Cybersecurity: Make It a Habit!

UNIVERSITY OF CALIFORNIA

Information Security Awareness

Good habits are the foundation of cybersecurity just like 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. Try to make these habits automatic. They will help protect your information, your family and your work. They'll also reduce your risk of getting scammed!

1. Always think twice before clicking on links or opening attachments.

- Even if they look like they're from someone you know.
- Whenever possible, go to web pages by a path you know is legitimate instead of clicking on a link in a message.
- If an attachment is unexpected, contact the sender by a method you know is legitimate to confirm they sent it.

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.
- Check your financial statements and credit reports regularly.

3. Protect your passwords.

- Make them long and strong.
- Never reveal your password to anyone.
- Use different passwords for different accounts.
- Use different passwords for work and non-work activities.
- Click "no" when websites or apps ask to remember your password.
- Use strong authentication where possible, such as multi-factor authentication (MFA), fingerprints, and tokens.

4. Protect your stuff! Lock it up or take it with you before you leave.

- Secure your area and lock your computer screen before leaving them unattended – even just for a second.
- Take your phone and other portable items with you or lock them up.
- Password protect all of your devices. Use strong authentication where possible.

security.ucop.edu

5. Keep a clean machine! Keep your devices, apps, browsers, and anti-virus/anti-malware software patched and up to date*.

- Automate software updates.
- Restart your devices periodically.
- *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.
- For critical work files, use storage options that are approved by your UC location and are backed up regularly
- For personal files, save a backup copy of anything critical on a separate hard drive, data stick, CD/DVD, etc., and store it securely.
- Test your backups periodically.

7. Delete sensitive information when you are done with it.

- Follow UC's records retention schedule.
- Better yet, don't store it in the first place if you don't need to.
- UC definitions of sensitivity levels: security.ucop.edu/policies/

8. If it's suspicious, report it!

- Report suspected scams and other suspicious activity to your supervisor, and follow your location's reporting protocol.

For more information visit security.ucop.edu

Credits:

Icons for Habits #1, 2, 4-7 by VisualPharm (http://icons8.com/), licensed under Creative Commons BY (version unknown) (https://creativecommons.org/licenses/by/4.0/). Endorsement not implied.