Putting Security into Cybersecurity

Americans are spending more time online, but our increasing dependence on technology creates opportunities for cybercriminals to take advantage of gaps in security and personal knowledge.

To help our members and others interested in online safety, we spoke to Geoffrey Floding, SECU Vice President of Threat Intelligence, for tips and advice on personal cybersecurity. Geoffrey discusses the popular cybercrime techniques and how to identify them, how to protect yourself and your family, and what to do if you think you have become a victim.

Question: Are there common techniques cybercriminals use?
Geoffrey: Phishing emails are a cybercriminal's most popular attack method. This technique seeks to acquire sensitive data or access to a computer by either engaging the victim directly, or by tricking the victim into clicking a link or opening a document. These emails can appear as if sent from a legitimate business.[1] In the last year we have seen criminals also use text messages and phone calls to trick users into installing software on their computers or giving them their personal information.

Question: Are there immediate ways to spot cybercrime?
Geoffrey: Please be cautious if an email, text, or phone call asks for personal information or access to your computer systems. Individuals should always validate who they are dealing with and be careful about what they share.

Question: What can people do to protect themselves against cybercrime? Can I do anything to protect my family, like an elderly parent?
Geoffrey: The best anyone can do is remain vigilant, only click on links from or respond to individuals that the user knows or is expecting and communicate this strategy to your family. Just as you would not give information to a stranger over the phone, you should not give information over email or text message. It is also important to remember that a legitimate company or service will never ask you for your password.

Question: How do we start to teach kids about staying cyber-safe today?
Geoffrey: Letting kids know that, regardless of the medium, they need to keep their personal information private and not overshare online is essential. The U.S. Cyber Security and Infrastructure Agency (CISA) has published a **list of tips and recommendations for parents** with some additional links for more information.

Question: How do I know if I am a victim of cybercrime, and what should I do if I think I have been attacked?
Geoffrey: If you suspect you are a victim of a cybercrime, either by having unknown charges show up on a bank statement, or having your identity used without your knowledge, it is best to contact the Credit Union immediately. Contact information and resources are available to members on the **State Employees' Credit Union website**.

SECU
State Employees' Credit Union®

In addition to these suggestions, the Cybersecurity & Infrastructure Security Agency offers four steps everyone can take.

- **Think Before You Click! Recognize and Report Phishing**: Think before you click if a link looks a little off. It could be an attempt to get sensitive information or install malware.
- **Update Your Software**: Do not delay—act promptly if you see a software update notification. Better yet, turn on automatic updates.
- **Use Strong Passwords**: Use long, unique, and randomly generated passwords. Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- **Enable Multi-Factor Authentication (MFA)**: You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.

[1] *Editor, C. S. R. C. C. (n.d.). Phishing - glossary: CSRC. CSRC Content Editor. Retrieved from csrc.nist.gov*

SECU
State Employees' Credit Union®