Being Proactive On Cybersecurity

You’ve read the headlines, organizations big and small, including even large retailers and mega companies, are not immune to data breaches and hackers’ increasingly sophisticated schemes. But you can protect yourself from becoming victims by staying vigilant.

Technological protections alone are not always enough - incorporate good cybersecurity habits into your daily routine.

Sometimes you can do everything right and still fall victim. Numerous data breaches at well-known companies have affected millions due to no fault of the people impacted. In addition, natural disasters are often followed by a wave of scams, such as phony donation websites.

Practice these three tips to protect yourself from the unexpected:

1. Review your bank and credit card statements monthly. This is often the first place you will see signs of identity theft. If you think you may be a victim of identity theft, see the identity theft resources here for help;
2. Back up your critical files – store backups in a physically separate location from the originals, and test them periodically;
3. Always think twice before clicking on links or opening attachments, this is the best way to protect yourself against scammers. 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 he or she sent it.

Additional cybersecurity awareness information and resources are available on UC’s Information Security Awareness website: https://security.ucop.edu/resources/security-awareness/index.html

Good Cybersecurity Habits
Here are simple habits that can help protect your information, privacy, pocketbook, family, friends, and work:

1. Always think twice before clicking on links or opening attachments;
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 (also called two-step authentication) wherever possible;
4. Protect your stuff! Lock it up or take it with you before you leave, 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.