10 cybersecurity best practices:

Cybersecurity best practices encompass some general best practices—like being cautious when engaging in online activities, safeguarding private information, and reaching out for help when you encounter something suspicious. Here's a deeper dive into the 10 cybersecurity best practices every internet user should know and follow.

1. Safeguard your data

In your daily life, you probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited phone call or text message. It's important to exercise the same caution online. Cybercriminals have been known to impersonate trusted websites or authorities to trick you into providing personal information by:

- Creating email addresses and websites that look legitimate
- Faking caller ID information
- Taking over company social media accounts and sending seemingly legitimate messages

It might sound obvious, but do your due diligence before sharing this information. Hackers can use this information to hack personal accounts (like bank accounts), sell on the deep web, or even commit identity theft.

However, you may need to be more careful than you think. For instance, if you share a picture online that shows a whiteboard or computer screen in the background, you could accidentally reveal information someone shouldn't see. Avoid oversharing on social media, and always check that a site requesting personal information is legitimate and secure.

2. Avoid pop-ups, unknown emails, and links

Beware of phishing. Phishers try to trick you into clicking on a link that may result in a security breach.

Phishers prey on internet users in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize. With just one click, you could enable hackers to infiltrate your entire computer network.

Here's a rule to follow: Never enter personal information in response to an email, pop-up webpage, or any other form of communication you didn't initiate. Phishing can lead to identity theft. It's also the way most ransomware attacks occur.

3. Use strong password protection and authentication

Strong, complex passwords can help stop cyberthieves from accessing your information. Simple passwords—think "12345" or your spouse's/child's name—can make access easy. If a cybercriminal figures out your password, it could give them access to your network or account information. Creating unique, complex passwords is essential.

It’s also a smart idea to change your passwords on a regular basis. Changing and remembering all of your passwords may be challenging, but a password manager can help.
Another way to protect your account access is by enabling multi-factor authentication. This adds an additional layer of protection by asking you to take at least one extra step—such as providing a temporary code that is sent to your smartphone—to log in.

4. Connect to secure Wi-Fi

Home Wi-Fi networks should be secure, encrypted, and hidden. You can add an additional layer of protection by using a virtual private network (VPN). A VPN is a service that provides online privacy and anonymity by creating a private network from a public internet connection.

Free public Wi-Fi networks in places like coffee shops can put your data at risk of being intercepted. A VPN encrypts your connection so your online activity, including the links you click or the files you download, can’t be accessed by cybercriminals or other snoops.

But keep in mind that some VPNs are safer than others. Norton Secure VPN provides powerful VPN protection that can help keep your information private, even when using public Wi-Fi.

5. Enable firewall protection

Having a firewall for your home network is the first line of defense in helping protect data against cyberattacks. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web.

Think of a firewall as a gatekeeper to your computer. You want to keep your sensitive data in and keep prying eyes and malware out. A firewall monitors network traffic and enforces rules about access set in conjunction with other layers of security.

6. Invest in security systems

Everyday internet users might hesitate when considering the cost of investing in a quality security system. That usually includes protections like:

- Strong antivirus and malware detection
- External hard drives that back up data
- A VPN to keep internet browsing private
- Parental controls
- Site screening to block fake sites that steal passwords
- A password manager to create, store, and protect strong passwords
- Regular system checks

Even though a quality security system can be expensive, all of the devices you use at work and at home should have the added protection of cybersecurity software. Get Norton 360 Deluxe to help protect your devices against the wide range of today’s cyber threats.

7. Update your security software and back up your files

Following IT security best practices means keeping your security software, web browsers, and operating systems updated with the latest protections. Antivirus and anti-malware protections are frequently revised to target and respond to new cyber threats.

You should also secure and back up files regularly in case of a data breach or a malware attack. Your most important files should be stored offline on an external hard drive or in the cloud.

8. Contact an IT professional

IT professionals are your friends in regard to all things cybersecurity. Reach out to your security provider or other trusted tech professional about information security.

It's a good idea to talk to IT if:

- You're troubleshooting a software or hardware issue
- You've received a security warning from your internet security software
- You plan on traveling and using public Wi-Fi

Remember to make sure IT is, well, IT. Beware of tech support scams. You might receive a phishing email from someone claiming to be from IT. Their goal is to trick you into installing malware on your computer or mobile device or providing sensitive data. Don't provide any information. Instead, contact your security service provider right away.

9. Read the Privacy Policy

It's not enough to practice good cybersecurity habits yourself—if you're shopping online or sharing private information with an individual or company, you should also ensure they're implementing the appropriate cybersecurity measures to keep your data safe.

If you're unfamiliar with a website or vendor, take a look at their website privacy policy to ensure their data privacy and protection process are compliant. This policy should list:

- The purpose of collecting personal data
- How and why that information may be shared
- Your rights regarding the processing of your personal data

If their privacy policy fails to provide this information—or if the site isn't able to provide you with a policy—your information likely isn't being sufficiently protected.

10. Embrace education and training

While cybersecurity software can protect against some cyberattacks, the biggest threat to your network is you—74% of data breaches are caused by human error and negligence, like misconfiguring databases or falling for a phishing scam. Take the time to educate yourself on the latest cybersecurity threats and best practices. Here are a few suggestions to help you stay on top of the evolving cybersecurity landscape:

- Subscribe to a tech newsletter
- Read up on local privacy and data protection regulations

- Follow your security provider on social media

A little technical savvy helps, too. Learning basic computer hardware terms, software skills, and security components can save time when you contact support, and they need quick access and information to resolve an issue.

Only you can help prevent cyberattacks

Knowing these cybersecurity basics can help strengthen your breach vulnerabilities. Remember: Just one click on a corrupt link could let a hacker in.