AAAGGGH Cyber Security

Free Starter Guide

Welcome to understanding the cyber security considerations we all should be making

First written: 05 August 2025

Cybersecurity Basics: How to Stay Safe Online (Without Getting Overwhelmed)

You've already probably have been hacked. You just don't know it yet.

A quick, shocking, and practical guide for everyday people.

Introduction

I've been working in cybersecurity for a long time now, and I've seen things that genuinely stop you in your tracks. Moments where you think, 'How is this even possible?' The truth is: it's not only possible but it's happening. Every day, and far more often than most people realise.

What shocks me most isn't the attacks themselves. It's how casually we walk through digital minefields without even knowing it. We connect to Wi-Fi at cafés, click links in messages, reuse the same old passwords, and download apps because someone told us they're fun. Our phones, our laptops, even our smart fridges are connected, and that connectivity has a dark side. Funny thing is most of us don't even know of or want to see the dark side of the tech we use?

This isn't about scaring you. It's about showing you the reality, the same reality I teach students and professionals about every week. Once you see what's really going on, you'll never look at your everyday online habits the same way again.

Here's a simple teaser question! Do you even have anti-virus software on your phone? If not, why not? You wouldn't dream about using your P.C. or Laptop without it. However, I'll bet the phone in your hand has way more personal data than your desktop or laptop!

What Most People Get Wrong

Let me say this clearly, if you're online, you're a target. It doesn't matter if you're not famous. It doesn't matter if you have 'nothing to hide.' Cyber-attacks aren't always personal, they're opportunistic. Criminals cast wide nets, and anyone can get caught. Anyone.

Every day I meet people who laugh and say things like "I have no money in the bank to steal". But its not all about money so it's time to stop with the kind of, it won't happen to me, attitudes and get serious about cyber security!

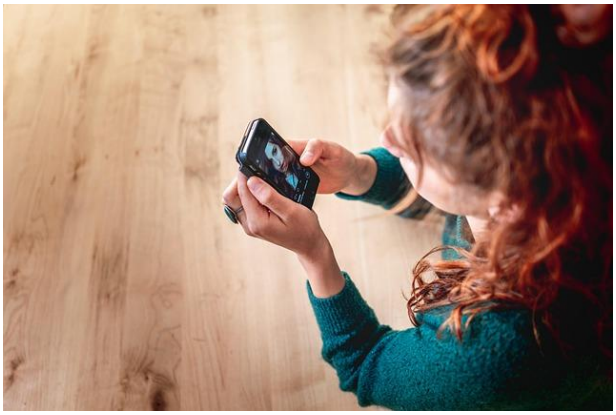
Here's the trap, most people believe they'd recognise a scam when they see one. But scams today are crafted to not look suspicious. More to the point, scams are often designed not to be seen at all. You could have it happen and not notice a thing! They're clever, believable, and often look like they came from someone you trust. That's not bad luck, that's design.

And when people say, 'I've never been hacked'? I always ask, are you sure? Because by the time you realise something's wrong, it's usually far too late. There are many attacks that could, for example, steal your password and you wouldn't even know.

Real Examples That Hit Close to Home

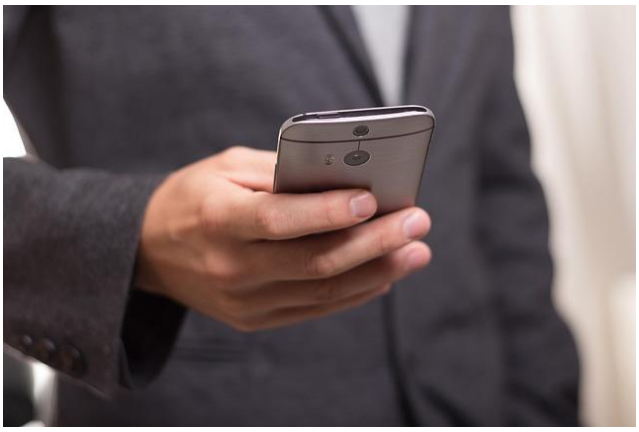
These are not rare edge cases these are the kinds of stories I hear and see all the time. Consider these for example:

The Hacked Message



A woman gets a Message from her 'daughter' saying she's lost her phone and needs money urgently. She transfers €400 before realising it was a scam. It looked completely real same profile photo, same tone of voice, even the same nickname she always used. The message said her daughter had changed phones and couldn't access her banking app. "Please just send it now, I'll explain later," it read. In the panic of the moment, the mother didn't stop to question it. She later found out her daughter's real phone was never lost the entire message came from a scammer who had spoofed her identity.

The Shared Information



A man shares regular updates on social media, photos of his dog Max, birthday wishes from friends, the name of his local football club, check-ins at his favorite coffee spot. It all seems innocent. But over time, someone is quietly collecting these details. One day, his account locks him out and asks security questions: pet's name, favorite team, birthdate. The attacker knows them all, because the man unknowingly handed them over one post at a time. He didn't click a bad link. He didn't fall for a fake login page. He just lived his life online and someone used it to walk through the front door.

It Is All Of Us

What connects these attacks and so many more? Simple, these are normal people doing normal things and paying the price for it. Its so easy to get scammed when we put our trust in the hands of strangers.

These aren't stupid mistakes. They're honest, human ones. And that's what makes them so dangerous. The more we trust technology, the easier it becomes to be tricked by it.

The Good News: You Can Still Take Control

Here's where it gets better, you don't need to be a tech wizard to protect yourself. You don't need to understand encryption or coding. You just need to be a little more aware and change a few habits. That's it.

Think of this like locking your front door. You don't do it because you expect a break-in. You do it because it's smart, simple, and it stops most of the trouble before it starts.

5 Cybersecurity Threats You've Probably Never Thought About (But Should)

1. Your Social Media Posts Are Helping Hackers Build Your Profile

We don't realise how much we give away.

A photo of your child blowing out birthday candles? That's not just cute that's a potential password clue: names, dates, pets, schools, even hobbies. All easily visible in your timeline.

Cybercriminals piece this information together like a puzzle. They don't guess your password. They calculate it based on your life.

Every "Happy Birthday, Liam!" or "Off to Galway for the weekend!" could be one more clue in the wrong hands.

Even more so its not always humans doing this. There are sophisticated and free pieces of software that do the collecting for the criminals.

2. Your Phone Passcode Isn't Private — You Type It in Public

We unlock our phones constantly, in shops, on buses, at work. But have you ever thought about who might be watching?

Your passcode is often the key to your digital wallet. Once someone sees you enter it, even once, they don't need your fingerprint. They just need a second of opportunity when you leave your phone behind, or it's stolen.

Most people don't lose money when their phone is hacked. They lose it when their phone is stolen and they made it easy. Whats worse is that people often re-use the same pin. It could be, and often is, be the pin number for your ATM card or house alarm!

3. QR Codes Are Often Dangerous

They're everywhere — in restaurants, posters, packages, ads.

But here's what most people don't know, a QR code doesn't show you where it's going. It could lead to a legitimate-looking site that quietly installs spyware or asks you to "log in."

And because it's a QR code, people don't question it. It feels clean, quick, modern. That's why hackers love it.

You wouldn't click a shady link in an email, but you might scan one stuck to a café table. Same trap, new packaging.

If you want to check this for yourself open your favorite search engine and search for QR code generator. See how easy this is!

Bonus Scare! Ok I shouldn't call it a bonus scare but here's something to make you think. If you did that and looked for a QR code generator now check out how easy it is to generate NFC Tags, or worse still clone them, or even worse again read from them!

4. Bluetooth: Your Invisible Risk

We think of Bluetooth as harmless background tech but it's a gateway.

When left on, your phone constantly broadcasts its presence to nearby devices. Hackers can exploit Bluetooth to connect, intercept data, or plant malware especially in public spaces like airports, malls, and conferences.

If you're not actively using a Bluetooth device, turn it off. Your phone shouldn't be shouting in a crowd.

Hackers don't even need to be close to you. They could be doing this from the other side of a busy restaurant! Or, even outside the building!

5. Your Browser Extensions Could Be Spying on You

That cute productivity tool you added to your browser? The one that organizes tabs or checks grammar?

Some of these extensions collect and sell your browsing data and worse, some have access to everything you type.

Even if the extension starts off safe, it could be sold to a shady company and updated silently to include tracking.

You locked your front door, but handed the keys to a stranger — because they offered to sort your tabs.

Thinking Time! If you don't understand tech and you get some new add on or plug-in because it makes your life easier, how do you know what it is doing. I am a developer and can tell you now that I can make a piece of software that says on your screen it is doing something but in the background could do ten other things you don't want done!

Here are five things you can start doing today

1. Think. If you don't understand it do you really need it!
2. Question. If you don't know how or why it does something, why are you letting it?
3. Never Trust. Always look for proof, always look for evidence and never take anything at face value.
4. Simplify. Don't bombard your life with tech that is making you not be able to think for yourself. Every thought removed from you is
5. Walk away. If if it doesn't seem right, you don't understand it and you don't need it then leave it alone. You will be better off without it.

What's Next?

This guide is just the tip of the iceberg. Now that you've seen how vulnerable daily life can be, it's time to go deeper. In upcoming guides, we'll walk you through deep, complex, brave, opportunistic, planned and many other types of cyber vulnerabilities and attacks that we all face every day.

Want the full series? Sign up on the website and get access to all future guides.

Quick Self-Check: Are You at Risk?

Answer honestly, if you say 'yes' to any of these, then you've already taken the most important step: awareness.

- Do you know the tech we use can also be used against you?
- Have you ever been denied access even though you are sure your username & password were correct?
- Have you ever clicked on a notification just so it will go away?
- Have you ever clicked a message, link or anything just because you were in a hurry or distracted?
- Have you ever let technology make a decision for you that you wouldn't make yourself?
- Have you ever thought, 'I'm not interesting enough to be hacked'?