CyberSec
15 Starter Tips

Tobias Sattler
tobiassattler.com | cybersec.help

Top Causes for Security Breaches

Malware

Insider Misuse

Digital Theft

Physical Theft

Social Engineering

Improper Disposal

You can prevent most security breaches by following these 15 starter tips.

#1 – Update your Software and Hardware

Unpatched software and hardware are a gateway for cybercriminals.

Turn on automatic system updates for your device. You may search for firmware updates manually as some do not support auto-updates.

Make sure your web browser uses automatic security updates.

Keep your web browser plugins and software updated, too.

#2 – Use Antivirus Protection and Firewall

Antivirus software blocks malware and other malicious code from entering your device and compromising your data.

Use trusted Antivirus vendors, only one tool on your device, and keep it up to date.

A firewall helps you defend against malicious attacks. Windows and macOS come with a built-in firewall.

Router often provides a built-in firewall, too. Check it out.

#3 – Apply Strong Passwords and use Password Manager

Use strong passwords: minimum 8 characters, lower- and uppercase, numbers, and symbols.

Password manager can help you to generate strong passwords and to organize your accumulated passwords.

Don’t use the same password for multiple accounts. If one gets leaked, the impact is substantially lower.

Do not share passwords or hints. If you have to, then make sure the connection is secure / encrypted.

#4 – Make use of Two-Factor or Multi-Factor Authentication

Adds a layer of security to the normal login process.

You have to enter an additional code, either a one-time password, personal code, or fingerprint.

Don't use SMS delivery for two-factor authentication, because it is not bug-proof, but still better than nothing.

Most platforms offer two-factor: Google, Amazon, Facebook, Instagram, Twitter, LinkedIn, GitHub, and many more.

#5 – Be aware of Phishing

Cybercriminals try to trick you into revealing sensitive information. That often leads to ransomware attacks or stolen credit card details.

Malicious links can come from friends who have been infected, too.

Be suspicious of the emails sent to you in general—check where they came from.

Don’t open emails and attachments from people you don’t know.

#6 – Protect your Personal Identifiable Information (PII)

PII includes information, such as name, address, phone numbers, date of birth, Social Security Number, IP address, location details, or any other physical or digital identity data.

Cybercriminals can steal your identity and use it for all kinds of fraud.

Be cautious about the information you share on the Internet.

Consider reviewing your privacy settings across all your social media accounts.

#7 – Encrypt your device

Hardware encryption is an essential tool to keep you safe.

Windows and macOS have a free built-in encryption. Linux has excellent tools, too.

Mobile devices usually come with hardware encryption by default. If you use an Android phone, you should manually check it.

Depending on your password and the encryption algorithm, cracking encrypted hardware is impossible by usual standards.

#8 – Use end-to-end encryption for communication

Only the communicating users can read their messages. It prevents potential eavesdroppers.

Most messengers now offer end-to-end encryption by default. However, you should check if group chats and VoIP calls are encrypted.

Email encryption is still not widely used, but essential especially in a business context. Setting up a GPG key is relatively easy.

If you check your emails, then encryption should also be considered. The IMAP and SMTP protocols offer a secure way, too.

#9 – Secure your Mobile Devices

More than 3 billion mobile devices worldwide are in usage.

Use a strong passcode—not your birthday.

Install apps from a trusted source, keep your device up to date, and back it up once in a while.

Check your privacy settings and be aware of your Personal Identifiable Information.

#10 – Backup your Data

Backups are essential for personal security. It's better to be safe than sorry.

Windows and macOS have a free built-in backup service. Linux has excellent tools, too.

If you lose your device or the device got destroyed, you don’t lose everything.

Follow the 3-2-1 rule for even more security. 3 copies of your data, 2 different types of media, and 1 copy in an offsite location (e.g., Cloud).

#11 – Don’t just throw it away

Disposal of hardware should be well thought out. Don’t just throw it away.

If you have transferred all data to a new device and made a backup, you can reset the old device to factory settings.

If you have sensitive data stored, you may consider scrapping it. Some companies shred the hard drives on-site.

You may consider reselling your hardware. In any case, hardware should be disposed of properly, as many parts can be recycled.

#12 – Trust is good, but don’t trust everyone

You meet new people, and during the small talk, you will be asked a lot about your business or personal things like your favorite color or movie, your first pet, etc.? Be cautious.

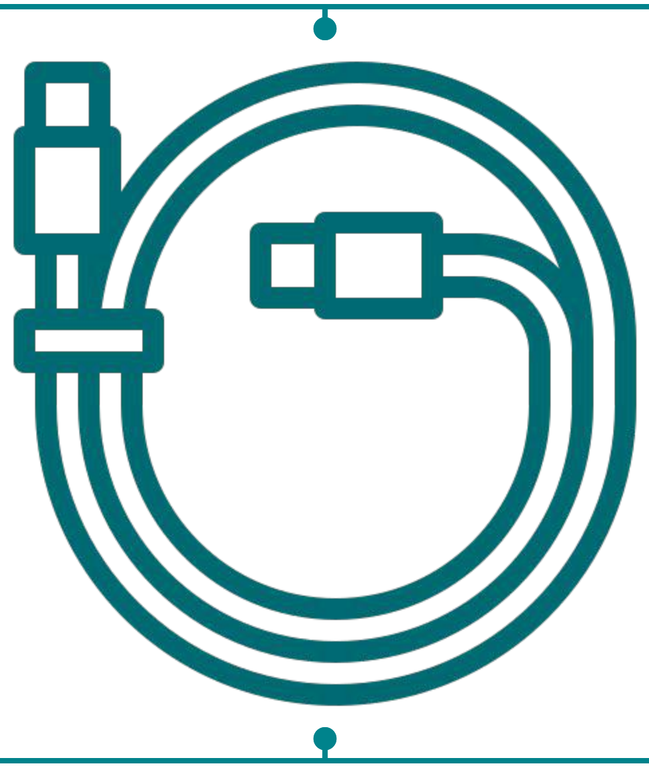
In social engineering, the attacker exploits the "human factor" as the supposed weakest link in the security chain to realize his criminal intent.

A classic example is the pretend system administrator who calls the employee because they supposedly need the user's password to fix a system error or security problem.

Use social networks responsibly. Think carefully about what personal information you disclose there, as it can be collected by criminals and misused for deception attempts.

#13 – Don’t use stuff that you don’t know

You ran out of battery, and you ask a stranger to lend you a battery charger or cable? Don’t do it.



While it is tempting to, cables, like the O.MG Cable, allow attackers to hack you.

You found a USB stick, and you want to check what is on it? Don’t do it.

That could be a trick to infect your device and network. Give the stick to a security expert for analysis.

#14 – Avoid Public Wi-Fi

Public Wifi can be helpful-especially abroad. However, don't use it without a Virtual Private Network (VPN) if you don't trust the provider.

Public Wifi is usually not encrypted. Therefore other devices can see your traffic.

Some Public Wifi are asking for personal information or billing data—be cautious.

Use your cell network if you don't have a VPN when security is vital.

#15 – Review your Data regularly

Check your online profiles and accounts once a year, and keep them up to date.

Delete old accounts that you no longer need or want.

Expiring credit card details or changes to your address can cause problems.

Check your credit card statement regularly to see if there are any movements you're not aware of.

In case something happened

There are no universal rules, because each case can be different. However, if you think that your affected in someway, then

1. Keep calm – it has happened to others
2. Get help from an expert to guide you
3. Inform your family and friends in case your private accounts or devices are affected
4. Inform your employer if your business could be affected
5. Monitor your financial and credit card details

Thank you!

See more on cybersec.help

References: (1) Icons made by Freepik (2) Cover made by TheDigitalArtist