Cybersecurity: Make It a Habit!

October 2017

Every new cyber-attack or scam seems to be accompanied by a barrage of cybersecurity tips, pointers, dos and don’ts that we’re expected to follow to keep ourselves and our families safe and secure. While sometimes specific tips and awareness messages are important, it’s easy to get overwhelmed and tune it all out.

One way to simplify cybersecurity is to focus on just a handful or two of good habits that can help protect you across a variety of situations. Good habits are the foundation of cybersecurity just as they are for safety and security in the physical world -- like locking your front door or wearing your seat belt in the car.

Here are eight important cybersecurity habits to incorporate into your online life. They will help to protect you, your information, your family, and your work against a wide variety of cybersecurity threats. They'll also reduce your risk of getting scammed! Try to make these habits automatic.

1. Always think twice before clicking on links or opening attachments. Sometimes all it takes is that extra split second to realize that you might be being tricked.

2. Verify requests for private information (yours or anyone’s), even if the request seems to come from someone you know. Con artists know how to fake their identity.

3. Protect your passwords. Make them long and strong, never reveal them to anyone, and use multi-factor authentication (MFA, also called 2-step authentication) wherever possible. Also use different passwords for university and non-university accounts.

4. Protect your stuff! Lock it up or take it with you before you leave, even if you’ll only be away for a second. And password protect all of your devices.

5. Keep a clean machine! Keep your devices, apps, browsers, and anti-virus/anti-malware software patched and up to date*. Automate software updates and restart your devices periodically to ensure updates are fully installed.

   → Find out what you need to do, if anything, for devices managed for you*

6. Back up critical files. Store backups in a physically separate location from the originals, and test them periodically.

7. Delete sensitive information when you are done with it. Better yet, don’t store it in the first place if you don’t need to.

   → UC employees: Follow the UC records retention schedule.

8. If it’s suspicious, report it!

Icons for Habits #1, 2, 4-7 by VisualPharm, licensed under Creative Commons BY (version unknown). Endorsement not implied.
For more detail about any of these habits, please visit
https://security.ucop.edu/resources/security-awareness/habits.html

Please visit UC’s Information Security Awareness website for additional cybersecurity-related
information and resources: https://security.ucop.edu/resources/security-awareness/index.html