

Protect Against Cyber Attacks

Cyber incidents can be costly and time-consuming to correct. While every cyberattack is different, there are cybersecurity best practices in four key areas that can help keep your device, digital identity and personal data protected.

\$10.3 billion
in cybercrime
losses in 2022

SOURCE | FBI, Internet Crime Complaint Center
Releases 2022 Statistics, 2023

**74% of data
breaches include
the human element,
such as phishing**

SOURCE | Verizon, Data Breach Investigations
Report, 2023

**35% increase
in total data
breaches over the
past year**

SOURCE | Constella Intelligence, Identity
Breach Report, 2023

Here are several steps you can take to help avoid today's ever-changing cyber threats.

Ensure Password Hygiene



These rules apply to computers, mobile devices, online accounts, wireless routers, smart TVs, video doorbells and other smart home devices.

Create a strong password | Use at least 12 characters that mix upper- and lowercase letters, numbers and symbols.

Don't repeat passwords | Use a different password for every site and app, and do not use similar passwords across several sites.

Avoid auto-saving | Don't let your apps or web browser auto-save your passwords.

Multi-factor authentication | When possible, opt-in for two or more verification steps for logins to protect access to your information.

Safeguard Remote Work



Be hyper-vigilant when working or communicating from locations outside your home or work locations.

Avoid public Wi-Fi | Public Wi-Fi networks are easily compromised and spoofed by hackers, providing access to any device that connects so they can steal information or install malware.

Use a VPN | When you must connect to public Wi-Fi, use a virtual private network (VPN), especially when using mobile devices.

Lock your devices | Lock your device when you're not using it and protect it with a PIN, swipe pattern, fingerprint or facial recognition.

Avoid Social Engineering



Many data breaches start with social engineering attacks (such as phishing emails) that trick victims into clicking malicious links or infected attachment.

Check sender address, spelling and grammar | Unusual email addresses, as well as poor spelling and grammar, can indicate a phishing attempt.

Be wary of links | In emails, hover your mouse over the link to check the address. Avoid SMS links altogether.

Trust your instincts | If you're at all suspicious of a message, delete it or disconnect.

Research charity requests | Many unsolicited charity pitches online are scams. Do your research to make an informed, safe contribution.

Secure Software



Software is at the foundation of your digital security, including operating systems and apps.

Use authentic, licensed software | Free knock-off or pirated software often include malware. Get well-known software directly from a reputable source.

Update software | Install the latest patches and security updates to your OS and applications, and ensure your cybersecurity software is current.

Back up your data | Some cyberattacks delete or corrupt files. Create a full image backup of your system — including the operating system, boot media and applications — and store it on an external drive.

IdentityForce, a TransUnion brand, empowers consumers and organizations of all sizes to be less vulnerable to the financial and emotional consequences of cyber threats and identity crimes. For more information, visit identityforce.com.

ABOUT IDENTITYFORCE

IdentityForce, a TransUnion brand, offers proven identity, privacy and credit security solutions. We combine advanced detection technology, timely alerts, identity recovery services and 24/7 support with over 40 years of experience to get the job done. We are trusted by millions of people, global 1000 organizations and the U.S. government to protect what matters most.