i7 Technologies

10 Top Security Tips

1. Keep Your Software Up to Date

One of the most important cyber security tips to mitigate ransomware is patching outdated software. This includes operating systems, applications and network device firmware updates. This helps remove critical vulnerabilities that hackers use to access your devices. Here are a few quick tips to get you started:

- 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
- Check router settings and make sure it either notifies you or is set to automatically update

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. Both Windows and Mac OS X come 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! According to the National Institute of Standards and Technology's (NIST) password policy framework, you should consider:

- A minimum of eight characters and a maximum length of at least 64 characters.
- The password should contain at least one lowercase letter, one uppercase letter, one number, and four symbols but not the following &%#@_.
- Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa).
- Restrict context specific passwords (e.g. the name of the site, etc.).
- Restrict commonly used passwords (e.g. p@ssw0rd, etc.) and dictionary words.
- Don't use the same password twice.
- 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
- Restrict sequential and repetitive characters (e.g. 12345 or aaaaaa).
- Restrict context specific passwords (e.g. the name of the site, etc.).

If you want to make it easier to manage your passwords, try using a password management tool or password account vault. Most antivirus suites on the market today include this tool. Make sure you know how to recover your passwords if your password manager fails.

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.

According to NIST, an SMS delivery should not be used during two-factor authentication because malware can be used to attack mobile phone networks and can compromise data during the process.

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

Phishing scams are here to stay and get more prevalent every year. In a phishing scheme attempt, the attacker poses as someone or something the sender is not to trick the recipient into divulging credentials, clicking a malicious link, or opening an attachment that infects the user's system with malware, Trojan, or zero-day vulnerability exploit. This often leads to a ransomware attack. In fact, 90% of ransomware attacks originate from phishing attempts.

A few important 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!
5. If you're unsure, call the company or the friend and question the email.

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. You would be amazed perhaps even frightened at the amount of information someone can gain just from your phone number!

In the new "always-on" world of social media, you should be very cautious about the information you include online. It is recommended that you only show the very minimum about yourself on social media. Consider reviewing your privacy settings across all your social media accounts, particularly Facebook. Adding your home address, birth date, or any other PII information will dramatically increase your risk of a security breach. Hackers use this information to their advantage!

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. Make sure your device has a lock screen timeout
3. Install Apps only from Trusted Sources
4. Keep Your Device Updated – Hackers Use Vulnerabilities in Unpatched Older Operating Systems

5. Avoid sending PII or sensitive information over text message or email
6. Leverage Find my iPhone or the Android Device Manager to prevent loss or theft
7. Perform regular mobile backups using iCloud or Enabling Backup & Sync from Android

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 VPN software, 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. Most antivirus companies offer a VPN service either as part of a package or an addon.

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

Data breaches seem to be more common place than ever. With Norton Lifelock, LinkedIn, T-Mobile, Microsoft and Facebook among the larger more recent companies breached 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.

Top Causes of Security Breaches

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.

Need help understanding the information or guiding you through securing your network and devices? Contact us either by phone or email.

(208) 518-9379
contact@i7tech.net
www.i7tech.net