10 CYBER SECURITY TIPS

Hacking, phishing, and malware incidents are becoming the number one cause of security breaches today. But, what's more troubling, these hacking attempts are the result of human errors in some way. Education and awareness are critically important in the fight against cybercriminal activity and preventing security breaches.

1. Keep Your Software Up to Date

- Turn on automatic system updates for your device
- Make sure your desktop web browser uses automatic security updates
- Keep your web browser plugins like Flash, Java, etc. updated

2. Use Anti-Virus Protection & Firewall

Anti-virus (AV) protection software has been the most prevalent solution to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data. Use anti-virus software from trusted vendors and only run one AV tool on your device.

Using a firewall is also important when defending your data against malicious attacks. A firewall helps screen out hackers, viruses, and other malicious activity that occurs over the Internet and determines what traffic is allowed to enter your device. Windows and Mac OS X comes with their respective firewalls, aptly named Windows Firewall and Mac Firewall. Your router should also have a firewall built in to prevent attacks on your network.

3. Use Strong Passwords & Use a Password Management Tool

You've probably heard that strong passwords are critical to online security. The truth is passwords are important in keeping hackers out of your data! Choose something that is easy to remember and never leave a password hint out in the open or make it publicly available for hackers to see

- Reset your password when you forget it. But, change it once per year as a general refresh.

4. Use Two-Factor or Multi-Factor Authentication

Two-factor or multi-factor authentication is a service that adds additional layers of security to the standard password method of online identification. Without two-factor authentication, you would normally enter a username and password. But, with two-factor, you would be prompted to enter one additional authentication method such as a Personal Identification Code, another password or even fingerprint. With multi-factor authentication, you would be prompted to enter more than two additional authentication methods after entering your username and password.

5. Learn about Phishing Scams – be very suspicious of emails, phone calls, and flyers

A few important cyber security tips to remember about phishing schemes include:

1. Bottom line – Don't open email from people you don't know
2. Know which links are safe and which are not – hover over a link to discover where it directs to
3. Be suspicious of the emails sent to you in general – look and see where it came from and if there are grammatical errors
4. Malicious links can come from friends who have been infected too. So, be extra careful

6. Protect Your Sensitive Personal Identifiable Information (PII)

Personal Identifiable Information (PII) is any information that can be used by a cybercriminal to identify or locate an individual. 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.

7. Use Your Mobile Devices Securely

According to McAfee Labs, your mobile device is now a target to more than 1.5 million new incidents of mobile malware. Here are some quick tips for mobile device security:

1. Create a Difficult Mobile Passcode – Not Your Birthdate or Bank PIN
2. Install Apps from Trusted Sources
3. Keep Your Device Updated – Hackers Use Vulnerabilities in Unpatched Older Operating Systems
4. Avoid sending PII or sensitive information over text message or email

8. Backup Your Data Regularly

Backing up your data regularly is an overlooked step in personal online security. The top IT and security managers follow a simple rule called the 3-2-1 backup rule. Essentially, you will keep **three** copies of your data on **two** different types of media (local and external hard drive) and **one** copy in an off-site location (cloud storage).

If you become a victim of ransomware or malware, the only way to restore your data is to erase your systems and restore with a recently performed backup.

9. Don't Use Public Wi-Fi

Don't use a public Wi-Fi without using a Virtual Private Network (VPN). By using a VPN, the traffic between your device and the VPN server is encrypted. This means it's much more difficult for a cybercriminal to obtain access to your data on your device. Use your cell network if you don't have a VPN when security is important.

10. Review Your Online Accounts & Credit Reports Regularly for Changes

With the recent Equifax breach, it's more important than ever for consumers to safeguard their online accounts and monitor their credit reports. A credit freeze is the most effective way for you to protect your personal credit information from cyber criminals right now. Essentially, it allows you to lock your credit and use a personal identification number (PIN) that only you will know. You can then use this PIN when you need to apply for credit.