Security Habits of Effective PC Users.

Posted At : March 31, 2014 8:23 AM | Posted By : Admin
Related Categories: Internet, Social Media, Security, Hewlett Packard

You might not think about it when you're browsing the web, shopping online and interacting on social media, but you are the first line of defense against cyber security risks. The power to be safe is in your hands and at your fingertips. Developing and maintaining good habits can make online activity much safer and more enjoyable for you and your colleagues.

Here are a number of good habits take only minutes to learn and are easy enough to incorporate into your daily work life.

Create strong passwords
Passwords are usually the first, and sometimes only, protection against unauthorized access. They are the keys to your online kingdom, so keep these guidelines in mind.

- Many websites will let you know whether your password is safe when you're in the process of creating it. Pay attention to that, and if the site indicates that your password is weak or not secure, create a better one.
- Do not use your name, common phrases or words or acronyms that can be found in the dictionary—including foreign languages.
- Avoid prefixing or suffixing your password with numbers or using known keyboard patterns like "Qwerty2."
- Stop making sense. Create passwords that use a variety of letters, symbols and cases so you're less predictable to hackers and password-cracking systems.
- Use a random-password generator app like **1Password** to create and store unique passwords.

For more information on passwords and password management, see our article "**Create safer passwords**."

Lock your computer screen
You never know who might use your computer when you're not around, so it's important to lock your screen to prevent unauthorized access. In the office, a co-worker, guest or a service provider might view or use your unattended computer. This is an easy way for private information to become public.

It only takes a few seconds to lock your PC. Just press the Ctrl+Alt+Delete keys and then select the option "Lock this computer." For your smartphones and tablets, use the passcode feature, as

these devices are just as vulnerable as your PC.

Secure mobile devices from loss
While mobile devices such as smartphones, tablets and laptops are valued for their portability, this convenience can become a security risk. It's easy to lose or misplace these devices, so be sure to:

- Make a list of phone numbers and email addresses to report stolen or lost devices
- Use a hardware cable lock for your laptop, or store it in a locked drawer
- Keep smartphones and tablets with you when in public
- Never put devices in your checked baggage when traveling

Protect data on mobile devices and removable media
Mobile devices and removable media, such as USB drives, enable us to easily share and transport information, but can lead to the loss or misuse of data. Although it's important to protect the actual devices themselves from loss, it's equally important to protect the information they contain by:

- Turning on and accepting software updates
- Creating regular backups of important data
- Erasing all data before you discard, donate or give away a device
- Encrypting all data, if possible
- Using anti-virus software and keeping it up-to-date

Identify URLs before clicking
Simply stated: think before you click. A malicious website that looks legitimate is a common method used by criminals. However, verifying the real destination is easy—just place your cursor over the displayed URL, and the true destination will reveal itself with a small pop-up. Don't click if it looks suspicious.

For URL shorteners like tinyurl.com and bit.ly, simply add a plus sign (+) to the end of the URL to display its true source. For QR codes, choose a reader app that allows you to preview the destination before opening the link. And when it comes to mobile apps and software, download from a trusted source, like Google Play, Microsoft.com or Java.com.

Use public Wi-Fi safely
Public Wi-Fi is riskier than corporate or home Wi-Fi because you can't determine its setup and security features. So, take extra precautions when using it.

- Do not access sensitive personal accounts, such as financial accounts
- Ensure websites use HTTPS and display a lock icon
- Watch out for “shoulder surfing” from people and security cameras
- Never use a public computer, such as one in a hotel lobby, to access personal information
- Use only for general web browsing, e.g., weather forecasts and restaurant reviews

Think before you post to social media

Social media provides a convenient, fun way to stay in touch with friends and family. But be cautious about what you post. Understand both personal and business risks, and take the following precautions:

- Always comply with your company’s rules for business conduct
- Ask friends and family to keep your personal information private, including relationships
- Be cautious about participating in games and surveys or clicking on links suggested by others
- Review and update your social media privacy and security settings often

Use daily

Bad habits might die hard, but good habits can protect you from cyber threats. You are the first line of defense in protecting yourself, your colleagues and your devices against security risks. And as criminal methods and tactics are becoming more advanced, it’s more important than ever to establish and maintain good security habits.