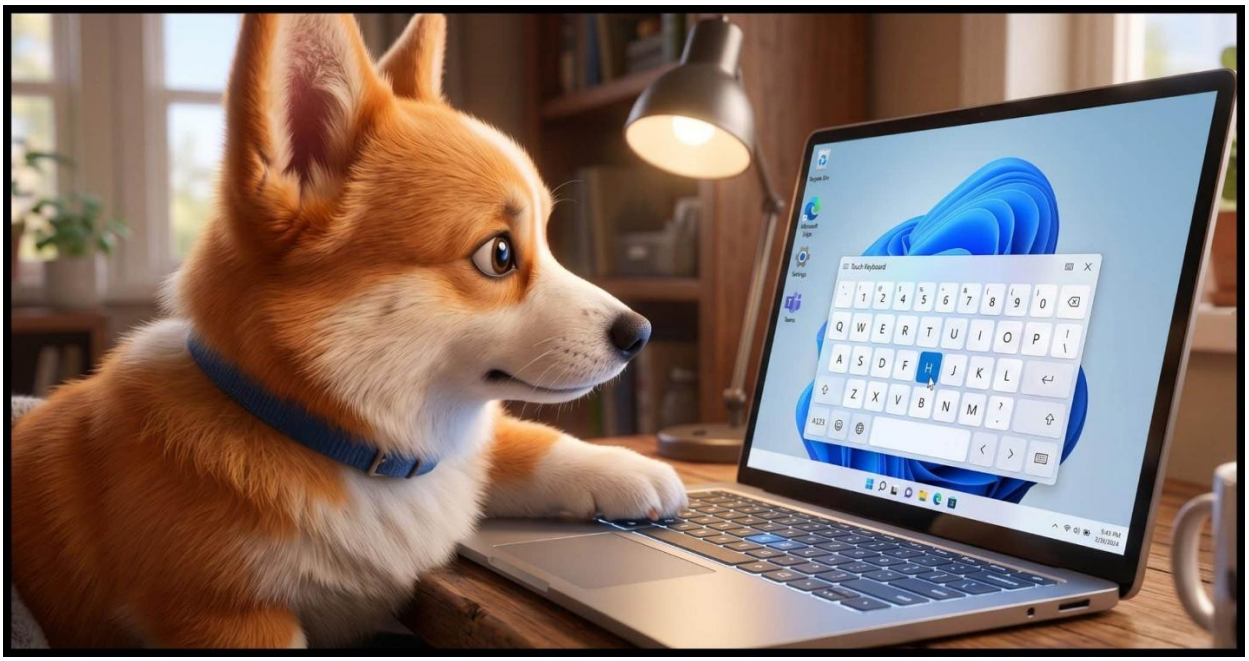
The bottom line is, if you're not careful when you install software — even software from reputable vendors — you may end up with things you never expected or wanted.

There's nothing "potentially" unwanted about it.

[96] https://askleo.com/6643
[97] https://askleo.com/4906
[98] https://askleo.com/24027

Will Using an On-Screen Keyboard Stop Keyloggers?

> “ *Will using the on-screen keyboard in Windows stop keyloggers?*



The short answer is *no*.

I get a surprising amount of pushback on this, but the truth remains: while virtual keyboards might stop some keylogging, it's nothing you can count on to be 100% effective. It doesn't stop most keyloggers these days.

Keyloggers are malware that records your keystrokes. The goal is to capture login usernames and passwords so hackers can get into your accounts. Let's look at the various ways your keystrokes can be intercepted and logged.

The keyboard connection

When you type a key on your keyboard, a microprocessor within it sends signals via a cable or wireless connection to your computer.

Here we encounter the first point of vulnerability. No, not the microprocessor in the keyboard (technically possible, but exceptionally unlikely), but the cable — or rather, what the cable plugs into.

Public computers are particularly lucrative targets. Someone comes along and installs a physical device between the computer and keyboard that intercepts and logs every keystroke entered. Sometime later, they come back, remove the device, and take all the information that users entered.

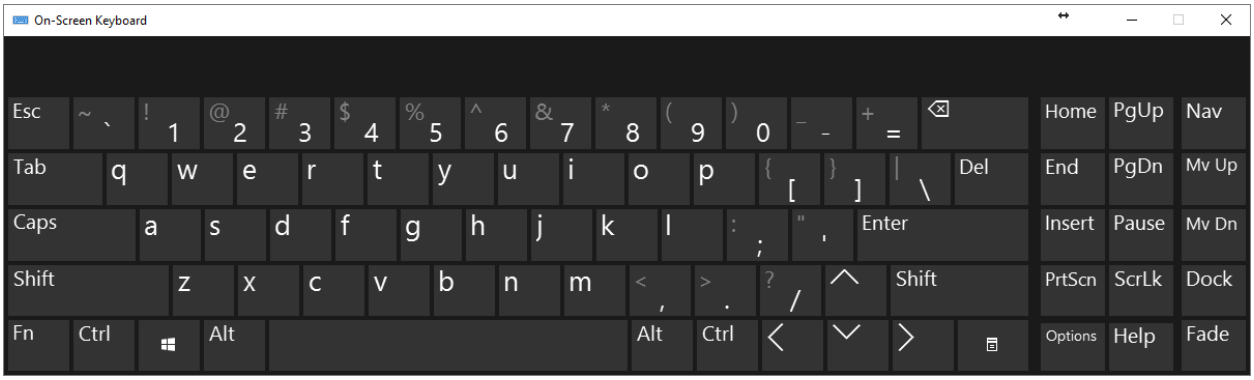
Wireless keyboards can be worse, because they broadcast the keystrokes you're typing. Any receiver within range can listen in. Wireless keyboards encrypt their data, so in theory the information should be safe, but the quality of the encryption varies based on the age and make of the keyboard. In addition, the concept of "in range" turns out to be further than most people think, particularly for a thief with equipment dedicated and tuned to this purpose.

On-screen keyboards protect you against those two specific keyboard-related threats because they bypass the components of the keyboard hardware that could be compromised.

The bad news is that hardware-based keyloggers are rare. Software-based threats are more common.

The keyboard software

Once your keystrokes arrive at the computer from the keyboard, they are processed by a keyboard device driver, which (to oversimplify) translates the keyboard *scan codes* to the letters, numbers, and symbols Windows applications expect.



Keyloggers typically insert themselves into the receiving end of this process: they get the keystrokes from the keyboard as they are passed on to Windows.

This is where the on-screen keyboard scenario gets interesting. The on-screen keyboard application is a virtual keyboard. It has its own device driver that makes it look like a real keyboard to Windows.

As a result, the keystrokes it sends to Windows can easily be captured by the same keylogging software that captures keystrokes from the real keyboard, if that keylogger has been installed in the proper place.

A keylogger is just malware

The two most important concepts to remember are these:

- Keyloggers are just malware.
- Malware can do anything.

What you might call a keylogger can capture more than keystrokes. Let's say you use the on-screen keyboard by using your mouse to point and click at the image of a key on the keyboard. A keylogger could, then, for every mouse click:

- Capture the location of the mouse on the screen.
- Capture a screenshot image of the screen, or just the area "around" the mouse pointer.

The keylogger, then, has captured a series of images showing exactly where you clicked and in what order. In other words, it's captured your virtual keystrokes: your mouse clicks and what you clicked on.

Note that this approach to keylogging bypasses one of the more common so-called security techniques of randomizing the keyboard layout on the screen. You still have to see where to click, and the logger simply logs what you see and where you click, regardless of how the keyboard is laid out.

And that's just one technique any malware could use to capture what you're entering.

Keyloggers as threats

How big a threat is all this?

In my opinion, "normal" keyloggers — those that record only keystrokes — are a fairly common threat, and are one reason why security software, general internet safety, and the use of common sense are important. So yes, they're out there, in the same way that any malware is "out there" trying to get you to install it on your device.

The real question is, how pervasive are the more sophisticated keyloggers, which capture more than keyboard keystrokes using other techniques to effectively achieve the same result?

It's hard to say. But again, keyloggers are "just" malware. **If they're on your machine at all, you have a problem, and that problem may not be limited to logging what you type**. Like any malware, you might not even realize it's there until it's too late. As a result, focusing on solutions targeted only at thwarting keyloggers is not only misguided but diverts your attention from a much bigger problem.

If you have a keylogger, you have malware.

Focus on preventing or removing malware of all sorts, and you'll be avoiding or removing keyloggers as a side effect.

Do not rely on a virtual keyboard of any sort as a security measure.

How Do I Make Sure Windows Is Really, Completely Up to Date?

> *"When trying to solve a problem, one of your steps is to "make sure Windows is as up to date as possible." Doesn't Windows do that automatically?*



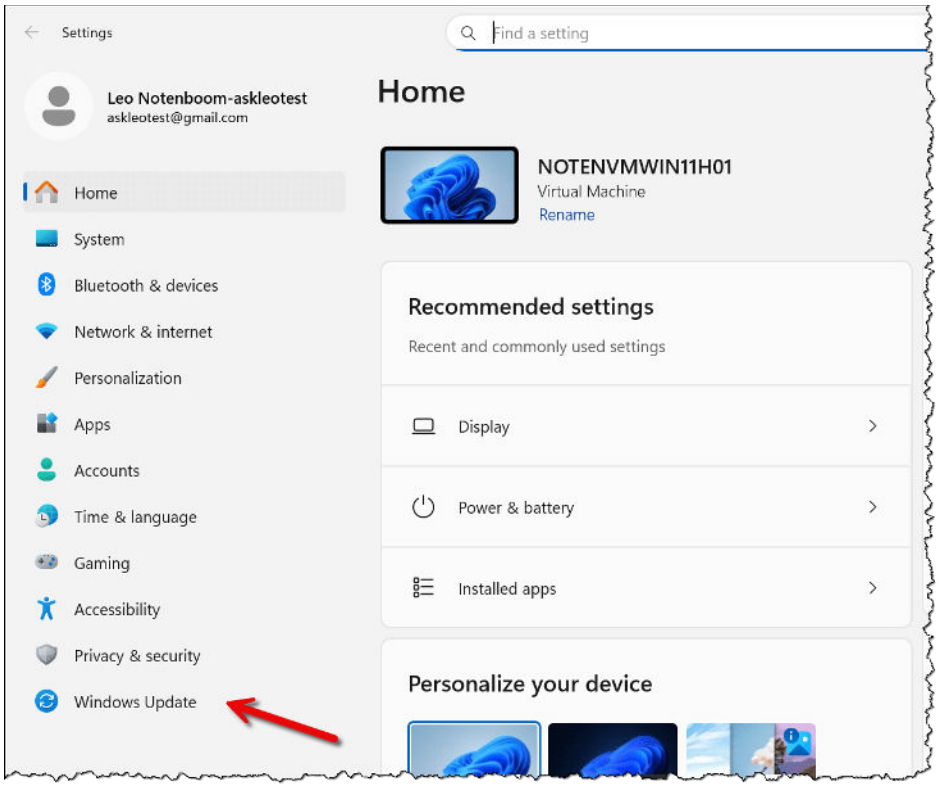
Yes.

And no.

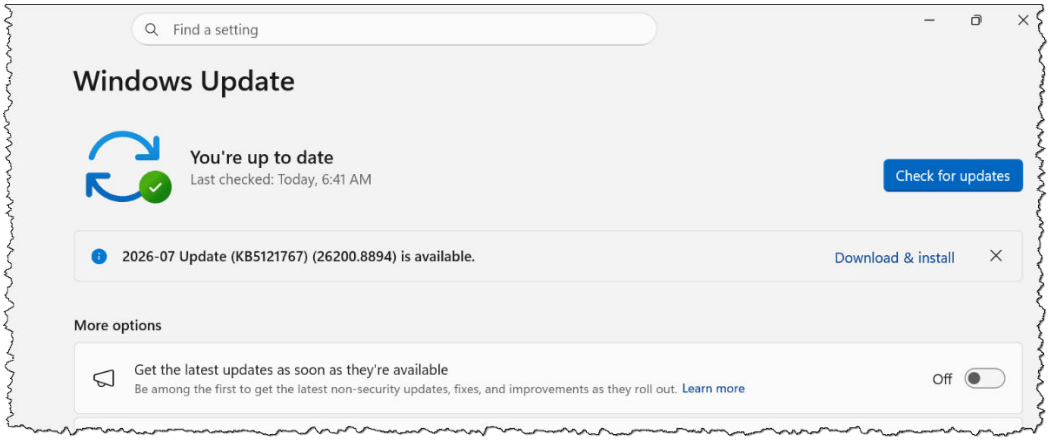
Even with Windows Update turned on and working properly, you might find more updates are available. Let me explain what I mean by "Make sure Windows is as up to date as possible."

Checking for updates

Right-click on the Start button and then on **Settings**. In the Settings app, click on **Windows Update** (or **Update & Security** in Windows 10).



This will display the Windows Update settings page.



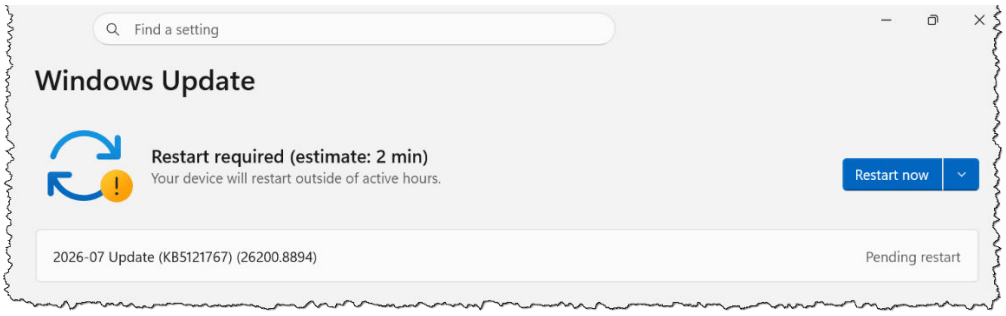
Windows may start checking for updates immediately. Let those downloads and installs complete.

If there are optional updates available (as there are in the example above), click on Download and install to take those updates as well.

The key point here is clear: take all the updates that are offered.

Reboot if needed

After updates are downloaded and installed, you may be told that a restart is required.



Lather, rinse, repeat[99]

Now do the whole thing again.

- Go to the Settings app.
- Click on Windows Update.
- If Windows Update doesn't automatically check for updates, click the Check for updates button to have it check again.
- Install all available updates, rebooting if necessary.

Repeat this process over and over until **Check for updates** indicates you're fully up to date.



Windows is now "as up to date as possible."

What about "Get the latest updates as soon as they're available"?

The option to "Get the latest updates as soon as they're available" isn't part of this discussion. What we're most concerned about is that your system has the latest security and other bug-fix related updates.

However, if you truly want Windows to have all "the latest non-security updates, fixes, and improvements", turning this option on will include even more updates. You'll be even more up to date.

[99] For those not familiar with the reference, these are common usage instructions on bottles of shampoo in the U.S. (https://en.wikipedia.org/wiki/Lather,_rinse,_repeat) Computer programmers will note that it's an infinite loop.

My recommendation is to turn this option on so you'll get not only the latest security and bug-fix updates but any feature updates as well. My belief is that you'll eventually get these updates anyway; this option ensures you get them sooner.

Why Windows Update didn't do all of this automatically

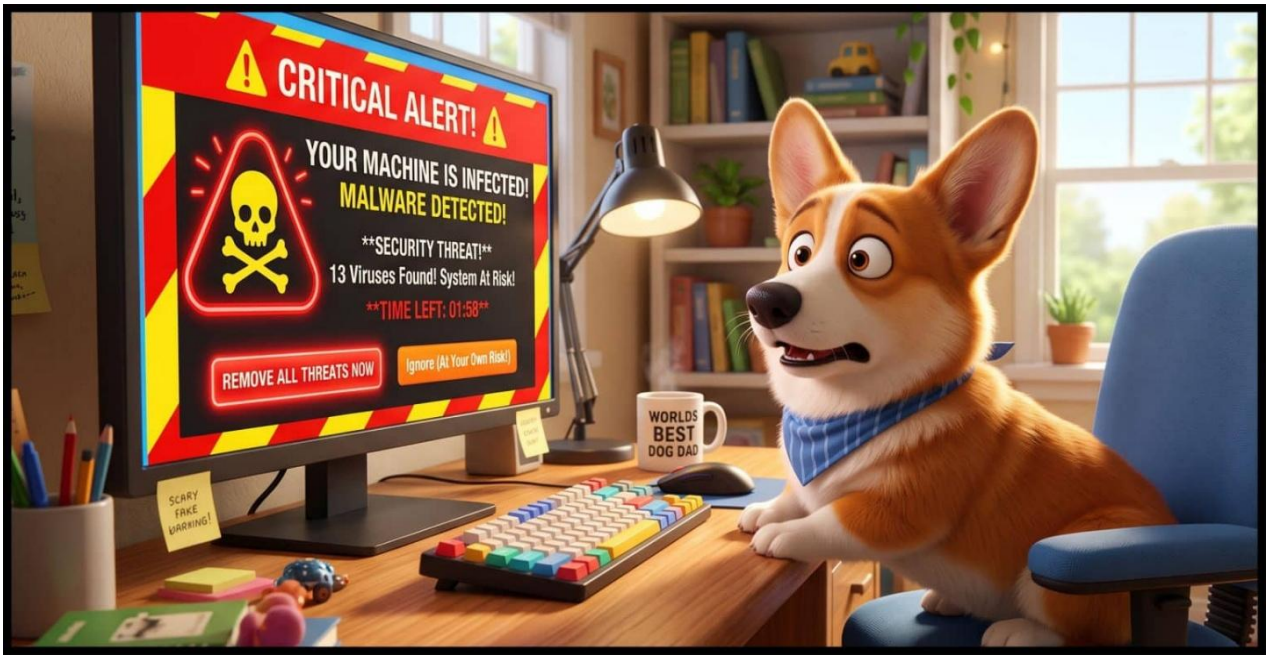
So why might there be updates available that Windows hasn't recognized?

- The update was made available after the last time Windows Update checked. (Updates for Windows Defender are most common.)
- You've set a delay before taking updates in the Windows Update settings.

The first is most likely, as you'd probably already be aware of the second.

I Got a Pop-Up Virus Warning. Is My Computer Infected?

> *“I’ve recently started getting a new warning message when I visit some sites. It says that my computer is tracking all the adult sites I’ve visited and that this will affect me in various ways. It recommends that I install a drive-cleaning program to remove these tracks. Does this mean that my computer was infected by a virus, trojan, or some kind of tracking software? Have I been hacked by someone? And do you recommend that I install the drive-cleaning software? Is it safe?*



Do not install that software.

If you get a message that says you are infected and recommends a specific product to fix it, the answer is simple: *don’t do it*.

You may need to do a few other things, but following some random pop-up message’s instructions to download a specific product isn’t one of them.

The clue: it’s in your browser

Some forms of malware attempt to look like legitimate pop-up messages from Windows or the applications you have on your computer.

But they’re not.

One of the easiest ways to determine this is to close your browser. If the message goes away when you close your browser, then the message was *presented by a webpage, not your computer*. A webpage has no way to know if your computer is infected.

It's extremely unlikely that you've been hacked.

It's just trying to fool you.

It's a trap.

The scam

It's not technically malware — at least, it's not malware on your machine. Yet.

Several scams operate as follows.

- **They present a scary pop-up message** that your computer is infected with malware, has vulnerabilities, or that something else is wrong.
- **They tell you to download a free program** to resolve the problem.
- **The download, when run, presents more scary alerts** about how compromised your machine is. And/or, the download, when run, installs malware on your machine.
- **You're then encouraged to purchase** the "full" version to clean it all up.
- The paid version may or may not actually do anything bad… except take your money.

Some downloads include a phone number to call. The number, of course, puts you in direct contact with the scammer. They have you install malicious software, often including remote access tools, so they can do even more damage when you're not looking.

The question is, where does that initial message come from?

The website you just visited.

Some websites present these misleading messages as a form of advertising. Others show them because the website's been hacked.

The point is to scare you into downloading and running a specific program to resolve what may or may not be an issue. In some cases, the point is to scare you into downloading and installing malware.

What should you do?

If you get a warning that includes a recommendation to download a specific product to resolve the problem, don't.

If you get one of these warnings when you visit a specific website, maybe don't go to that website anymore, as it's probably been hacked.

Instead, learn to keep yourself safe.[100] That means having anti-malware tools and keeping them up to date. Keeping yourself safe means that you can confidently ignore any fear-mongering pop-up messages.

If you get a message indicating a problem and it does not recommend a specific solution, then maybe pay attention. It might be from Windows or from your anti-malware tools. Learn to recognize messages that come from those sources.

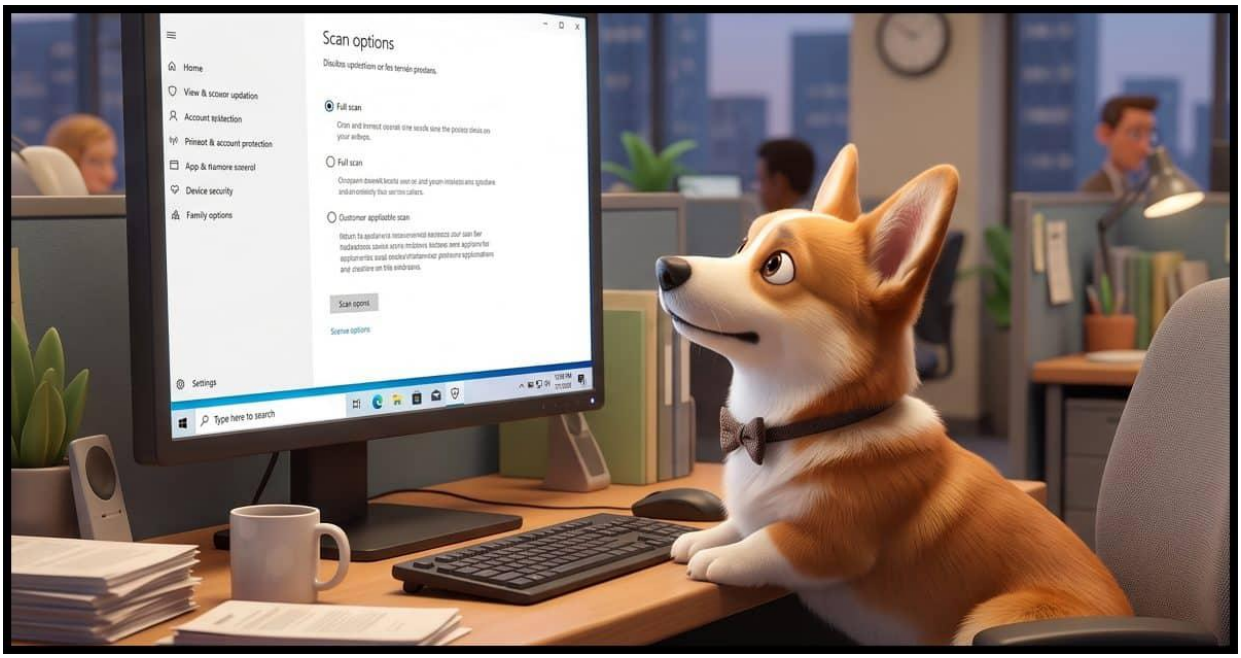
If you believe there's a problem, address the problem with the tools *you* choose.

If you get a message, with or without a specific recommendation, update and run your anti-malware software right then and there. If there's a problem, that should take care of it — again, using tools you selected.

As long as you're staying safe, you can typically ignore the other messages that try to play on your fears.

[100] https://askleo.com/2374

How Do I Run a Full Scan Using Windows Defender?



When we are faced with the hint, suspicion, or removal of malware, one of the more common recommendations is to run a full, up-to-date scan with your security software.

I'll walk you through the process of doing that with Windows Security (also known as Windows Defender or Microsoft Defender).

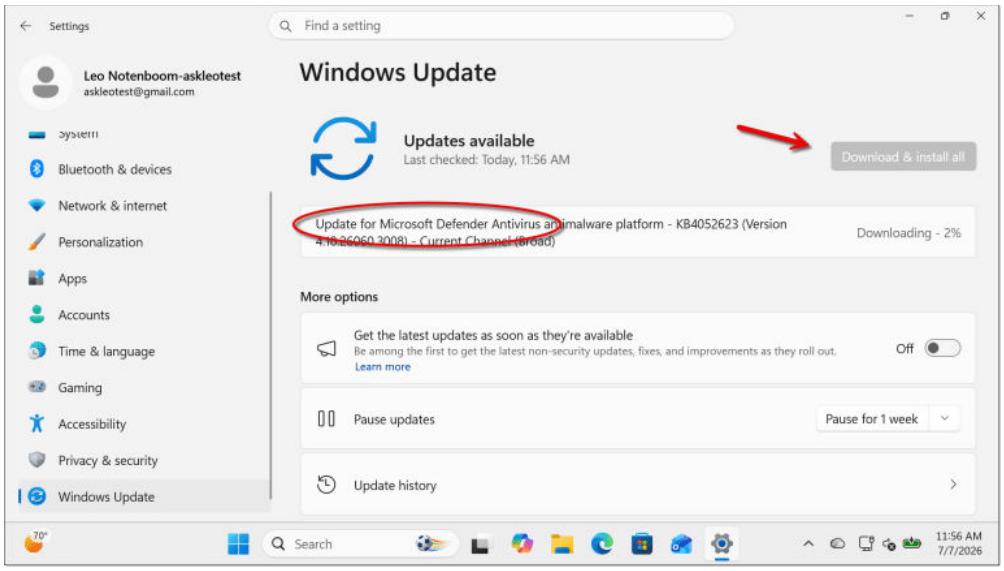
First: Update

Before running the scan, make sure your security software is as up to date as possible. That means running Windows Update.

In Settings, go to **Windows Update** and click on **Check for updates**.

Even if Windows tells you the machine is up to date, click on **Check for updates** anyway. You may discover an update for Microsoft Defender.[101]

[101] My theory is that it's updated up to several times a day.



This ensures you have the latest and greatest information and tools to catch the latest malware.

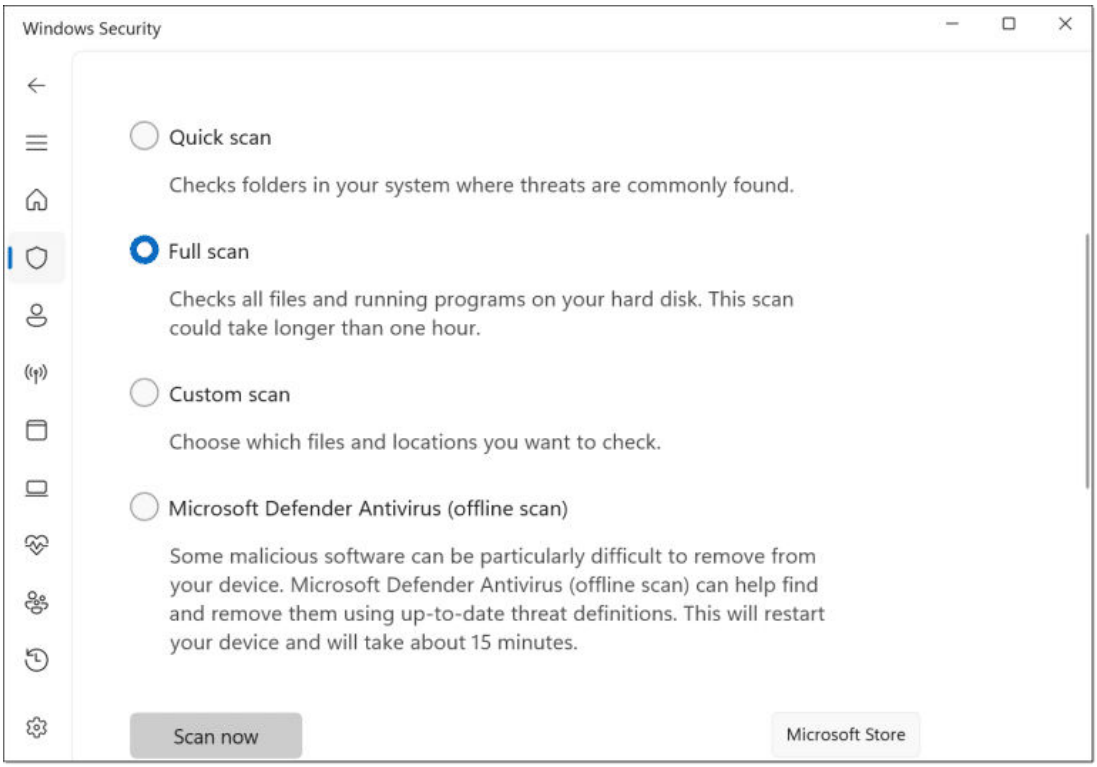
Next, scan with Windows Security

Click on **Windows Security** in the left-hand column (Windows 10), or **Privacy and Security** (Windows 11). In the resulting Settings page, click on **Windows Security**.

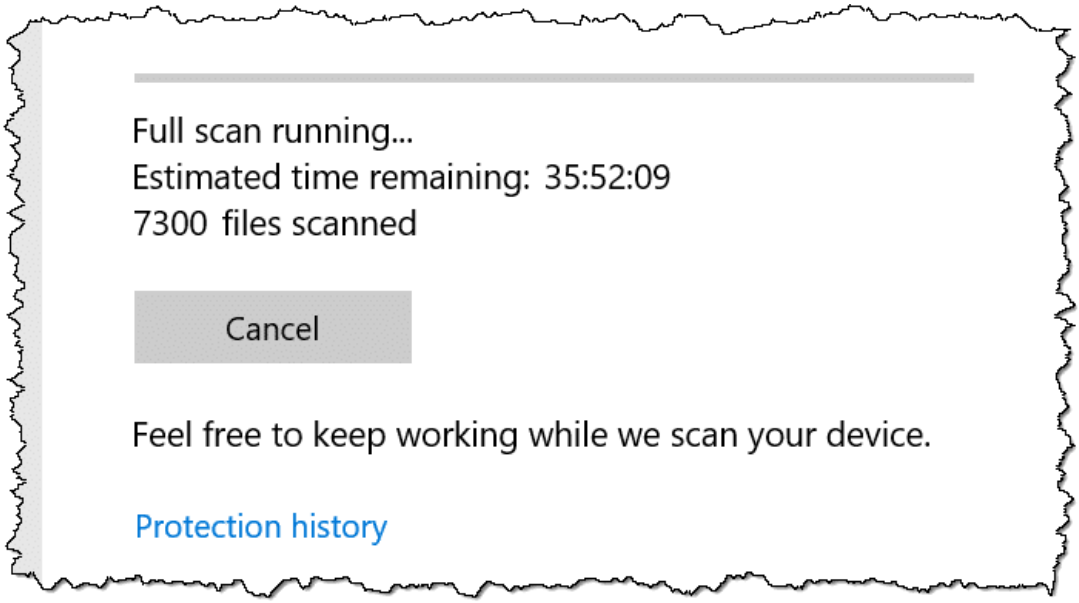
Click on **Virus & threat protection**.



Click on **Scan options** (the link is just below the "Quick Scan" button).



Click on **Full scan** and then **Scan now** to begin the scan.



As noted in the various messages along the way, a full scan can take a very long time. You can continue to use your computer while it scans, though you may find performance is decreased.

A full scan is no guarantee

Running a full scan — even an up-to-date scan with the latest information about the latest threats — is no guarantee that all malware will be discovered and dealt with. This is true for every anti-malware tool. Not all tools catch all malware.[102]

You can never let down your guard.

That being said, though, running up-to-date scans is something you can do to significantly stack the odds in your favor, especially after other forms of malware removal or if you just suspect malicious software on your computer.

Try this

Run a full scan sometime when you don't need it. You'll get a sense for what to expect and what it looks like on an uninfected machine.

Don't be surprised, however, if you do encounter threats, and make sure to quarantine them.

Then, next time you have or suspect malware, you'll have this tool in your arsenal, ready to help you stay safe.

[102] https://askleo.com/4728

Part 4: Protect Your Laptop

How Do I Use an Open Wi-Fi Hotspot Safely?

> *"I've returned to the same coffee shop where I was a few months ago when I noticed that my email had been hijacked/hacked. This time, I'm using my phone, but the last time, when I noticed the hack, I was using my computer and doing email over an open-internet, free Wi-Fi network.*
>
> *Do you think that could be the source of the problem or just a coincidence? I'm still afraid to email from here.*



As we can't diagnose the past, let's look ahead instead.

It can be absolutely safe to send and receive email, or even other tasks, from a coffee shop or other location that provides unsecured or "open" Wi-Fi. In fact, I do it all the time.

But you do have to follow some *very* important practices to ensure your safety.

The open Wi-Fi problem

The problem with open Wi-Fi hotspots is that the wireless radio connection between your computer and the wireless access point nearby is not encrypted. That means any data you don't actively encrypt is transmitted in the clear, and *anyone within range can eavesdrop* and see it. Encryption prevents that.

Important: Know whether your connection is encrypted or not. If you connect to a hotspot and the operating system on your computer requires a password for it to work — say with a password provided by the barista or hotel clerk — that's not an open Wi-Fi hotspot, and you may be OK.

When you're required to provide a password before you can connect, the Wi-Fi access point is using some form of encrypted connection.

On the other hand, if you can connect without a password and your browser immediately takes you to a webpage that says, "Enter a password" (as in a hotel) or "Check to accept our terms" (as in many other open hotspots), *it is not encrypted, and it is not secure*. It is an open Wi-Fi hotspot.

Turn on the firewall

Fortunately, firewalls are "on" by default in most operating systems.

However, when you're at home, you may use your router as your firewall and keep any software firewall on your computer disabled. That works well, as the router stops network-based attacks before they ever reach your computer… while you're at home.

But when you're on an open Wi-Fi hotspot or connected directly to the internet via other means, that software firewall is *critical*.

Make *sure* your firewall is enabled before connecting to an open Wi-Fi hotspot.[103] Various network-based threats could be present on an untrusted connection, and it's the firewall's job to protect you from that.

Secure your desktop email program

If you use a desktop email program such as Outlook, Windows Live Mail, Thunderbird, or others, you *must* make certain it is configured to use SSL/secure connections for sending and downloading email.

Typically, that means that when you configure each email account in your email program, you need to:

- Configure your POP3 or IMAP server to access your email using SSL, TLS, or SSL/TLS security options, and usually a different port number.
- Configure your SMTP server to send email using SSL, TLS, or SSL/TLS security options, and usually a different port number.

How you configure these settings depends on the email program you use. The specific settings depend on the email service.

Once configured with the proper settings, you can feel secure downloading and sending mail using an open Wi-Fi hotspot.

Secure your web-based email

If you use a web-based email service like Gmail, Outlook.com, Yahoo, or others via your browser, you *must* make sure it uses an HTTPS connection. Fortunately, most major email services now rely on HTTPS.

[103] https://askleo.com/2689

In years past, accessing email using a plain HTTP connection might well have been the source of many open Wi-Fi-related hacks: usernames and passwords are visible to any hackers in range who cared to look. HTTPS prevents that.

Secure all your other online accounts

All web-based (aka "cloud") services that require you to log in with a username and password should either be used only with HTTPS from start to finish or be avoided completely while you're using an open Wi-Fi hotspot.

With more and more services provided online, this is getting to be a larger problem. Fortunately, most are aware of the issue and are using HTTPS properly.

Using the cloud is a great way to manage your digital life from wherever you may be, but security remains key. Using HTTPS is critical when you're out and about.

Use a VPN

This one is for the road warriors: the folks who are always online while they travel, often hopping from coffee shop to coffee shop in search of an internet connection as they go.

A VPN, or Virtual Private Network, is a service that sets up a securely encrypted tunnel to the internet and routes *all* of your internet traffic through it. HTTPS or not, SSL/secure email configuration or not, all of your traffic is securely tunneled, and no one sharing that open Wi-Fi hotspot can see a thing.

This service typically involves a recurring fee.[104] As I said, they're great for road warriors, but probably overkill for the rest of us as long as we follow the other security steps described above.

A VPN also has the side effect of protecting you not only from the hacker in the corner but from the coffee shop IT guy or whoever is providing the internet connection.[105]

Use different passwords

Finally, it's important to keep your account passwords different from each other[106] and, of course, secure.[107]

That way, should one account be compromised by some stroke of misfortune, the hackers won't automatically gain access to your other accounts.

Remember, even when you use an open Wi-Fi hotspot properly, a hacker can still see the sites you're visiting, even though they cannot see data you exchange with it. That means they'll know exactly what sites to target next.

---

[104] In fact, I avoid free VPNs, as they run a higher risk of tracking or exposing your information in other ways.
[105] https://askleo.com/3004
[106] https://askleo.com/11788
[107] https://askleo.com/4844

Consider not using free Wi-Fi at all

As I said, it can be safe to use open Wi-Fi, but it's easy for it to become unsafe.

One common solution is to use your phone instead.

While it is possible, a mobile/cellular network connection is *significantly* less likely to be hacked. In fact, I use this solution heavily when I travel.

Most mobile carriers offer one or more of the following options.

- **Use your mobile device**. Many phones or other mobile devices, such as iPhones, iPads, Android-based phones, and others, are quite capable email and web-surfing devices, and typically do so via the mobile network. (Some also use Wi-Fi, so to avoid the security issues we're discussing, be certain you're using the mobile broadband connection.)
- **Tether your phone**. Tethering means you connect your phone to your computer — usually by a USB cable, but in some cases, via a Bluetooth connection — and the phone acts as a modem, providing a mobile broadband internet connection.
- **Use a dedicated mobile modem**. These are USB devices that attach to your computer and provide a mobile broadband internet connection, much like tethering your phone.
- **Use a mobile hotspot**. Instead of tethering, many phones can act as Wi-Fi hotspots themselves. There are also dedicated devices, such as MiFi, that are dedicated hotspots. Either way, the phone connects to the mobile broadband network and provides a Wi-Fi hotspot accessible to one or more devices within range. When used in this manner, these devices are acting as routers and must be configured securely,[108] including a WPA2 password, so as not to be another *open* Wi-Fi hotspot susceptible to hacking.

I have a phone that can act as a hotspot. I find this to be the most flexible option for the way I travel and use my computer. I find this to be the most flexible option for the way I travel and use my computer.

Don't forget physical security

Laptops are convenient because they're portable. And because they're portable, they're also easily stolen.

Unfortunately, it only takes a few seconds for an unattended laptop to disappear. I never leave mine alone. Even if I need to make a quick trip to the restroom, the laptop comes with me. There's just no way of knowing that absolutely everyone around me is trustworthy.

In that same vein, I also prepare in case my laptop does get swiped. Specifically, that means:

- My hard drive is encrypted.
- My sensitive data is stored in folders that are encrypted using Cryptomator. Those folders are not mounted unless I need something.

[108] https://askleo.com/11107

- 1Password, my password management software, is set to require a password re-prompt after a certain amount of inactivity.
- I have two-factor authentication enabled on as many accounts as support it, including 1Password.

Computer theft and recovery is a larger topic that is only slightly related to using open Wi-Fi hotspots. Clearly, though, if you are a frequent user of open hotspots in your community or when you travel, a little attention to theft prevention and recovery is worthwhile.

Security and convenience are always at odds

As you can see, it's easy to get this stuff wrong, since doing it securely takes a little planning and forethought.

But it's important. If you're not doing things securely, that guy in the corner with his laptop open could be watching all your internet traffic on the Wi-Fi connection, including your account username and password as they fly by.

And when that happens, you can get hacked.

Fortunately, with a little knowledge and preparation, it's relatively easy to be safe.

How to Protect Data on a Laptop

> *"How can you set a strong password in a laptop so that data can't be stolen?*



It takes much more than a strong password. In fact, it takes at least a couple of passwords, plus some settings, plus some encryption on top of it all.

Given that laptops are so easily lost and/or stolen, let's walk through the four steps I recommend to protect the valuable data you have stored on them.

1. Lock your UEFI[109]

If your computer's UEFI[110] (also known as BIOS) supports it, configure it to require a password before booting. This prevents strangers from starting your laptop, much less accessing what's on it directly.

Exactly how you do this varies depending on the make and model of your computer. Not all UEFI interfaces are the same, and not all support the same set of features. Check with your computer's manufacturer for specifics. If you're able to set one, *do not* forget the password.[111]

[109] I'll use UEFI to refer to both UEFI and BIOS.
[110] https://askleo.com/glossary/uefi/
[111] https://askleo.com/4777

This will not only prevent someone from accessing what's on the machine but will also prevent them from making changes to the machine. For example, with a BIOS password set, they should not be able to change the boot order and boot from anything other than the settings you've chosen.

While you're at it, turn on Secure Boot[112] if it's not already on. This restricts the computer from booting into untrusted operating systems or installing unauthorized UEFI replacements. Caution: turning Secure Boot on or off may change how your system boots and render the operating system inaccessible. If this happens, simply revert the change and the machine should return to normal. Consider setting Secure Boot prior to your next operating system installation if this happens.

2. Lock your hard disk

This is the single most important step on this list. By "lock your hard disk", I mean use whole-disk encryption. This can take any of several forms:

- Windows BitLocker,[113] if your edition of Windows supports it.[114] Be certain to back up the encryption key when offered.
- VeraCrypt whole-disk encryption.[115] As it is passphrase-based, do not lose or forget the passphrase.
- A hard disk encrypted at the hardware level. This manifests much like a UEFI password: you must specify a passphrase prior to being able to boot from the drive. Once again, do not lose the passphrase.

Encryption is the ultimate protection for your data. Even when all else fails and a hacker or thief makes off with the hard drive from your machine, they still won't be able to access the data on it without knowing the passphrase or encryption key.

Neither will you, should you ever lose the key or forget the passphrase… so don't.

3. Lock your login

You should have a strong password for your computer's login, particularly if you use a Microsoft account. Unlike a local machine account, your Microsoft account is also accessible — and therefore vulnerable — online.

Using additional login methods — like a PIN or facial recognition — is something I discourage for mobile computers with sensitive data. They represent additional places hackers can poke and prod. Guessing your strong password is unlikely, but a short PIN can easily be exposed in other ways. It concerns me that a good photo might squeak by facial recognition tools, so I'd avoid it as well.

Long, strong passwords remain the best protection.

[112] https://go.askleo.com/secureboot
[113] https://askleo.com/17437
[114] BitLocker is not available in Home editions of Windows.
[115] https://askleo.com/27408

While you're at it, make sure there are no additional login accounts enabled on your machine. If the normally hidden account called "administrator" is enabled, disable it (assuming your normal login account is administrator-capable).[116]

4. Lock your laptop



When traveling, a friend of mine never leaves his laptop alone without physically locking it to something else in the room, like a table.

Most laptops have a slot for what's called a Kensington lock.[117] It's a standard design to securely tether mobile devices in place.

Even with all the precautions already taken — UEFI passwords, encrypted disks, and secured accounts — it's still important to make sure the laptop itself can't be stolen.

As I've said many times, if it's not physically secure, it's not secure.

A story from the trenches

Much of the above came to mind when a friend handed me a laptop and asked me to see if I could make it usable again. It had been part of a corporate network that they no longer had access to, so they could not sign in. They just wanted to be able to use the machine for themselves and didn't really care about what was on it; any photos could be restored from copies on their mobile phone.

I discovered the machine's hard disk had been encrypted using BitLocker, and of course we did not have access to the corporate encryption key. The result? The data on the machine was completely inaccessible. I was able to back up the hard disk, but the encryption remains in place. I'm not sure the backup will ever be useful, other than to restore the laptop to the state it was in when I got it.

On the other hand, without needing a UEFI password, I was easily able to change the boot order and boot from a Windows 10 setup drive. This allowed me to install Windows 10 from scratch and erase everything on the drive, encrypted or not.

I hate to harp on it, but…

Much of what I've described above relies on an encryption key, passphrase, or strong password.

Do not lose them. If you do, you will be the one locked out, and everything on your machine may be rendered inaccessible. That's the whole point of this type of security.

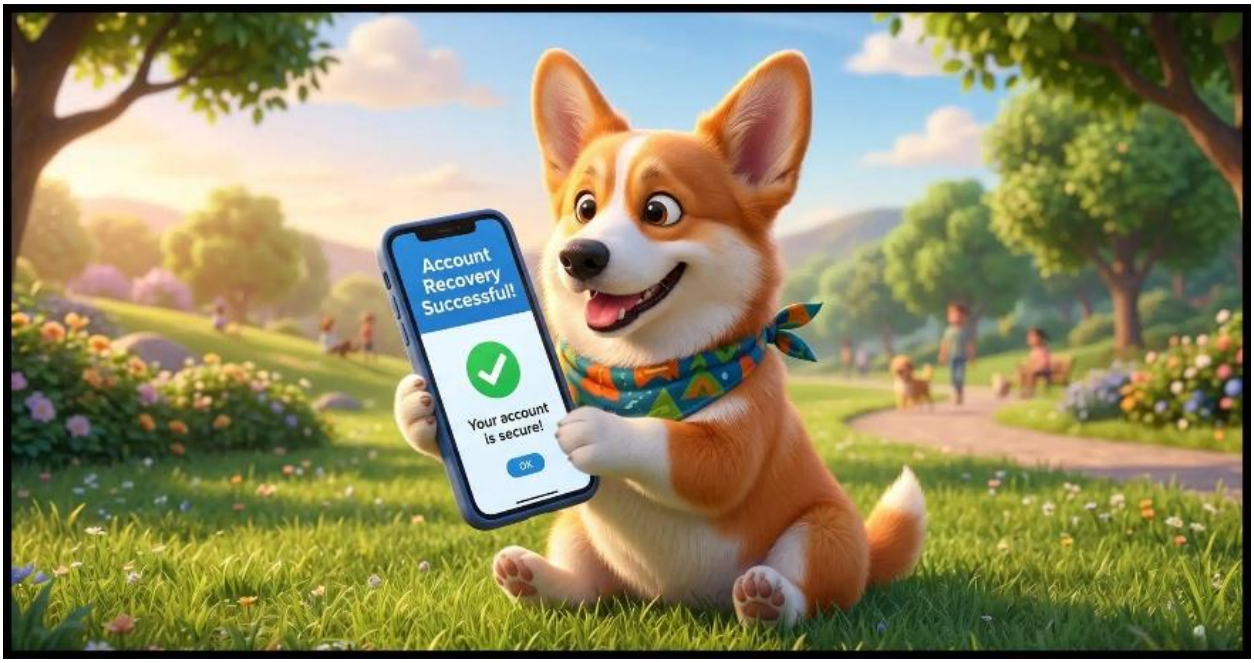
There are no back doors. I mention this again because of the fairly constant stream of questions from folks wanting to get into accounts or devices for which they've lost their passwords, passphrases, or encryption keys.

---

[116] https://askleo.com/4757
[117] https://go.askleo.com/kensington

Part 5: Protect Your Online World

Please Set Up and Maintain Account Recovery Information



It might be as important as backing up.[118] It's certainly close.

I hear at least daily from people desperately trying to regain access to their accounts because they can't sign in for some reason. The number of people who will never regain access[119] would surprise you more. I see it at least daily.

It doesn't have to be that way!

Recovery information has one purpose

You know you are who you say you are.

But if you lose your password, it doesn't look like you are who you say you are. If you were the rightful account holder, after all, you would know the password.

I know, I know! That's not the case if someone has hacked you or you lost that little green notebook with all your passwords scrawled in it. But the service has no way of knowing that. Your username/password combo[120] is how you prove to them you are who you are.

[118] https://askleo.com/30103
[119] https://askleo.com/15584
[120] Plus your second factor, if you have that configured.

What most services do realize, though, is that people are people. Sometimes we forget our password. Sometimes our accounts are hacked.

Recovery information is how you prove you are who you say you are and should be given access to the account.

You must set up recovery information before you need it

The reason recovery information works is because you set it up *while you have access to your account*. It's information you add to the account in case of future problems.

Hopefully, you'll never need to use it. But you must set it up just in case.

If you never set it up, then should your password ever stop working, *you'll have no way to prove you are authorized to access the account.*

You must keep recovery information up to date

Most people facing account loss due to failed recovery attempts did set up recovery information when they set up their accounts. That's good, but it's not enough.

Many of these accounts are years old (and that's one reason you care so much about them). The recovery information you configured back then can fall out of date. Maybe you no longer have that recovery phone number or email account.

Out-of-date recovery information is just as bad as not having it at all. It might even be worse if it gives you a false sense of security.

You must keep it up to date. Check it periodically (some services now occasionally prompt you to do this), and/or proactively update it when something changes.

Type of recovery information

There are several different types of recovery information you can set up.

Alternate email addresses. Make sure you still have access to the email account to which the recovery code will be sent. If you do not, recover *that* account or configure a different one.

Mobile phone number. Contrary to what conspiracy-minded folks might believe, this is not used to gather more tracking data on you. (The mobile services already have plenty of that.) Make sure that any mobile number configured in your account is a number at which you can currently receive a text message. If you change numbers, update your recovery information. If you lose your mobile phone, replace it quickly and have your existing phone number ported to the new device. Since text messages are tied to your mobile number, not a specific device, the new phone will still work to receive recovery info.

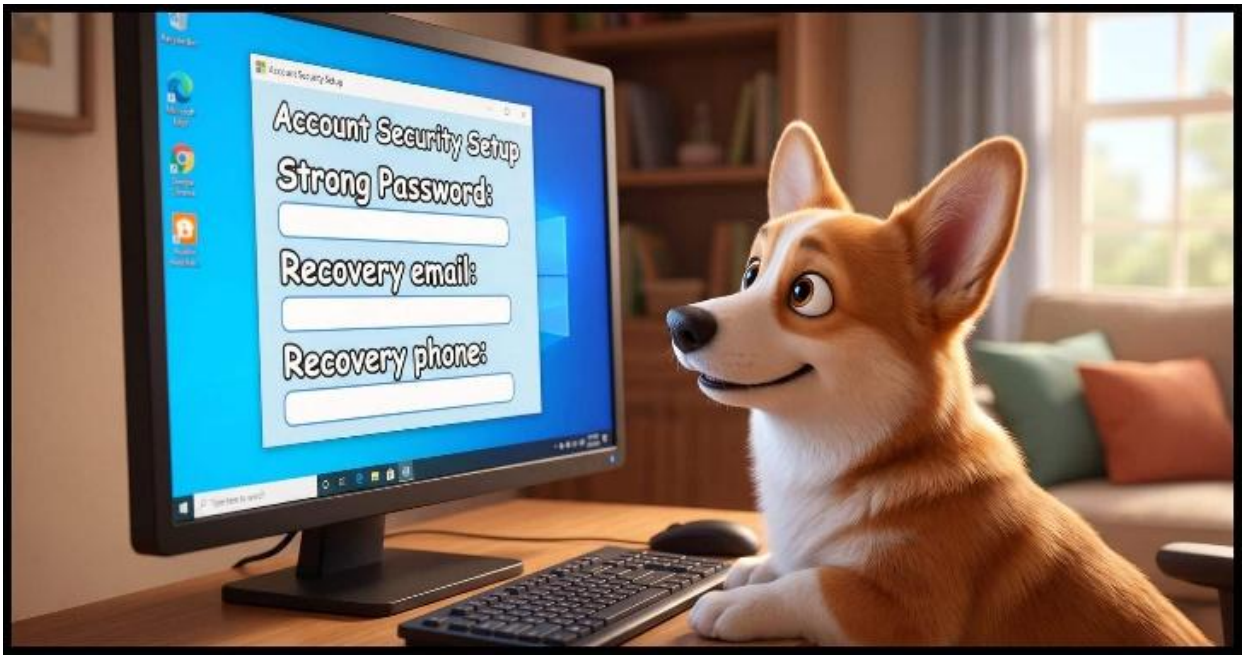
Landline phone number. This is less common, but some services allow you to use a landline and call you with a recorded confirmation code in case of recovery. Like a mobile number, if your landline number ever changes, make sure to change it in your account recovery information.

Recovery codes. Some services let you generate one or more "recovery codes" — random numbers that, in the event of password failure, can be used once to sign in to your account. The issue here is that you must create and save them somewhere secure so they're available when needed (password managers are great for this).

Secret questions. Some services still use them, but they should not. It's been shown that the answers to secret questions are often guessable (or researchable) and significantly less secure. If you have a choice, use an alternative method. If you have no choice, make up nonsense answers to the questions and store your responses somewhere secure (like that password manager).

12 Steps to Keep from Getting Your Account Hacked

> *"My account has been hacked into several times. If I'm able to recover it, it just gets hacked again. Sometimes I can't recover it, and I have to start all over with a new account. What can I do to stop this all from happening?*



I don't get this question a lot, but I really wish I did. What I get instead, repeatedly, is "I've been hacked, please recover my account/password for me!" (Which, for the record, I cannot do, no matter how often or how nicely, or not so nicely, I'm asked.)

The only salvation is prevention, and this applies to email, social media, and pretty much any online account you have.

What can you do to make sure your account doesn't get hacked in the first place?

1: Select a good password

You'd be shocked at how easy many passwords are to guess. Your pet's name, your pet's name spelled backwards, your favorite TV character's catchphrase, your boyfriend or girlfriend's name (or "ilove" followed by that name), and so on.

If you think people can't guess it, **you are wrong**. They can and will.

"iLoveMikey" is a *bad* password. "j77AB#qC@^5FT9Da" is a great password. You can see the problem, though: great passwords are hard to remember.

So compromise.

- Avoid single or pairs of full English words or names unless you make a longer pass*phrase* of at least three (preferably four or more) words.
- Include a mix of uppercase and lowercase letters and numbers.
- Make sure the password is at least 16 characters long.

"Macintosh" is bad. "Mac7T0shB00k" (based on the easy-to-remember "Macintosh Book") might be good. "HondaPrelude" is bad, but "SilbrPre7ood6" (based on "Silver Prelude 6") might be ok.

Bottom line: pick a random-looking password you can remember but *they* would never guess… and assume that they are really great guessers.

For more, see Your 6 Strongest Practical Password Techniques, Ranked.[121]

2: Protect your password

A scenario I see much too often starts with "I thought I could trust my boyfriend/girlfriend/husband/wife/co-worker, so I gave them my password. Then we had an argument."

How much damage can someone do if they're angry with you and they have the password to your account? A lot.

It's simple: Trust no one. *I'm serious about this*. Your friends are your friends until one day they're not. Naturally, there are exceptions, but if there's the least bit of doubt, don't reveal your password. *Especially* if someone is pressuring you to do so.

For more, see The Biggest Risk to Your Privacy.[122]

3: Set and protect your secret answers

It's fallen out of favor as not being particularly secure, but many systems still use a secret question and its answer as the key to account recovery or password reset. The problem is, many people choose secret answers nearly anyone can guess or easily find out.

However, *there's nothing that says your answer has to correspond to the question*. Pick an answer that is unrelated to the question. Perhaps your city of birth should be Crayola, Chardonnay, or WindowsExplorer. Treat secret answers like another password. Make it long, obscure, completely unrelated to the question, and impossible for someone else to guess.

As long as you can remember it when needed, it doesn't matter what it is.

For more, see How to Choose Good Security Questions.[123]

---

[121] https://askleo.com/132876
[122] https://askleo.com/27036
[123] https://askleo.com/4624

4: Set (and maintain!) alternate email address(es)

Many services use one or more alternate email addresses to mail you a password recovery link if you forget yours. You must set this up **before** you need it.

First, *make sure to configure* that option using an email account on a different system. Create and use a Yahoo account for your Outlook.com alternate email, for example.

Second: *don't lose the alternate account*. For many systems, if you can't access that alternate email account, you cannot get your password back, and you will not be able to recover your primary account. Remember to log into that alternate account every so often to keep it from being shut down for inactivity.

I've seen too many people lose their alternate email address or let the account lapse and then find themselves totally out of luck when they really need it to recover their primary account.

For more, see Please Set Up and Maintain Account Recovery Information.[124]

5: Set (and maintain!) mobile or other telephone number(s)

This is similar to an alternate email address, and can be used in place of one if you've configured it beforehand. Once again, you must set this up *before* you need it.[125]

If you can't access your account, the service will text you a recovery code. (If you don't text or have a text-capable phone, some can call you with an automated voice recording of the recovery code.) You then enter the code, proving you have access to the phone number you previously configured as belonging to that account, and regain access.

Keep this number up to date! I regularly hear from people who've lost access to their accounts permanently because the phone number they originally configured[126] is no longer theirs.

Also, keep in mind that this number must be able to reach you where you are, and may even be triggered as an additional security measure if you travel outside of your normal area. If that's not possible, configure some other form of security, such as the alternate email mentioned above, or other techniques offered by your service provider.

For more, see A One Step Way to Lose Your Account Forever.[127]

---

[124] https://askleo.com/149957

[125] I often hear from folks who are concerned that providing a phone number is just another way to track you. I don't buy into that conspiracy theory. Providing a phone number is all about being able to prove you are the rightful account owner should you ever lose access to the account.

[126] https://askleo.com/15264

[127] https://askleo.com/15584

6: Enable two-factor authentication

Two-factor (or *multi-factor*) authentication is the current holy grail when it comes to account security. **With two-factor properly enabled, hackers cannot get into your account *even if they know the password***.

The second factor that proves you are who you say you are is typically either:

- A mobile app that provides a random number on demand that you must provide when you log in
- A text message sent to a phone number you configure when you set up the account, which you then also enter at login

Once logged in, you can disable this requirement on machines you use frequently. Hackers are not able to provide the second factor, so they can't get in.

For more, see Two-Factor Authentication Keeps the Hackers Out.[128]

7: Other provider-specific techniques

Some providers have additional recovery techniques. For example, you can create a recovery code for your Microsoft account[129] that you save somewhere safe and use to recover your account.

Look for options like these or others within the services you use regularly.

And remember, you must set them up *before* you need them.

For more, see Recover Your Microsoft Account Later by Setting Up a Recovery Code NOW.[130]

8: Use a different password on every site

I've written about this extensively: it's important to *use different passwords* on each of your important sites.

If a hacker manages to discover your password on one account, they will go try your username and password, or email and password, on a multitude of other services. If you used the same password on another service they happen to try, that account will quickly be hacked as well.

Password managers like 1Password, RoboForm, and others are excellent ways to maintain multiple, complex passwords for multiple sites without needing to remember them yourself.

For more, see Why Is It Important to Have Different Passwords on Different Accounts?[131]

[128] https://askleo.com/16401
[129] https://askleo.com/16142
[130] https://askleo.com/16142
[131] https://askleo.com/4931

9: Use a password manager

I realize that "hard to guess" is at odds with "easy to remember", and both are at odds with not re-using passwords.

That's where password managers (also called password *vaults* or *safes*) come in.

If you forget your password, forget the answer to your secret question, lose access to your alternate email account, or somehow lose the ability to use any of the password recovery mechanisms provided by the service, well, to put it bluntly, you are SOL: severely out of luck.

Don't forget your own password. Don't forget the answer to your own secret question(s). If you must write your information down, keep it in a secure place. A sticky note on your monitor under your mouse pad is not secure. Your wallet might be secure. A locked cabinet or safe might be secure. A properly encrypted file on your computer might be secure.

But remembering this information securely is exactly what password managers are designed to do for you.

For more, see Are Password Managers Safe?[132]

10: Be skeptical

You should never be asked to email anyone your password. Ever.

You should never be asked to hand over a two-factor code at any time other than when you're signing in via the official sign-in interface.

Common phishing attempts threaten you with account closure unless you respond to the email with information about your account (like your login name and password). Those emails are bogus. Mark them as spam and ignore them. Any email that requires you to respond with any information that includes your password is almost certainly a phishing scam.

Similarly, many phishing scams try to get you to click on a link to do something important relating to your account. Instead of taking you to the service, they take you to a fake page that looks like the service but instead is a page designed to capture your username and password when you try to log in. If you have any doubts, don't click the link in the email. Instead, go to the service in question yourself using your web browser. If there's something important, it'll almost certainly be presented there.

For more, see: Phishing: How to Know it When You See It.[133]

11: Remember that free services have little to no support

The vast majority of the account hacks I hear of — the hacks where people are ultimately unable to recover their accounts — involve free services with little to no support.

[132] https://askleo.com/5555
[133] https://askleo.com/16491

There may be a knowledge base or a peer-to-peer support forum, but there is rarely someone to email and almost never someone to call.

You are responsible for your own account security.

It's often true, and certainly safest to assume, that no one will help you should something go wrong. That means it's up to you to take the preventative measures I've outlined and keep your information up to date as things change.

For more, see Are Free Email Services Worth It?[134]

12: Learn from your mistakes

Finally, if you realize that:

- The answers to your secret questions are obvious, or
- You no longer have access to your alternate email address (or never set one up), or
- You no longer have access to your old mobile number (or never set one up), or
- Your passwords are short and lame, and you use the same one everywhere…

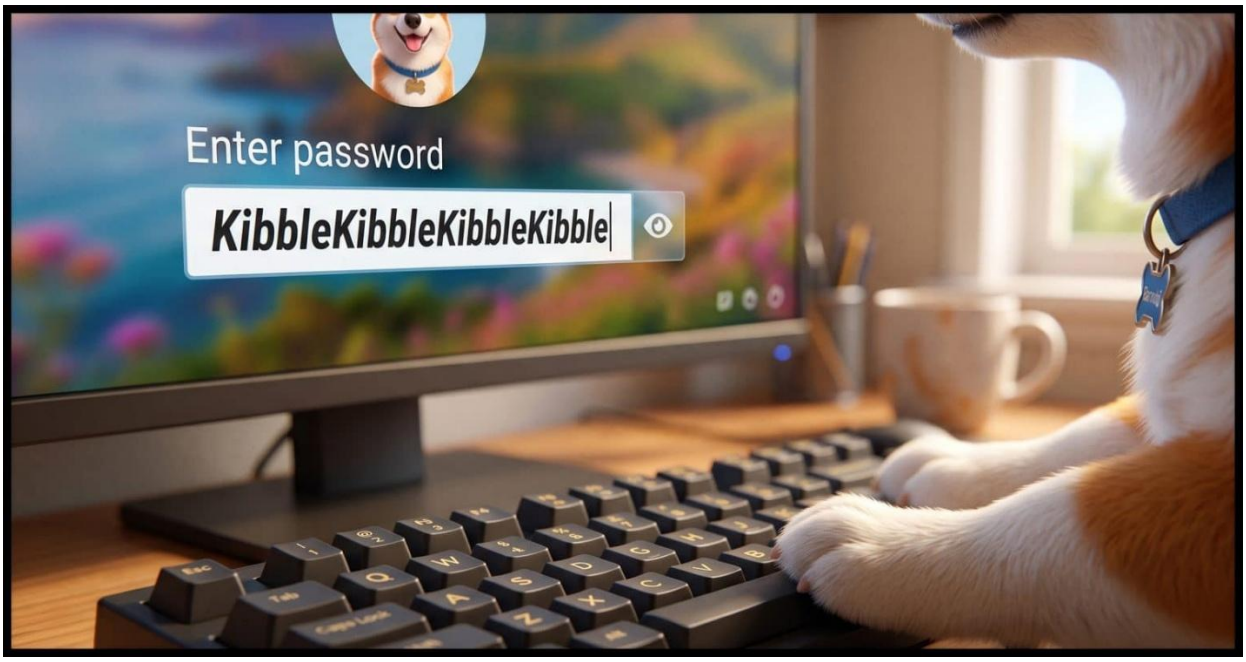
Fix it *now*! Before it's too late.

Trust me: if you get hacked and it's for one of those reasons, or you lose access to your hacked account because you didn't bother to prepare, you'll kick yourself.

And you may very well lose access to that account and all its data forever.

[134] https://askleo.com/2217

How Long Should a Password Be?



For a long time, the common thinking was that the best, most practical passwords consisted of a random combination of upper- and lowercase letters, numbers, and a special character or two. If so composed, the password length needed to be only eight characters.

Randomness remains important, but as it turns out, size matters more. Much more.

And eight characters aren't enough these days. It's not even close.

Large-scale account hacks

When you hear about lots of accounts being stolen by a hacker from a service provider, you're naturally concerned that the hacker might now have access to your account username and password. If the service was storing your *actual* password, that could indeed be the case. (If a service is storing your *actual* password,[135] they don't understand security or they have made some horrifically bad decisions.)

In fact, most services store[136] an encrypted (technically, a "hashed") form of your password. For example, if my password were "password" (and that's a very poor password, of course), then a service might store

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

[135] If they can respond to an "I forgot my password" request with your *actual, current* password, then they have stored your password. This is bad. Best practice is to reset it to something new, either via a reset link, or by emailing a new password to you *exactly once*, after which the service no longer has it.
[136] https://askleo.com/136163

as the hash value that corresponds to that password.[137]

That means that hackers do *not* get a list of usernames and passwords. What they get is a list of usernames and password *hashes*.

And what's great about hashes is that you can calculate a hash from a password, but *you cannot calculate the password from the hash*.

As a result, one would think that if a password is hashed, it's pretty unhackable, right?

Sadly, not so much.

Dictionary attacks

The most common type of password attack is simply a high-speed guessing game. This doesn't work on a log-in page;[138] they're slow and deny further access after too many failed attempts. But this technique works wonderfully if the hacker has the entire database of account and password hashes sitting on their computer.

These attacks start with exhaustive lists of possible passwords, including:

- Common, simple passwords.
- Common combinations of words.
- Common "obfuscations" of words (instead of "password", maybe "PaSsWoRd", "p4ssw0rd", and so on).
- Lists of all the variations people think will hide their passwords.
- Lists of previously discovered passwords. This might be the most successful because people so routinely reuse passwords across multiple sites.

They calculate the hash of each guess, and if it matches what was found in the database of account information they stole, they've figured out the password for that account. It's easy for hackers to make an amazing number of guesses — millions and millions of guesses — in a short amount of time.

That's why you're not using a short password or common obfuscations... right?

That's why *a password created from a totally random combination of characters is best*. It forces hackers to move on to a true brute force attack of every possible combination to gain access.

Brute force attacks

Computers are fast. In fact, the computer on your desk is so fast that its ability to do simple operations is measured in terms of *billions* of operations per second.

[137] For the curious, I'm using an un-salted sha256 as the hashing function here. That's technically better than md5 or sha1 that's commonly used.
[138] https://askleo.com/14547

Creating a password hash is not a simple operation on purpose. However, it's still something that can be done very quickly on most computers today. Spread the work over many machines — perhaps a botnet — and the amount of processing power that can be thrown at password-cracking is amazing.

The net impact is that it's now feasible to calculate the encrypted hash values for *all possible eight-character passwords* comprised of upper- and lowercase alphabetic characters and digits.

Seventy-two possible characters (26 lowercase, 26 uppercase, 10 digits, 10 different special characters) in each of the eight positions equals 72^8 or 722,204,136,308,736, or over 722 trillion combinations.

This seems like a lot until you realize that an offline attack (which is easily performed once you've stolen a database of usernames and encrypted passwords) can be completed in a few hours. (This assumes technology that can "guess" something like 10 billion passwords per second, which is quite possible.)

It doesn't matter what it is; *if your password is eight characters long, the hackers now have it*, even if it was well hashed by the service they stole it from.

Why 12 is better and 16 is better still

As we've seen, eight-character passwords give you over 722 trillion combinations, which can be guessed in an offline brute-force attack in hours.

Sixteen characters give you over 521 octillion (72^16 = 521,578,814,501,447,328,359,509,917,696). The offline brute-force guessing time in this case would be measured in centuries.

Twenty characters? That's 14,016,833,949,999,999,673,980,362,756,575,985,664 (72^20) combinations. Apparently, that's 14 undecillion.[139]

That's why 20 is better than 16, and both are better than eight (or my previous recommendation of 12).

What about special characters?

I usually leave out special characters from my passwords unless the system I'm using that password on requires them.

Here's the deal: instead of 72 raised to the power of the password length, it's 62 (upper and lowercase letters plus digits). Let's run those numbers:

- 16-character random password: 62^16 or 47,672,401,706,823,533,450,263,330,816 - 47 octillion combinations.

[139] I'm relying on Claude here for the names.

- 20-character random password: 62^20 or 704,423,425,546,998,022,968,330,264,616,370,176: 704 decillion combinations.[140]

So, to begin with, those numbers are fine. However, adding even a single non-special character gets you more additional combinations than using special characters would.

- 16-character random password with special characters: 72^16 or 521,578,814,501,447,328,359,509,917,696.
- 17-character random password with no special characters: 62^17 or 2,955,688,906,000,000,004,464,446,537,728, or five times more possibilities.

Yes, using special characters makes your password better, but *significantly better yet is to add one more character*.

Or two. Or six.

Long passwords are good; passphrases are better

What's the difference? In general:

- A password is a random string of characters.
- A passphrase is a longer string of words.

Passphrases are easier to remember, so it's easier to make long ones — and as we saw, *password length is the single easiest way to increase the security of a password*.

"gZdKJ4nkZDk2dTaahN79" is a nice, secure 20-character password that's difficult to remember. In fact, about the only way to use this is with a password manager that remembers it for you.

On the other hand, "Its fleece was white as you know nothing John Snow", at 50 characters, is wonderfully long, secure, and most of all, memorable. Much like the now-canonical example of "Correct Horse Battery Staple" (29 characters), you might even have a difficult time forgetting it.[141]

The biggest problem with passphrases? Many services that use passwords don't allow spaces or such lengthy passwords.

What about quantum computing?

Of late, quantum computing has entered the discussion. The concern is that its capabilities are supposed to be such that no password is safe.

That's not quite true.

Two things keep me from worrying about it.

---

[140] For the curious, that's 704 decillion, 423 nonillion, 425 octillion, 546 septillion, 998 sextillion, 022 quintillion, 968 quadrillion, 330 trillion, 264 billion, 616 million, 370 thousand, 176.

[141] Particularly if you're a Game of Thrones fan. And yes, I know that John Snow is actually Jon Snow. That's another level of handy yet easy-to-remember obfuscation.

First, while we've heard the hype and promise of quantum computing, it's still a long way off. Hackers aren't getting it any time soon, and while corporations and nation-states will probably have initial access, you'd have to be targeted for them to even care about your passwords or the accounts you have. *We're talking many years* before any of this becomes commonplace.

Second, we're already seeing the development of quantum-resistant encryption algorithms. While there's currently no way to tell what's being used to hash your password (a form of encryption), it's likely that some passwords are already being stored in quantum-resistant form.

As I said, it's just not something I'd worry about today.

Shouldn't services fix this and do better?

Absolutely, they should. And many do.

As I've stated above, passwords shouldn't be kept in plain text anywhere by the service at all, yet some do.

There are techniques that make brute-force attacks significantly harder, yet many services use techniques that are *easier* than the example above.

Some services do a great job of keeping your information secure. Some services don't. The problem is that *you really can't be certain which is which*.

To be safe, you have to act like they're all at risk.

The bottom line

The bottom line for staying safe is simply this:

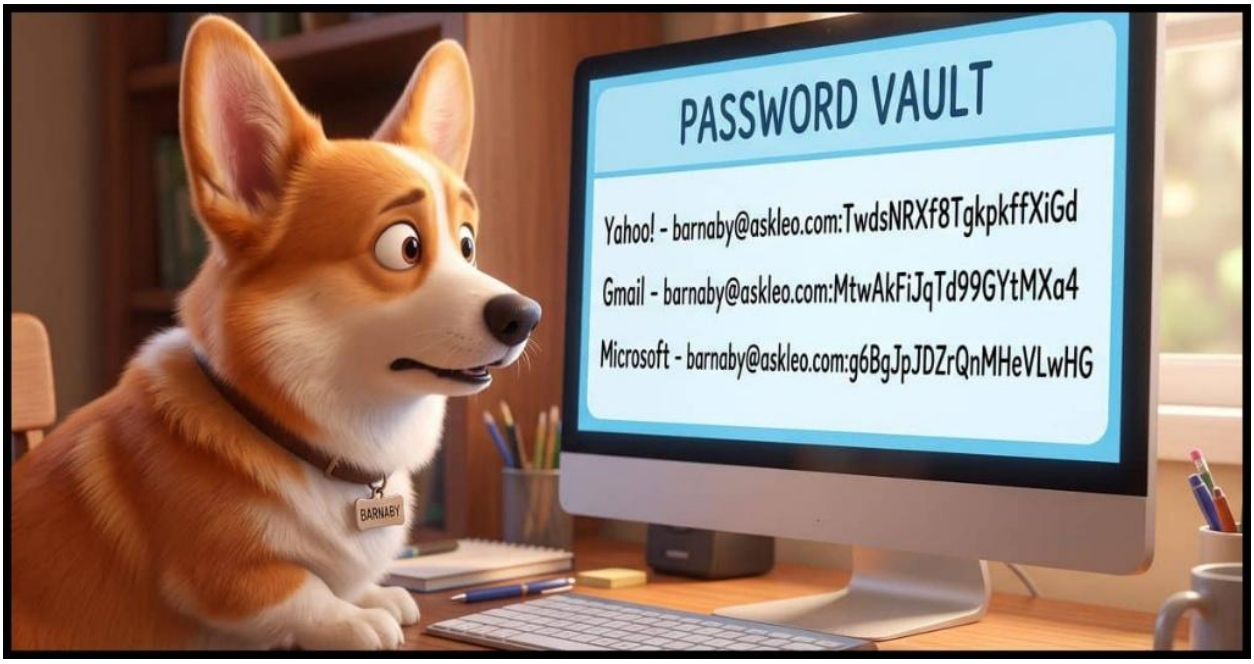
- *Don't trust that the service* you use handle passwords properly. While many do, it's painfully clear that many do not, and you won't know which kind you're dealing with until it's too late.
- *Use longer passwords*: 16 characters at minimum, and 20 if possible.
- *Use even longer passphrases* where they're supported or where information is particularly sensitive.
- *Use a different password* for each different site login you have. That way, a password compromised on one service won't give hackers access to everything else.[142]

Even the best eight-character passwords should no longer be considered secure. Twelve is barely "good enough for now," but you should be using 16 to 20 for the long run.

[142] https://askleo.com/11788

Why Is It So Important to Have Different Passwords on Different Accounts?

> *"Is it safe to have the same password for all of my email accounts? If one has an account in Yahoo! mail, Gmail, Rediff mail, etc., and sets the same password for all of them, will it be easier for a hacker or phisher to find out about it?*



Using different passwords is *much* safer than using one password everywhere. In fact, *it's critical*.

Why?

Because hackers know that most people have more than one account and that most people don't take the trouble to set different passwords.

Admit it, you're lazy

I'll admit it: I'm lazy. When it comes to managing passwords, I'll bet money that most people are.

One password everywhere is *so much easier*. It's easier than even the easiest password management system.

It simplifies our lives not to have to remember passwords or use any special tools to remember for us.

The problem is, it makes hackers' lives easier, too.

Hackers know we're lazy

Hackers know that people find it easier to have one password everywhere.

Hackers know that people generally have more than one account.

Hacking a single account acts as a foot in the door to the others and leads to all sorts of mayhem.

One account leads to more

It's easy to guess that if a person logs in with username X and password Y on a system like Yahoo! mail, it's likely they'll replicate both username X and password Y on other services.

Once they've breached one account, hackers get clues that let them access other accounts.

Account confirmations and notifications are frequently sent via email. What that means is that your hacked email account contains many clues as to what other accounts you have.

If you use the same password everywhere, it's easy sailing for the hacker to quickly try to log in as you at multiple services.

For example, your Facebook login is your email address and a password. Well, if they've hacked your email account and you use the same password everywhere, they now know how to log in as you on Facebook.

The hack might not be your fault

Hacks happen through no fault of your own. You could maintain perfect security and still end up compromised.

Consider all the places you have online accounts. Let's assume that the one with the poorest security gets hacked, and the contents of their entire username/password database are stolen.

You just got hacked, and it wasn't your fault.

However: if you're using one password everywhere, the hackers now know it.

There can't be only one

The bottom line is that using one password everywhere is a risk you shouldn't take.

At a minimum, use unique passwords for your important accounts, like banking and other financially related activities *and email*.

All of your email accounts are important, particularly if they can be used for password recovery on other accounts. All a hacker needs to do is hack your email account and then run over to some other account and request a password reset to be emailed to the email account they now control.

Managing lots of passwords

Whenever I talk about giving each login a different, strong password, people strongly object. "No way am I going to remember all those passwords, especially if you're going to insist that they're complex on top of everything else."

You don't have to.

For example, I don't know my online banking password. Who's going to remember something like yFK86jk8q45B? (And no, that's not it. I said something like that.)

Yet I use my account frequently.

Let your computer do the remembering for you.

I'm a big fan of password management programs, in particular 1Password.[143]

It creates a secure database of your login IDs and passwords and stores them so that only you can get at them with your single, master password. (And yes, *that* password needs to be strong and memorable.)

Password vaults ease the entire process of logging in by filling in the user ID and password for you; you don't even need to know what they are.

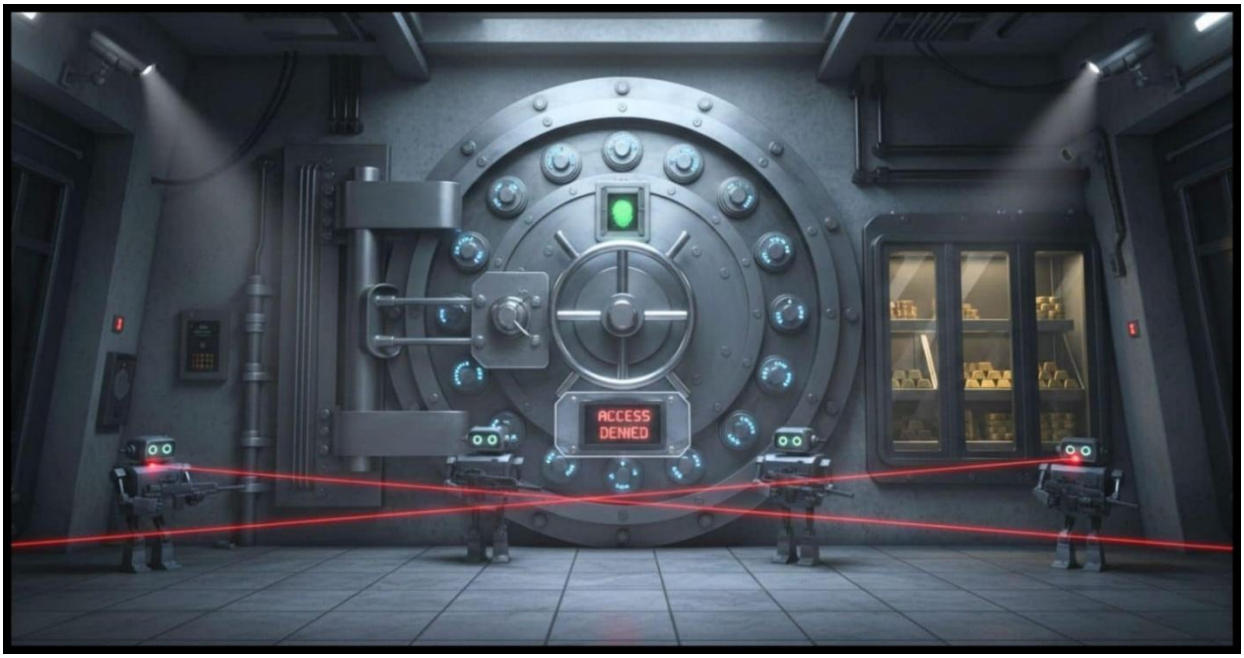
They use strong encryption to keep your password database secure on your machine(s) and support synchronizing or accessing that database across multiple computers and mobile devices.

And they enable you to use different and strong passwords on every single site.

[143] https://askleo.com/152844

Why Password Managers are Safer than the Alternatives

> *"Recently I tried to use RoboForm for an account at a large financial institution, but I couldn't get it to work. In response to my inquiry, this institution said they do not permit log in using credentials that are stored on software because the security of the password could become jeopardized if my computer were hacked, invaded, etc. Is this true? Am I safer not to use tools like RoboForm?*



There are people who believe that using password managers represents a single point of failure. Very technically, they are correct: if someone gains access to your password manager, they have access to everything within it.

Not so technically, I strongly believe they are misguided.

Using a password manager is *significantly* safer than the alternatives.

Security best practices

Password security demands that you:

- Have good, strong passwords (long and complex).
- Keep them nowhere but in your head (memorable).
- Use a different password on every site or service (unique).

Yes, indeed, that would be ideal.

Without using a password manager, it's also completely impractical. A human brain cannot meet all those requirements for the many, many passwords most of us have. At least one, if not two, will be compromised without the aid of a password vault.

Without a password manager

Without a password manager, you'll compromise your security in some way.

- You'll choose a less secure, easy-to-remember password (short and/or not complex).
- You'll use the same password at multiple sites (not unique).
- You'll save the password using technology that is not secure (not memorable).

Any one of those can significantly compromise your security.

With a password manager

Password managers make best practices trivially easy. Using a password manager allows you to:

- Generate and use secure, complex, and appropriately long passwords.
- Never need to type or remember passwords — the password manager remembers them for you.
- Use different passwords on different sites.

These are things that people *don't* do unless they have a tool in place to help them. Password managers are specifically designed to do exactly that securely.

Most password managers add several features that make improved security even more convenient. They can:

- Synchronize your information across multiple computers.
- Be used on mobile devices.
- Automatically fill in not just passwords, but common web forms.
- Securely store other types of information.

And they do all of that with more security than alternatives.

If you're compromised, you're compromised

It is true that if your computer is compromised, all bets are off. Malware *could* gain access to whatever it is you have stored on the computer.

For example, while I'm logged into my password manager, all the information could technically be available to software running on my machine — good software or bad.

That's a serious concern, and not to be taken lightly.

But it's a concern that exists *regardless of whether you use a password manager or not*. All bets are off if a keylogger captures what you enter when you log in to your bank account.

Avoiding a password manager doesn't increase your security one whit.

But are password managers safe?

Yes. Password managers are safer than any practical alternative.

There are no absolutes — that, too, is a practical reality. There is no such thing as absolute security.[144] As I said earlier, if you fall victim to malware, all bets are off, no matter what technique(s) you use.

Password managers are the safest way to keep a record of your online account information, but they are no safer than:

- The master password you use to access the password manager.
- Your own ability to use your computer safely.[145]

The last one scares most people, but my claim is that using password managers is, in fact, one way to use your computer more safely.

What I do

I keep my machine(s) secure by doing the traditional things that you hear over and over:[146] keeping software up-to-date, running up-to-date scans, avoiding malicious websites and downloads, not falling for phishing, and so on.

I use 1Password[147] to manage my passwords and additional security information.

I use Google Authenticator, a form of two-factor authentication, to access my 1Password vault. You can't get in to my 1Password account *even if you know my master password*. To get access to my 1Password vault, you need both my master password *and* my mobile phone.

I have 1Password automatically log out after some amount of time on any device which I'm not 100% certain won't get stolen or accessed without my permission.

I keep my master password secure and complex.[148]

I back up my 1Password vault regularly.

I'm not going to claim it's impossible for anything bad to happen — that'd be a foolish claim. I am, however, very satisfied with the risks and trade-offs, and absolutely convinced that using a password manager keeps me as safe as possible — and safer than not using one at all.

Let's face it: even doing business *offline* has risks and trade-offs.

Use a password manager. Please.

---

[144] https://askleo.com/16029
[145] https://askleo.com/2374
[146] https://askleo.com/2374
[147] https://askleo.com/152844
[148] https://askleo.com/5440

My Email Is Hacked. How Do I Fix It?



It seems like not a day goes by when I don't get a question from someone that boils down to their email account having been hacked.

Someone, somewhere, has gained access to their account and is using it to send spam, access other online accounts, hassle contacts, and more. Sometimes passwords are changed, sometimes not. Sometimes traces are left, sometimes not. Sometimes everything in the account is erased — including contacts and saved email — and sometimes not.

If that's happening to you, your email account has been hacked.

Here's what to do next.

1. Recover your account.
2. Change your password.
3. Verify and/or change your account recovery information.
4. Set up two-factor authentication.
5. Check your out-of-office messages, autoresponders, forwards, and signatures.
6. Check all related accounts for possible compromise.
7. Let your contacts know.
8. Start backing up.

And perhaps above all, learn from the experience so it doesn't happen again.

1. Recover your account

Log in to your account using your email provider's website.

If you can log in successfully, consider yourself extremely lucky and proceed to Step 2 right away.

If you can't log in even though you're sure you're using the right password,[149] the hacker has probably changed your password. The password you know is no longer the correct password.

You must then use the "I forgot my password" or equivalent account recovery options offered by the service.

This usually means the service will send password-reset instructions to an alternate email address you have access to or send a text message to a mobile phone number you set up previously.

If the recovery methods don't work — because the hacker changed everything, because you no longer have access to the old alternate email or phone, or because you never set up the alternate email or phone — you may be out of luck.[150]

If recovery options don't work, your only recourse is to use the customer service phone numbers or email addresses provided by that email service. For free email accounts, there is usually no customer service. Your options are generally limited to self-service recovery forms, knowledge base articles, and official discussion forums, where service representatives may or may not participate. For paid accounts, there are usually additional customer service options that are more likely to help.

Important: *If you cannot recover access, it is now someone else's account*. I can't stress this enough. It is now the hacker's account. Unless you've backed it up, everything in it is gone forever, and you can skip to Step 6. You'll need to set up a new account and start over.

2. Change your password

Once you regain access to your account (or if you never lost it), *immediately* change your password.

As always, make sure it's a good password:[151] easy to remember, difficult to guess, and long. In fact, the longer, the better,[152] but make sure your new password is at least 16 characters, and ideally 20 or more (if the service supports it).

But don't stop there.

3. Change or confirm your recovery information

While a hacker has access to your account, they might leave your password alone so you won't notice the hack for a while.

But whether or not they change your password, *they may change all the recovery information*.

[149] https://askleo.com/15079
[150] https://askleo.com/15584
[151] https://askleo.com/5440
[152] https://askleo.com/4844

The reason is simple: if you change your password, the hacker can follow the "I forgot my password" steps and reset the password out from underneath you using the recovery information they set.

Thus, you need to check all of it — and change much of it — right away.

- Change the answers to your secret questions if your account uses them. They don't have to match the questions (you might say your mother's maiden name is "Microsoft", for example); all that matters is that the answers you give during a future account recovery match the answers you set today, so write them down somewhere secure.
- Check the alternate email address(es) associated with your account and remove any you don't recognize. The hacker could have added their own. Make sure you have alternate email addresses configured and that they are accounts that belong to you and that you can access them. I really can't emphasize that last point enough: the number of accounts that are lost because folks could not access the recovery email address is amazing.
- Check any phone numbers associated with the account.[153] The hacker could have set their own. Remove any you don't recognize. Make sure that if you provide a phone number, it's yours and no one else's, and you have access to it. Again, I can't emphasize the last point enough: the number of accounts that are lost because people could not access the recovery mobile number is scary.

These are the major items, but many services use additional information for account recovery. Take the time now to research that information. If it's something a hacker could change, change it.

Overlooking information used for account recovery allows the hacker to hack back in. Take the time to carefully check and reset all as appropriate.

It's a simple trap that too many people fall into, causing them to lose their email account forever. Check out A One-Step Way to Lose Your Account Forever.[154]

4. Set up two-factor authentication

If you don't have it enabled on your account already, now is the time to enable two-factor authentication.

Why? Because if you had enabled it, you wouldn't be here. Two-factor authentication means that *even if hackers discover your password, they still can't sign in*. They don't have the second factor — your phone, an authentication app, access to a specific email address, etc. — that you do. Without that second factor, they can't get in.

And don't let the hype about SMS being less than secure stop you if that's your only option. A) It's more than secure enough for the average user. B) It's still better than no two-factor authentication at all.[155]

[153] https://askleo.com/15264
[154] https://askleo.com/15584
[155] https://askleo.com/70786

5. Check out-of-office messages, reply-to, forwards, and signatures

If your email service provides an out-of-office feature, a vacation autoresponder, or an automatic signature, it's possible people already know you're hacked.

Hackers have been known to set an autoresponder in a hacked account to automatically reply with spam. Each time someone emails you, they get this fake message in return, often written so it sounds like you sent it.

If your account includes the ability to set a different "Reply-To:" email address, make sure that hasn't been set. Hackers set this so individuals who think they're replying to you end up replying to the hacker instead.

Make sure your email is not being automatically forwarded to another email address. If it's available, hackers often set this option to receive copies of every email you get. They can use this to break into your account again even after you recover it.

Check any signature feature the service supports. Hackers often set up a signature so that every email you send includes whatever they're promoting, including a link to a malicious website.

6. Check related accounts

This might be the scariest and most time-consuming aspect of account recovery. The risks are high, so understanding this is important.

While the hacker has access to your account, they have access to your email, including past email.

Let's say the hacker sees a notification email from your Facebook account. The hacker now knows you have a Facebook account and the email address you use for it. The hacker can go to Facebook, enter your email address, and request a password reset.

That password reset is sent to your email account, which the hacker has access to.

As a result, the hacker can now hack your Facebook account by virtue of having hacked your email account.

In fact, *the hacker can now gain access to any account associated with the hacked email account*.

Like your bank. Or PayPal.

Let me say that again: *because the hacker has access to your email account, he or she can request that a password reset be sent to it from any other account for which you use this email address*. In doing so, the hacker can hack and gain access to those accounts.

Check your other accounts for password resets you did not initiate and any other suspicious activity.

If there's any doubt, consider changing the passwords on all those accounts as well. (There's a strong argument for checking or changing the recovery information for these accounts, just as you checked on your email account, for all the same reasons.)

7. Let your contacts know

Some disagree with me, but I recommend letting your contacts know your account was hacked, either from the account once you've recovered it or from your new email account.

Inform all the contacts in the online account's address book, because that's the address book the hacker had access to.

I believe it's important to notify your contacts *so they know not to pay attention to email sent while the account was hacked*. Occasionally, hackers try to impersonate you to extort money from your contacts. The sooner you let them know the account was hacked, the sooner they'll know that any such request — or even the more traditional spam that might have come from your account — is bogus.

8. Start backing up

A common reaction to my recommendation that you let your contacts know is, "But my contacts are gone! The hacker erased them all, and all of my email as well!"

Yep. That happens.

It's part of a hacker not wanting to leave a trail. They delete everything they've done, along with everything you have. Or had.

If you're like most people, you don't back up your online email. All I can suggest at this point is to see if your email service will restore it for you. In general, they will not. Because the deletion was not their doing, but rather someone logged into the account, they may claim it's your responsibility.

Hard as it is to hear, they're absolutely right.

Start backing up your email now. Start backing up your contacts[156] now.

For email, that can be periodically downloading your email to a PC, or setting up an automatic forward of all incoming email to a different account, if your provider supports that. For contacts, it could be setting up a remote contact utility (relatively rare, I'm afraid) to mirror your contacts on your PC, or periodically exporting your contacts and downloading them, which is what I do.

9. Learn from the experience

Aside from "you should have been backing up", one of the most important lessons to learn from this experience is to consider all the ways your account could have been hacked and take appropriate steps to protect yourself from a repeat occurrence.

- Use strong passwords that can't be guessed, and don't share them with *anyone*.
- Use a password manager.[157]

[156] https://askleo.com/5937
[157] https://askleo.com/5555

- Use two-factor authentication.[158]
- Don't fall for email phishing attempts. If an email asks for your password, it is bogus.[159]
- Don't click on links in email you are not 100% certain of. Many phishing attempts lead you to fake sites that ask you to log in and then steal your password when you try.
- If you're using Wi-Fi hotspots, learn to use them safely.[160]
- Keep the operating system and other software on your machine up to date, and run up-to-date security software.[161]
- Learn to use the internet safely.[162]

If you are fortunate enough to identify exactly how your password was compromised (it's not common), then absolutely take measures so it never happens again.

10. If you're not sure, get help

If the steps above seem too daunting or confusing, get help. Find someone who can help you get out of the situation by working through the steps above.

While you're at it, find someone who can help you set up a more secure system for your email and advise you on the steps you need to take to prevent this from happening again.

Then follow those steps.

The reality is that *you and I are responsible for our own security*. That means taking the time to learn how to set things up securely and then doing so.

Yes, additional security can feel like an inconvenience. In my opinion, dealing with a hacked email account is significantly more inconvenient and occasionally downright dangerous. It's worth the trouble to do things right.

If that's still too much… well, expect your account to get hacked again.

Addendum: Is it my computer or not?

When faced with this situation, many people worry that malware on their computer is responsible.

That is rarely the case.

In the vast majority of these situations, *your computer was never involved*.

The problem is not on your computer. The problem is that someone figured out your password and logged into your account. They could be on the other side of the planet, far away from you and your computer (and often they are).

---

[158] https://askleo.com/16401
[159] https://askleo.com/3863
[160] https://askleo.com/4790
[161] https://askleo.com/3517
[162] https://askleo.com/2374

Yes, it's possible that a keylogger was used to capture your password. Yes, it's possible that your PC was used improperly at an open Wi-Fi hotspot. So, yes, absolutely, scan it for malware and use it safely, but don't think for a moment that once you're malware-free, you've resolved the problem. *You have not*.

You need to follow the steps outlined here to regain access to your account and protect it from further compromise.

You'll use your computer to do it, but your computer is not the problem.

One more thing

In addition to the steps above, I suggest one more step: share this article or video.[163]

As I said, email account theft is rampant. Share this article with friends and family. The odds are good that one day, you will encounter someone whose account has been hacked and will need this information.

[163] The URL to share is https://askleo.com/5415.

Do I Need a New Email Address if Mine Is Involved in a Breach?

> *"My email address was in one of the breaches we keep hearing about. Is that address still safe to use? Should I get a new email address?*

As long as you can still log in to your account, there's no need to get a new address just because your email address was included in a breach.

There are steps you should take, but getting a new account is not one of them.

If you can't log in to your email account anymore, though, you may have no other choice.

If you can't log in

If you can't log in to your email account and you've pursued all the approaches to recover access, *it's not your account anymore*. Email Hacked? 7 Things You Need to Do NOW[164] covers the steps you need to take.

Whether or not it's related to any reported breach doesn't matter. Regardless of how it happened, you've lost access to your account.

When that happens, you have no other option; you'll need to get a new account and let your contacts know you have a new email address.

If you know which service was breached

If you learn that your email address is part of a breach, and you know which service was breached, the most important step to take is simple.

Change your password with that service.

Change it to a long, strong password you don't use anywhere else.

It's the bare minimum you need to do, but many times, it's all you need to do. You don't need a new email account or address because of it.

If you don't know which service was breached

This is a more difficult scenario:

- You learn your email address was discovered in a data breach.

[164] https://askleo.com/5415

- There's no information about exactly which online service(s) the breach came from.

When this happens, I do two things.

1. I change my email password in case it was my email provider that was breached. This is probably unnecessary and exceptionally rare, but I'd rather be safe.
2. I start watching for odd behavior on all other accounts that the email address is associated with (either as login ID or as primary/alternate email).

That last point is frustratingly vague, but it's the best we can do.

And, honestly, it's what we should do whether our email addresses show up in breaches or not.

Additional security

I don't panic when news of yet another breach appears because I apply strong security to all my accounts.

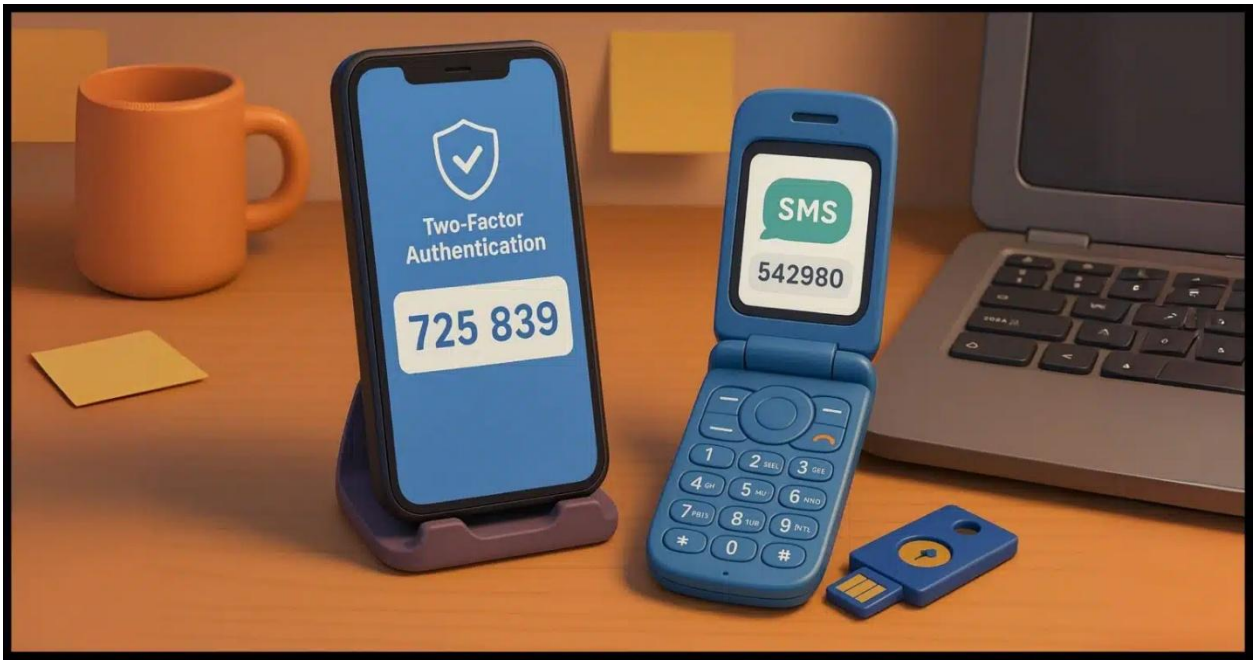
- Using strong passwords significantly reduces the probability that they could be cracked in a breach.
- Using different passwords everywhere means that when one breach happens, it can only impact the one account that's been breached.
- Using two-factor authentication means that even if my password is discovered, any attempts by others to use it will fail.

I strongly recommend you do the same, starting with your email account.

But there's no need to get a new email address because of a breach.

The bottom line is simple: maintain strong security to begin with, and breaches become a much less serious event. If you can track down which breached service included your email address, you can always change your password there for additional safety. Otherwise, just keep your guard up as normal.

Two-Factor Authentication: It's Not as Complicated as You Think



Two-factor myths include:

- You mean I have to do this every time I sign in?
- If someone gets my second factor, does that mean they can just waltz into my account?
- If I lose my second factor, doesn't that mean I'm locked out forever?
- Can't a second factor be faked/spoofed/intercepted, and doesn't that make it worthless?
- I don't have or want a mobile phone, so I can't use two-factor.

There's a lot of misinformation around two-factor authentication. This can lead people to avoid it, even though it's one of the most effective ways to secure their online accounts.

I want to clear up some of the myths around two-factor authentication. It's not nearly as confusing or as scary as you might think it is.

What is two-factor?

First, we have to define what we mean by two-factor authentication (2FA), which is sometimes referred to as multi-factor authentication (MFA).

Traditionally, you sign into an online account with a username and password. These are things you *know*. By keeping the password secret, your ability to provide it theoretically proves that you are you and should be allowed into the account.

A second factor is typically something you *have*.[165] For example, after 2FA is set up, after entering your username and password, you might be asked to prove you have access to your mobile device by entering a code that was sent to it. (I'll discuss other forms of 2FA below. Not all require a mobile device.) Your ability to provide the code that was sent to your device proves you possess the physical device, your second factor.

Two factors got you into your account: something you know (your password) and something you have (your device).

Requiring that second factor adds security because *even if a hacker somehow learns your password, they still can't get into your account* because they don't have your second factor.

It's NOT every time

Two-factor authentication is used only once:[166] *the first time you sign in* to an account on your computer. After that, your device becomes "trusted", and signing in later requires only your password, as before.

Of course, it's not quite that simple. Two-factor may kick in:

- The first time you sign in using a different browser.
- The first time you sign in on a different machine.
- The first time you sign in after clearing cookies.
- After some length of time defined by the service you're signing into; for example, after 30 days.
- If the service you're signing into detects "suspicious" activity on your account.

Those are rare, though, so in practice, you need to use two-factor only occasionally; certainly not every time you sign in.

Every sign-in from a hacker meets the "first time you sign in on a different browser/machine" criteria. Thus, they'll always be asked to provide your second factor, which they don't have.

A second factor alone is not enough

Remember, it's *two*-factor authentication. You need both your password and your second factor to sign in that first time.

That means having your second factor fall into the hands of a hacker is an issue *only if they also know your password*.

The people who might find (or steal) your second factor are rarely the same people who might gain access to your password. The former, of course, need to be close enough to get their hands on the factor, and the latter are typically overseas working their scams.

---

[165] A different type of second (or third) factor can be something you are, meaning some physical characteristic about you, such as your face, fingerprint, iris, or something else.

[166] As always, there are exceptions. "Never say never" and all that. But in general, and especially for consumer accounts, 2FA is required only the first time.

If you lose your second factor, you can quickly disconnect it from your account by signing into the account and turning off or changing the existing two-factor configuration.

Losing your second factor is an inconvenience, not a disaster

If you lose your second factor, you will not be locked out of your account.

There are two safety nets in place, plus a third if you take additional steps.

Backup codes. First, when you set up two-factor authorization for an account, you'll be prompted to create and/or save a set of backup codes. Each of these codes can be used once in place of your second factor. Once you sign in, you can temporarily turn off 2FA or change it to a replacement device. The backup codes need to be stored securely, but as long as they're accessible to you, you can always get back into your account.

Account recovery. Second, services offer many account recovery techniques (AKA "I forgot my password") to confirm you are who you say you are without your second factor. They may send an email message to an associated recovery account, a text message to a different recovery phone number, or any of several pre-configured recovery options. After you jump through these additional hoops, the service may accept your sign-in without the second factor. This doesn't invalidate 2FA as a security measure, because a hacker would have had to jump through all those hoops as well, which is extremely unlikely. Your ability to do so proves you are you.

A *second* second factor. There's a third safety net you can set up yourself ahead of time: an additional second factor. When using hardware keys as 2FA (see below), it's common to set up two keys, keeping one in a safe place as a backup. In that same vein, you could set up both SMS and app-based 2FA such that either could be used in the event the other is lost.

In all cases, and as long as you prepare (which most services require), losing your second factor is an inconvenience at worst.

Two-factor spoofing

There is no such thing as perfect security. Period.

That means that it is possible for hackers to spoof or bypass two-factor authentication in some situations. The two most common:

1. Mobile numbers can be stolen (AKA "sim swapping"), redirecting all SMS messages to the hacker.
2. Successful phishing attacks can intercept two-factor codes in real time.

#1 requires you to be individually targeted, and you can set up a PIN with your mobile provider to prevent unauthorized reassignment. For #2, you can pay close attention to signs of phishing to avoid being lured down this path.

Both spoofing techniques are rare and preventable. *Any two-factor authentication is better than no two-factor authentication.*

By using 2FA, you are stacking the odds in your favor, making it significantly less likely your account will be compromised.

Second factors

You don't always need a mobile phone or a smart device.

This varies based on the online provider with which you're setting up two-factor authentication, but often services allow a variety of devices to be used. These may include:

- A smartphone to run a TOTP (Time-based One Time Password) two-factor authentication app or service-specific authentication app.
- A mobile phone to receive SMS text messages.
- Any phone to receive codes via automated voice (sadly, this is rare).
- Email addresses unrelated to the account using 2FA. Your ability to receive a code, for example, at a specific pre-configured email address, can act as a second factor.
- Hardware keys such as the YubiKey.
- Any other device already signed into the account that can present a "Is that you signing in on that other device?" approval message.
- Your device's camera or fingerprint reader.

I've seen each of these act as a second factor on various services. Which ones are offered is up to each service.

Why bother with all this?

To be clear, 2FA is very little bother. The only thing that really changes after you set it up is that the first time you sign in to a new device or browser, you need to use your second factor. After that, it's the same sign-in process as before.

Password-based compromise happens daily. Due to bad passwords (which of course you don't use — right?), malware, brute-force attacks, breaches, or other forms of compromise, accounts are hacked often. Two-factor stops 99%[167] of these attempts dead in their tracks.

2FA provides peace of mind.

Take a few minutes right now and set up two-factor authentication on every account you have that supports it. Start with your password manager and then your email, financial, and social media accounts. Take care to follow the instructions carefully and create/save the backup codes you'll be instructed to set up.

A few minutes today could save you a giant headache in the future.

[167] OK, I made that up, but honestly, I expect the real number to be more like 99.99%.

Part 6: Protect Your Privacy

You're Just Not That Interesting (Except When You Are): Pragmatic Privacy



Privacy is a huge and controversial topic. I can't tell you what steps to take, what settings to change, what apps to avoid, or what services to choose. Not only are there seemingly infinite options, but the options keep changing.

There are also about as many opinions on the topic as there are internet users. Anything I say is just one more voice in the crowd… but that's not going to stop me.

Let's take a realistic look at your privacy and your options.

Two kinds of privacy

Privacy is a big term, so I want to define two types of it.

Implicit privacy is the privacy we assume when we use online services, operating systems, applications, and programs to manage our personal information and activities. Each has a set of rules — often some formal privacy policy — controlling their access to your information and what they do with it.

Explicit privacy is the privacy we control more directly with our choices. For example, choosing not to share a photo on social media is one form of explicit privacy. Keeping our passwords to ourselves is another. So are the settings we use to control who is allowed to see what we post.

The biggest difference between implicit and explicit privacy, in my mind, is the amount of control we have over it. We *implicitly* trust that the software and services will do as they say. We *explicitly* decide what to share based on what we believe may happen.

Privacy, policies, and Big Brother

Privacy — or lack thereof — when using popular services or software is big topic of discussion. For example, Window's tracking activity generates a great deal of concern. It's debatable whether the concern is warranted.

Any online service involves some amount of tracking. Visiting a simple website — even Ask Leo! — results in some amount of what might be considered tracking, usually in relation to advertising displayed on the site. Some consider that an invasion of privacy. The most common visible signs are advertisements that appear to follow you[168] from site to site as you browse the web.

All online services and websites can collect vast amounts of data derived from their users. Similarly, any software you install can collect usage information.

Whether or not you believe Big Brother is watching, the technology is there should he want to.

The (poor) choices we make

At the other end of the privacy spectrum are the (often poor) choices we make about what we share and with whom.

I often hear from individuals who have shared a password with a trusted friend, only to be surprised when their privacy is violated because the trust was misplaced.

We've all heard stories of individuals losing jobs or job opportunities because of statements, photos, or videos posted on social media. Call your boss names on Twitter, for example, and there's no one to blame but yourself when you're shown the door the next morning. Have you posted "funny" pictures of yourself after imbibing a tad too much alcohol? That could be the reason you don't get the next job or loan you apply for.

When it comes to privacy, we're often our own worst enemy.

You're just not that interesting

I say it often: you and I just aren't that interesting as *individuals*. That your operating system might track what you do is pretty meaningless in terms of *personal* privacy. That advertisers might use what websites you visit and things you click on to tailor the ads you see is pretty benign.

The companies collecting this data aren't looking at you as an individual. They're looking for *trends* from the data of millions of users to determine what's being acted on, what's influencing the crowd, and what they might do better.

I do it, too. For example, do I care that you, specifically, looked at my newsletter?[169] At a personal level I do, but I'm not going to sift through information on nearly 50,000 subscribers to see who did and who didn't. On the other hand, if 10,000 fewer people open the newsletter one week, that's

[168] https://askleo.com/5670
[169] https://newsletter.askleo.com/

information I want to act on. I can only do that by tracking the behavior of 50,000 individuals in aggregate.

The same is true for most any company. Your personal privacy isn't being violated, because nobody is looking at you specifically. One person just isn't that interesting; thousands or millions, on the other hand, almost certainly are.

But you might be interesting someday

There are two cases in which you could become interesting.

If you run afoul of the law. This isn't an issue for most. But if you live in an oppressive regime or are subject to investigation for your activities, it could be. Even this falls into two sub-categories: the unduly paranoid (a larger number of people than we might hope), and the legitimately concerned, for both legal and illegal reasons.

It is important to realize that if you fall into this category, law enforcement may have the right to collect information about you. This can include things we might brush off as irrelevant, like ad or service usage collected by your ISP or the services and software you use. I have to say law enforcement *may* have the right, because laws differ dramatically depending on where you live. Of more practical importance, perhaps, is that law enforcement capabilities vary dramatically based on everything from expertise to budget to jurisdiction to prioritization of limited resources.

Future opportunities. Some years from now, perhaps someone will research your history as part of a job application or something else where your record and reputation are important. What you post today, publicly or even privately, may influence their opinion tomorrow.

It's all so scary. What to do?

It'd be easy to read that last section, throw up your hands, and crawl into a hole, thinking privacy is a thing of the past — at least when it comes to the internet.

If you're a criminal, you probably should be concerned. The only thing preventing you from being exposed is the limited resources of the law enforcement agencies who really *do* care about you specifically. There are steps you can take, but I'm not the one to help you take them.

For the rest of us living more mundane lives, my advice is pretty simple.

First, *stop worrying about being tracked* by the companies providing the services you use. They don't care about you as an individual. There is plenty of room for policy debate about what kinds of information they should and should not collect and how they should or should not use it, but in my opinion, that has little chance of impacting you *as an individual*.[170]

[170] And if you're going to worry, then be more consistent. It's funny to me to get rants about the alleged privacy violations of, say, Google, sent via an @gmail.com address, or an account provided by Microsoft, whose activity is on par with Google. If the behaviors of the major service providers concern you that much, I know of no solution other than walking away from the internet entirely.

Second, *never post anything you wouldn't want made public*. Learn the privacy policies and settings of your social media and other applications. Change them and/or change your behavior accordingly. Public once is public forever; there's no calling it back from the internet.

Think twice about what you post privately, since you're trusting your private audience not to make it public someday without your approval. This includes social media, but email, text messaging, or other media. We've all seen situations where communications once thought private were made public to great embarrassment or worse.

Privacy remains your responsibility

I remain a strong believer in our wonderfully interconnected world and all the opportunities it presents.

Naturally, it brings risk as well as reward.

Ultimately, it's *our* responsibility to be aware of those risks, educate ourselves about the possibilities as well as the practical realities, and make careful choices accordingly.

You Can't Un-Ring a Bell: What Really Happens to Your Data When You Post Anything Online



When we post something online — say on social media — there's a reasonable expectation that what we post will remain in our control and be shown only to the audience we care about.

Reality is exactly the opposite: you lose all control of anything you post online, and it can end up in the hands of people (and corporations) you know nothing about. Even with privacy settings set to Private.

The service makes copies. Viewers get copies. Search engines, spiders, researchers, AI scrapers, and archivists make copies. And all of those entities generate *more* copies when they back up their data.

It starts the moment you hit Post



Let's say you post a photo of your dogs online. I'll post one here, but let's assume you're using social media.

The moment that photo is uploaded, copying begins.

- The service may create additional copies of your photo in different resolutions. On Ask Leo!, something like five different resized copies are created, each to be used in different contexts: thumbnails, page display, and "click for larger image" are examples of three different copies of the same image.
- The service may replicate photos across a content delivery network (CDN) so files are delivered more quickly

from CDN servers nearest to you. I use a small CDN that replicates into US East Coast and West Coast data centers. Large social networks may have hundreds, if not thousands, of servers scattered across the globe that eventually get copies of your photo.
- Hopefully, the service backs up to recover from any problems. Ask Leo! gets backed up daily, and social networks are likely backed up continuously. Each backup generates more copies.

This isn't malicious; this is how large services stay fast and reliable.

Your data has been copied to many places before anyone even sees it.

Every viewer gets a copy

There is now a copy of the photo displayed above on your computer.

That's how viewing webpages works: the browser downloads a copy of whatever is to be displayed — the text and any media included on the page — and places it in your browser's cache in case it's needed again sometime soon. What's "soon"? There's no way to know. Items that haven't been used again "for a while" are deleted from the cache to make room for newer pages you view.

In addition, you can save a copy of that photo yourself in several different ways.
- Right-click and "Save image as…"
- Right-click and "Copy Image"
- Take a screenshot

That last one is an example of my "If it can be seen, it can be copied" rule of thumb.

Regardless of how people save the image, you lose all control over it. They can do with it what they wish.

Search engines get copies

Search engines regularly make copies of whatever they find online. It's not just Google and Bing; there are hundreds of different search engines around the world. Any of them can scan whatever you post online.

While we normally think of searching as pointing us to where information can be found online, many search engines build their own local cache of data so they can present what they find more quickly. Searching Google Images is a good example: the results are images that come from Google's cache, not the original sites.

If wherever you posted your photo can be found in a search engine (as hopefully this page will be), then the images displayed on it are almost certainly copied to the caches of several different search engines.

Spiders, researchers, and scrapers get copies

Besides traditional search engines, other systems regularly "scrape" or copy content found online.

- Academic and research spiders: everything from class projects to specialized academic research databases are constantly scanning the web.
- Archive services are busy copying webpages for historical purposes. Perhaps the best known is archive.org,[171] but there are others.
- Like it or not, AI scrapers are slurping up everything they can find to train their models. Once again, this is more than just the big names you might think of, like OpenAI, Anthropic, and others. There are likely thousands of LLMs being trained on internet data constantly.

All can make copies of your photo.

Backups are even more copies

All of the services I've mentioned so far probably have backups.

Each time it is backed up, there are even more copies of your photo living in data center backups, long-term tape archives, or who knows what else these services might implement. How long their backups are kept is, of course, unknown and different for every service.

Let's not forget the backups taken by people who've viewed your content. If you back up your computer regularly, as I hope you're doing, then it's likely the next time your backup runs, it will include a copy of my photo above in your browser's cache.

But I marked it private!

Restricting your audience is a fine way to reduce the initial exposure of your post to, say, friends and family. Unfortunately, it really doesn't help.

- Your friends and family can download and make copies.
- Search engines — typically those internal to the service you're using in this case, but perhaps others — will have made copies.
- The service's backup will still have happened, and copies made of it.

The first one is the one that typically trips people up: a trusted friend copies and shares a photo beyond your initial privacy setting.

Clawing it back or taking it down?

You can, of course, remove your photo from wherever you posted it. I can, for example, remove the photo at the top of the page. That removes the original and perhaps most obvious copy of your photo. But it doesn't matter. All those copies I've talked about above have already happened. Your photo is loose in the wild. You've lost control over it.

You can ask sites to take it down or remove it from their caches. In the US, you can file a DMCA take-down request for services. Some might even do what you ask. Most will ignore you. And this

[171] https://askleo.com/2484

presupposes that you know where to look and who to ask. Sites and services you've never heard of will have already copied your photo.

Then there's that little thing called the Streisand Effect.[172] Sometimes asking for information to be removed backfires by drawing more attention to it.

The "right to be forgotten"?[173] When used successfully, it only removes search engine entries pointing to what you want to have removed. The sites that were pointed to continue to exist, along with all the non-GDPR-affected search engines and all the caches and backups I've discussed.

The bottom line: *think before you post anything*.

Maybe think of it as a "release" rather than a post or a share; you're releasing your photo into the wild. If you don't want something to be permanent and public, don't post it.

[172] https://en.wikipedia.org/wiki/Streisand_effect
[173] https://askleo.com/14510

Are You Giving Away Your Privacy?



In the 10 years since this article was first written, things have not improved.

Too many people are still posting — *explicitly, voluntarily* posting — their private information in public places.

On one hand, we rail against the loss of privacy posed by the various online services we use and the companies behind them, not to mention concerns that various governments might be snooping inappropriately.

On the other hand, we often hand out our private information without hesitation to anyone who wanders by.

Public is very public, and often, so is private

Part of it may be a lack of understanding.

As just one example, when you respond to something on Facebook, anyone can see it. You might think it's a direct line to only the poster, or perhaps restricted to only the poster and their "friends", but:

- It's often completely public to anyone on the internet.
- Even if it's not, it can easily be copied and reposted publicly.

The same holds true for website comments. Here's one example. Comments posted on Ask Leo! are not only visible to anyone who happens to come by, but they're regularly scanned by search engines and archived by internet archive sites. Not only is what's posted in a comment public, but once posted, it may never be completely removed from the internet even if it is removed from my site.

With all the controversy over internet privacy, shouldn't we understand that public is now more public than it's ever been? Billions of people could potentially see what you post.[174]

Public can have consequences

People post email addresses online *all the time* (and then wonder why they get spam).

Particularly with Q&A sites like Ask Leo!, some people are so desperate to get a response that they post their email address for the entire world to see in their comment. Not only will they get spam, but it's an open invitation for scammers to know exactly what they're looking for and then scam them with a fake solution. (I see this all the time on YouTube.)

And phone numbers? Would you put your phone number on a bathroom wall for anyone to see? Of course not. So why do people post them on blog comments and Facebook pages? I can only imagine that they're opening themselves up to all sorts of potential abuse or harassment.

Privacy is your responsibility, too

Yes, we should be ever watchful for corporate and government abuse, without a doubt.

But privacy starts at home. Just as with malware prevention, individuals are often the weakest link in the chain.

Watch who you're giving your information to. This goes beyond just email addresses and phone numbers. Just because a form randomly pops up asking for something doesn't mean you have to give it (or that it has to be accurate). Use common sense. Use good judgment.

[174] No, I'm not saying billions will, I'm saying that any of the billions of people on the internet today could.

The Biggest Risk to Your Privacy



I write a lot about various aspects of technological risk to privacy. The computers and services we use, the systems running them, and the applications and tools we rely on each add risk of some kind to our privacy.

And yet, in my experience, the greatest risk has little to do with technology.

We don't often consider it, yet I see privacy compromised more often due to this factor than for any other reason.

The biggest risk is people

Even with semi-regular news of data breaches, hacking, and other technological intrusions, the single biggest cause of privacy-related damage boils down to nothing more than people.

You're probably already making assumptions about which people to be concerned about, but I expect you're overlooking those who put our privacy most at risk every day.

Let's review some of the various types of people who can compromise our privacy: hackers, government, service providers, people we know, and ourselves.

Hackers, scammers, and other ne'er-do-wells

We hear a seemingly endless stream of news and word-of-mouth reports of privacy hacks every day. It's easy to think we're under constant threat from evil villains trying to get at our data.

In a sense, we are. There's no question that organized crime and other malicious entities have their sights set on gathering personal information and either using it for nefarious purposes directly or reselling it to those who will.

While your data could fall victim to the individuals in this category, it's important to realize that they aren't interested in you as an individual.[175] They care about gathering as much data as possible or scamming as many people as they can. They don't care who those people are — just that they're vulnerable.

These are the people from whom we can most easily protect ourselves by using technology and common sense. Security software[176] of various flavors and layers, coupled with skepticism[177] and our own smart habits,[178] is our first, best line of defense.

Governments and government agencies

You may think I'm including this because I'm concerned your government is spying on you.[179]

I'm not.

Oh, it's certainly possible, and in some countries even plausible, depending on your behavior and value to whoever might be watching. Once again, however, I strongly believe that most of us, in most countries, aren't worth the effort of individual government surveillance. We're just not that interesting.

No, what makes government one of the largest threats to our privacy is the laws and policies they enact or fail to enact. Weak government policy and enforcement around individual rights and privacy make it easier for others — in the government and elsewhere — to access and possibly misuse our personal information.

Most people don't pay attention to this unless they're already living under an oppressive regime, in which case it could be considered too late. I strongly suggest that paying attention and working within your system to ensure personal privacy rights is an important responsibility.

Employees, technicians, and policy makers

Many people are concerned about big business and corporations collecting and using our personal information.

I'm generally not. Other than making sure government regulations are in place to protect my information, as well as corporate policies that similarly ensure my privacy (whether legally required or not), I'm not that concerned about the information I know is out there about me… unless those companies get hacked or otherwise compromised. That possibility comes back to the people involved. I believe most breaches boil down to individual people making individual errors.

[175] https://askleo.com/22674
[176] https://askleo.com/3517
[177] https://askleo.com/21535
[178] https://askleo.com/2374
[179] https://askleo.com/6055

Consider the software engineer with little to no security experience who is put in charge of the security of my data. All the good intentions in the world won't make up for his or her inevitable oversight (which is probably more common than we suspect). Software developers and policy makers often operate under a "features first, security later" approach that can push service development — and with it, our personal information — beyond acceptable risk. Then, once a vulnerability is discovered, the hackers mentioned earlier swoop in to take advantage of the access to our information.

The most important thing you can do to secure yourself against these types of oversights is to know who you're dealing with and hold them accountable for the security of your information. Do business with companies with a proven track record. If you find you can't — if you need the services of an unproven entity — be particularly wary of the information you choose to share.

Friends and family, business contacts, and associates

We share a fair amount of information without thinking about the consequences of exposing it.

Sometimes that can be literal. People often come to me concerned that their video chats might be intercepted[180] by someone. As it turns out, the person they most need to be concerned about when they find themselves being blackmailed is *the individual at the other end of the conversation*.

The fact is, *no technology can protect you from the people you choose to share your information with*. Any technology can be circumvented in one form or another by the recipient. *If it can be seen, it can be copied* — even if it's just taking a picture of the computer screen while your sensitive details are displayed.

And of course, once something is posted publicly (and let's be clear: all social media is public, regardless of your privacy settings), it cannot be recalled.[181]

This is probably the single most common cause of privacy violations I've encountered over the many years I've been doing Ask Leo! — not big business or government, not massive data breaches, not malware, not even ransomware[182] — but one-to-one interactions in which individuals share too much and later regret it.

This risk is only growing on social media, which creates an illusion of intimacy and safety while nothing of the sort exists.

You

You are the biggest risk to your own privacy.

[180] https://askleo.com/10960
[181] https://askleo.com/24288
[182] Which is just malware. Particularly destructive, but malware nonetheless.

By sharing too much on social media, trusting too easily when some stranger calls[183] telling you your computer has a problem, or reaching out to the wrong people[184] in times of technological crisis, the biggest risk of all comes back to you.

And that's great!

Now, why, after all that gloom and doom about how our privacy can be compromised, am I so excited to point the finger at you?

Because the one thing you have control over is yourself.

You can become more knowledgeable. You can make better decisions. You can take responsibility for your privacy from here on out.

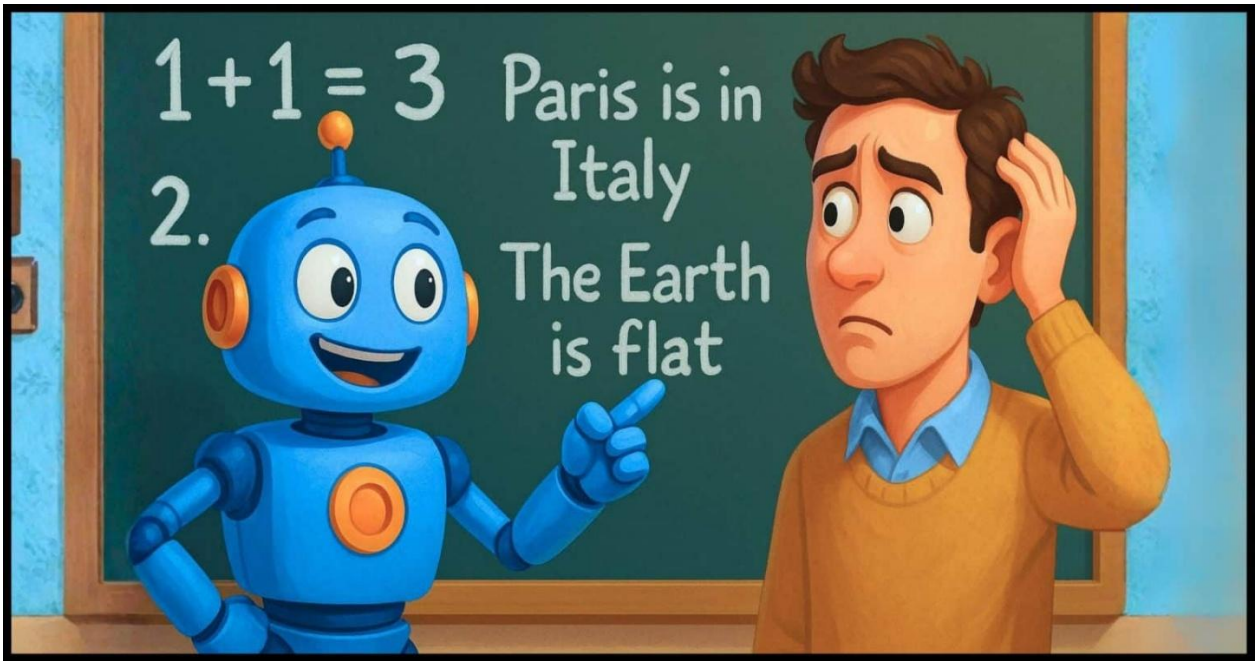
There's no requirement that you become a Luddite and walk away from technology in general — Lord knows I've certainly not done that. What's required is simple awareness — mindfulness, if you will — of exactly what, where, and with whom you share.

That last one is the most important. Your privacy is all about the people you share with.

[183] https://askleo.com/4164
[184] https://askleo.com/22072

Part 7: AI

Why I Cringe When I Hear People Are Using ChatGPT to Look Things Up



Don't get me wrong: used properly, AI is an amazing tool. I use it myself daily for everything from idea generation to image creation to summarization and more.

I also use it for search and Q&A. Mostly. Sometimes. With a great deal of trepidation and skepticism.

When I hear people "just" use AI now in place of more traditional tools and techniques, I get worried… really worried.

AI doesn't yet deserve your trust

When I say AI here, I'm referring to large language models (LLMs) such as ChatGPT, CoPilot, Gemini, Claude, and a host of others. They're certainly artificial, but whether they're an "intelligence" is up for debate, both technical and philosophical.[185]

To be clear, they don't "think". As others have pointed out,[186] they're really nothing more than a glorified, immensely powerful, auto-complete function. The "answers" you get from AI are nothing more than the words that are most likely to follow the words in your question. There was no thought put into it, just massive amounts of statistical analysis.

> *"Responses from Large Language Models like ChatGPT, Claude, or Gemini are not facts.*

[185] What does it mean to be intelligent, anyway?
[186] https://stopcitingai.com/

They're predicting what words are most likely to come next in a sequence. They can produce convincing-sounding information, but that information may not be accurate or reliable." (StopCitingAI[187])

Nonetheless, they're amazing. It does feel like they do a much better job of understanding[188] my various statements and queries than a traditional search engine. A vague, poorly worded question that might baffle traditional search, for example, can get spot-on results from an AI.

However, understanding my question is completely different from answering it correctly.

It's easy for us to evaluate what AI gives us and recognize — even be impressed with — its ability to understand what we mean or realize that it completely misinterpreted us.

It's nowhere near as easy to evaluate the response it gives us. Unless we're already familiar with the topic at hand, we have no objective way to evaluate whether the answer is correct.

This should scare you.

Its confidence is misleading

One characteristic of AI that was identified early on was the confidence it exhibited in its answers. It was humorous: AI was known for providing very confident and very inaccurate answers.

While its accuracy has certainly improved, the unwarranted confidence remains. If anything, it's taken on a new sheen of sycophancy. It not only provides answers with authority, it does so in a way that plays to our egos. It still gives confident answers couched in terms that try to please or suck up to whoever's asking it.

Sometimes it's right. I might even say that most of the time it's right. And yet, it's still often wrong. Sometimes a little, and sometimes very, very wrong.

With its confidence and eagerness to please, it's too easy to just assume it's correct and skip any kind of verification.[189]

This is another reason misinformation spreads: we assume the source is correct when it's not.

Where AI Q&A is helpful

I'm not saying not to use AI for questions or in place of search. I do it myself.

But.

I use it to *augment* what I know, not replace it. For example, I ask AI tech questions all the time. It's not uncommon for me to just copy/paste a question I've been asked into an AI — perhaps because I

[187] https://stopcitingai.com/
[188] Whatever "understanding" might mean.
[189] My theory is that when something acts "eager to please", it's more difficult to think critically about it because of our instinct not to offend… even though there's nothing here to be offended. Just my pet theory.

couldn't understand the question and AI might, but mostly because it's a quick way to generate *potential* answers.

I vet those potential answers. Because this is my area of expertise, I can weed out the right from the wrong, the pragmatic from the dangerous, and what's applicable from the irrelevant. If I need to, I can take what AI has provided and refine it with more queries — often in the AI, but also in more traditional searches (often including that on my site). This process often generates issues I wouldn't have thought of or that I wouldn't have thought of as quickly.

If you're not familiar with the subject to begin with, it's terribly easy for AI to lead you astray. I've heard from too many people who've made a further mess of things simply by blindly following the (no doubt very confident) instructions provided by an AI chatbot.

Skepticism is still required

If you're going to use AI to research information and answer questions, you must — MUST — remain skeptical of the information it provides. Ignore the confidence and be skeptical of the answer.

Double-check it. Check the references, if they're provided. Pit two (or more) AIs against one another and see how their answers differ.

Use a completely different technique to vet the answer you've been given. That could be your own experience, common sense, or more research into the topic at hand.

Just don't take AI-generated answers at face value unless or until you have something else that would lead you to believe that the answer is correct.

Experience over time may not help

One thing humans do is build trust over time. For example, if you've gotten an answer from me that turned out to be helpful, you're slightly more trusting in me the next time you have a question. This is how trust is built.

I'm not sure trust-building should apply to AI.

If you get a helpful answer from AI, you're more likely to go to it with your next question. Whether or not the previous answer should influence your level of trust is complicated.

If it's in an area closely related to your original question, some additional trust might be warranted. An example might include questions about how to get Windows File Explorer to display things a certain way. It could still be wrong, but the probability is less.

If it's in a different area, then no additional trust is warranted, period. That it answered a Windows File Explorer question accurately should have no bearing on the answer it might provide about something health-related. These are separate areas of information. (This concept applies to the humans you might ask these questions of as well. Ask me about Windows, but not that suspicious lump on your arm.)

Here's the problem: When is it really a different area? We don't always know.

An AI might have ingested more information on Windows File Explorer than on, say, the Windows Event Viewer, device drivers, Windows 11 versus Windows 8, or many other topics. The topics might feel related — they're all about Windows, in this case — but under the hood, they're dramatically different areas of information. Once again, that includes your human resources.

It's much too easy to extrapolate accuracy in one area into areas where that trust remains unwarranted.

This isn't really new

You'll note earlier I said, "Skepticism is still required". That's because in a very basic way, this shouldn't be new behavior for us at all.

We've long been skeptical of search engine results — even more so in recent years, as those results have been skewed by various competing interests ranging from politics to advertising to sponsorships to SEO-gaming and more.

Apply the same level of skepticism — and perhaps a skosh more — to AI.

Faking Reality: How AI Images Are Being Used to Scam You



The image above is not my car.

It looks like my car. The color is close, the model is correct, and the license plate is mine.[190] But I've never parked outside The Golden Banana strip club. I have no idea if such a strip club even exists.

That the AI-generated photo looks so real, however, is cause for concern. Deep concern.

Son of Photoshop

I think we've all come to be slightly suspicious of photos because of the rise of Adobe Photoshop and similar tools. In the hands of the right person, Photoshop can generate amazing things, ranging from altering existing photos to creating "photos" of things and situations that never happened. With talent and time, a Photoshop artist can create just about anything.

Emphasis, of course, on both talent and time.

AI removes both of those requirements. The image above was created by asking ChatGPT:

Please create a 16:9 photorealistic image of a blue 2025 Rivian R1S, Washington license plate "N7LEO" parked in front of "The Golden Banana" strip club at night.

Two minutes later, the image above appeared. It's plausible enough to pass for real to the casual observer.

[190] A Washington State "vanity" license plate with my ham (also known as amateur) radio call sign: N7LEO.

Scammers know this.

Example scam

A scam posted on Reddit's r/Scams subredit[191] brought this to my attention.

The original poster (or "OP") asked how the scammer was able to identify his license plate to use in the photo. It turns out that an assortment of information, ranging from vehicle type and characteristics to the name of the owner, is often available. It might be publicly available through shady services, or it might be illegally available to hackers knowing where to look (perhaps on the dark web).

But looking up a license plate associated with a specific person is apparently not that hard for those so criminally inclined.

And as we've seen, using that information *to craft a fake yet plausible image to use in an extortion scam takes all of a couple of minutes*.

It's about more than your car or your license plate

Using your car's information to create a realistic photo to attempt to scam you is only an example. Scammers don't have to extort you personally; perhaps they use fake images to sway public opinion. There's a range of uses.

- Photos in extortion attempts, no matter how realistic you think they look, are often AI-generated fakes. Scammers can use data discovered in breaches and elsewhere to create highly targeted scams, including bespoke images related to the targets of their scams.
- Photos on social media of someone doing something you'd never expect them to do are frequently AI-generated fakes.
- Sadly, photos from just about any organization with an agenda — political, social, or otherwise — are now often complete AI-generated constructions (or existing photos altered using AI) to reflect something that never really took place.

It's now trivial for anyone to create images that look real and are completely fake. Scammers, hucksters, and others with less than altruistic intentions are more than happy to use this new technology to fool us.

And fool us, they do, especially if the fake image is of something we want to see or confirms our preconceived ideas.

191 https://www.reddit.com/r/Scams/comments/1lwpm09/us_extortion_text_message_with_fake_strip_club/?solution=8a4051d77e5cbb658a4051d77e5cbb65&js_challenge=1&jsc_token=7afd7253fec22262ff1c52b1703fe9ecb77dd3d179bc83b223e2decf5dee44b8&jsc_orig_r=

How to avoid getting fooled

It all boils down to paying attention, and that's very difficult in today's fast-paced, attention-grabbing world.

For example, consider the photo above. There are signs it's fake. The most obvious is that the shadows are wrong: there should be a shadow to the right of the car caused by the bright strip club sign. A close look at the license plate shows it's "fuzzier", for lack of a better term, than the quality of the photo would imply it should be.

Of course, if you can compare it to reality, it becomes even more obvious: the vehicle color is off, and my roof rack is missing.

Yes, those all seem like small, even subtle clues, but they're easy to overlook, and scammers are counting on you to do exactly that. And yet they're exactly the kinds of things you should look for the moment there's any question at all.

And these days, there should probably always be a question.

Endnotes

Afterword

I hope this book helps you protect yourself against all the nasty things that happen to you in our internet-connected world.

If you find what you believe to be an error in this book, please register your book (the details are in an upcoming section) and then visit the errata page for this book. That page will list all known errors and corrections and give you a place to report anything you've found that isn't already listed.

Register Your Book!

I've got additional updates, errata, and other bonus materials for you:

- *Updates For Life* to this book, as they're released.
- Downloads of this book in any or all of three digital formats:
  - PDF (for your computer or any device that can view PDF files)
  - .mobi (ideal for the Amazon Kindle), or
  - .epub (for a variety of other electronic reading devices).
- Other bonuses and supplementary material I might make available in the future.

Registering gives you access to it all.

Visit https://go.askleo.com/regisfree *right now* and register.

That link is mentioned *only here,* and it's totally FREE to owners of this book.

About the Author

I've been writing software in various forms since 1976. In over 18 years at Microsoft, I held both managerial and programming roles in a number of groups, ranging from programming languages to Windows Help, Microsoft Money, and Expedia. Since 2003, I've been answering tech questions at the extremely popular *Ask Leo!* website (https://askleo.com) and in other entrepreneurial projects like this book.

Curious for more? Someone asked, and I answered on the site: Who is Leo? (https://askleo.com/who-is-leo/).

Feedback, Questions, and Contacting Leo

I'd love to hear from you.

Honest.

I truly appreciate reader input, comments, feedback, corrections, and opinions — even when the opinions differ from my own!

Here's how best to contact me:

- If you have a comment or a question about this book, I strongly encourage you to register your book, as outlined above, and use the prioritized comment form in the registered owner's center.
- If you prefer not to register your book, you can email me at leo@askleo.com.
- If you have a computer or tech-related question, the best approach by far is to first search *Ask Leo!* (https://askleo.com). Many, many questions are already answered right there, and finding those answers is much faster than waiting for me.
- If you can't find your answer using Search, visit https://askleo.com/book and submit your question. That's a special form just for book purchasers and it gets prioritized attention.
- If you just want to drop me a line, or have something you want to share that isn't covered above, you can use https://askleo.com/book, or email leo@askleo.com.
- If you're just not sure what to do, email leo@askleo.com. ☺

Copyright and Administrivia

This publication is protected under the U.S. Copyright Act of 1974 and all other applicable international, federal, state, and local laws. All rights are reserved.

Please note that much of this publication is based on my own personal experience and anecdotal evidence. Although I've made every reasonable attempt to achieve complete accuracy of the content in this book, I assume no responsibility for errors or omissions. You should use this information as you see fit and at your own risk.

Any trademarks, service marks, product names, or named features are assumed to be the property of their respective owners. They are used only for reference. Unless specifically stated otherwise, use of such terms implies no endorsement.

More Ask Leo! Books

If you found this book helpful, check out my library of books at https://askleo.com/shop.