

A silhouette of a person's head and shoulders is shown from the back, looking towards a bright rectangular light source, likely a computer screen. The person's hair is short and dark. The background is dark, and the light source creates a strong backlight effect.

10 Things You *Must* Do and 10 Things You *Can't* Do in Your Personal Cybersecurity Efforts

10 Things You *Must* Do in Your Cybersecurity Efforts

Protect Your Email Inbox: Email is ground zero for cyberattacks. When it comes to digital security, guarding your email inbox is paramount. This means never responding to suspicious emails and verifying the sender, especially when the email may contain important or sensitive information. Also, ensure your email has a strong, unique, password and you are using multifactor authentication.

Be Careful What You Download and Share: It is important to only download from trusted sources, especially when you are asked to download something from an email. Clicking on links or downloading attachments via email is a primary way that cybercriminals trick people and break into their accounts and/or steal their sensitive personal and financial information. Make sure you are only visiting trusted websites and if you get an email from a company asking you to click on a link to their website, navigate to the website yourself instead of trusting the link.

Use Strong Passwords and Multifactor Authentication: Use long, unique, complex passwords on all online accounts. This helps prevent credential stuffing and that a breach on a minor website doesn't impact critical accounts like your email or bank account. While strong passwords act as a first lock, multifactor authentication acts as a second level of protection. This requires a second device, authenticator, or physical security key to be accessed to enter the account, which would require a cybercriminal to have access to that as well.

Use a VPN, Especially When Traveling: A VPN (Virtual Private Network) is a service that scrambles your online data into unreadable code and routes it through a secure server, hiding your real location and digital activity. Using a VPN while traveling is important because it encrypts your internet connection to protect your data on unsecured public Wi-Fi networks. Airports, hotels, cafes, and train stations offer convenient public Wi-Fi, but these networks are often unencrypted and easy for cybercriminals to intercept. A VPN also stops snoopers from stealing your passwords, credit card numbers, and login credentials while using an insecure or public Wi-Fi network.

Beware of Quishing: Quishing is a relatively new and growing threat vector. It is when cybercriminals hide behind a QR code that you might see at a parking kiosk or restaurant. Be very careful when entering financial information or other personal information into a link from a QR code because it may be masking a malicious website designed to steal information such as a credit card number. People tend to trust QR readers, but like phishing websites or scam text messages, QR readers can often hide bad intentions.

Hang Up and Call Back: If you receive a phone call from a company or individual asking you to give up sensitive information, hang up and call the person or company back after you have verified the number. Remember that phone numbers can easily be spoofed. Also, AI-generated deepfake technology is improving and becoming more prevalent in social engineering attacks. This technology can be used to impersonate people, even loved ones that you know. Consider, especially with children, parents, or spouses, to establish a safe word that only you know in case someone uses deepfake technology to attempt to trick you into stealing money from you.

Avoid Sharing Sensitive Information via Email: You should avoid sharing sensitive information via email because standard email lacks end-to-end encryption and can be intercepted in transit across the public internet. Standard emails travel in plain text across multiple servers, making them vulnerable to

eavesdropping. Attackers can compromise email accounts, intercept messages, or breach receiving servers. Also, autocomplete mistakes, accidental "reply all" actions, or misaddressed messages can send private data to the wrong person. Major email providers can legally access or scan message content for spam, malware, or policy enforcement. Copies of emails and attachments also remain stored across multiple mail servers outside your control.

Never Overshare Online: It is important not to overshare online because exposing too many personal details puts your physical safety, digital security, and long-term reputation at serious risk. Posting real-time updates or photos while you are on vacation tells criminals your home is empty. Sharing your regular gym visits, running routes, or children's school lets strangers track your daily habits. Details like your first pet's name, your birthday, or the street where you grew up are often the exact answers used to reset your bank or email passwords. Criminals combine your public posts with data leaks to trick you with personalized phishing messages or fake investments. Once you post a photo or a message, it can be saved or screenshotted by others instantly. Even if you delete a post, platforms or search engines may keep copies on their servers. Embarrassing or overly personal details can resurface years later and hurt your job or school opportunities. This is especially true when it comes to children, and it is important to counsel them about these risks as well.

Monitor Bank Statements and Credit Reports: Monitoring your bank statements and credit reports is crucial to protect your money, catch mistakes, and maintain financial health. Monitoring your bank statements can help you find unauthorized charges or stolen card numbers early. It can also help you catch bank errors and help you spot incorrect fees, missed deposits, or wrong charges. Additionally, it can be a great way to track your spending habits and improve daily budgeting. Additionally, monitoring credit reports can help you spot identity theft and see if loans or credit cards have been opened in your name. It is a good idea to freeze your credit as well with the three credit bureaus (Equifax, Experian, and TransUnion) and to do so for children because children's credit can be stolen and it is often not noticed until a child becomes an adult.

Backup Critical Data: Data backup is the practice of making and storing extra copies of important files to protect against permanent loss, system failures, and cyber threats. Backups provide a safe way to restore files if malware or ransomware locks your main systems. Copies let you recover accidental deletions or overwritten documents. Hard drives fail and computers break, but a separate copy keeps your information safe. Offsite or cloud backups protect your files from local fires, floods, or theft. Cloud backups are useful but make sure you are protecting sensitive information with a strong password and multifactor authentication.

10 Things You *Can't* Do in Your Cybersecurity Efforts

Share Credentials with Individuals or Other Companies: Passwords should never be shared. This is especially true of software that holds critical or personally identifiable information (PII). Multifactor authentication should also be utilized on any applicable software, especially those holding critical data or information. Sharing credentials creates major security risks. Once you give a password to someone else, you may no longer control who sees your data. Every extra person who knows a password creates another chance for it to leak. Multi-factor authentication fails when multiple people use one login.

Reuse Passwords: Passwords, under no circumstances, should ever be reused. Passwords need to be unique. This is because if a password is discovered on one account, the same password will likely be tried on other accounts belonging to the user, making a leaked password (that has been reused) more valuable. Passwords must also be complex (using a combination of letters, numbers, and characters) as well as a certain length (at least eight characters long). This is because automated password crackers can crack simple passwords in seconds, making breaking into accounts with weak passwords effortless. Password management is critical for both organizations and individuals. It may be helpful as an individual to employ a password manager to help with password management.

Trust What You See Online: You should not trust everything you see online because anyone can publish unverified claims, and modern tools make fake media look completely real. Deepfakes allow individuals to create hyper-realistic fake videos, photos, and audio that mimic real people. If you see a deepfake, especially one designed to inflame (such as one with a political motive) don't share it. Meanwhile, much of the web is designed to sell products, push political views, or gain clicks rather than inform. And algorithms show you what you already like, which hides opposing facts and different viewpoints.

Respond to Suspicious Texts: You should not respond to suspicious text messages because any reply confirms to fraudsters that your phone number is active and monitored by a real person. Replying tells scammers your line is valid, which makes your number more valuable. Scammers often sell active phone numbers to other criminal groups. A simple reply allows fraudsters to build false trust and send more advanced phishing attempts. The safest choice is to ignore the text completely or use your phone settings to block the number.

Avoiding Software Updates on Devices: Keeping software up to date is essential for protecting your devices from security threats, fixing annoying bugs, and ensuring smooth performance. Developers find security holes and release fixes, called patches. Waiting to update leaves your device open to hackers and malware. Updates also remove glitches that cause crashes, freezing, or errors, making programs stable. New software versions often run faster and use system resources more efficiently. Updates bring new tools, updated designs, and better functionality to improve your experience. Regular updates keep your apps working properly with new operating systems and other connected devices.

Leave Your Devices Unlocked or Unattended in Public Spaces: Never leave your devices unlocked or unattended in public spaces because it exposes you to immediate physical theft, unauthorized data access, and severe account compromises. Anyone nearby can quickly read your private emails, browse personal photos, or copy sensitive files. Criminals can open banking or payment apps to steal money or transfer funds. An unauthorized person can send fake messages or emails from your accounts, damaging your reputation. A stranger can plug in a rogue USB drive to install malware or compromise the system in seconds, or a quick-handed thief can snatch your phone or laptop if you look away for even a few seconds.

Use the Same Email for Everything: Using one email address for all your online accounts creates a single point of failure that exposes your entire digital life to hackers if that inbox is compromised. Splitting your online presence across multiple email addresses is a fundamental necessity for modern cybersecurity. Gaining access to your main email means gaining access to your bank, shopping, and social media profiles. Small, unsecured websites often leak user databases, exposing your primary email address to criminal groups. Data brokers and marketing companies track your web activity by matching your unique email address across different platforms. A single email allows corporations to build a complete profile of your habits, purchases, and interests. Signing up for random newsletters or free trials floods your main inbox

with promotional junk. Scammers use leaked email lists to send convincing fake messages that mimic real services you use.

Stop Repeating the Basics: Cybersecurity seems complex, but it is deceptively simple. Often, the basics can thwart most cyberattacks. These basics include using strong passwords and multifactor authentication, updating software, protecting your personal and sensitive information, and avoiding clicking on links and downloading attachments. Focusing on mastering the fundamentals will go a long way to keeping you safe.

Stop Improving Your Cybersecurity Defenses: It is safe to say that the bad guys are constantly refining their methods of attack. Therefore, you must never get complacent. You must be aggressively working to harden your personal digital defenses.

Don't Be a Reactive Victim: This statement is not made to scare you. However, it is a reality. It's not a matter of *if* but *when* you are involved in a cyber incident, whether it is caused by a third party losing your information, falling for a scam, or accidentally sharing information you shouldn't have. It is going to happen at some point. That is why it is critical to move from reactive practices to proactive practices. Prepare now for a digital incident so you are not caught flat-footed when it does occur.



www.prestigepeo.com