THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

July 2022

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

Cybersecurity Awareness Month

Although October is a few months away we wanted to kickoff the months leading up to Cybersecurity awareness month (#BeCyberSmart) with the first of four topics that are being raised this year. In this month's newsletter we want to go over the shared responsibilities we all have in Cybersecurity, because it isn't only a cyber security team's responsibility; it is an individual responsibility. If everyone does their part – implementing strong security practices, raising awareness, and educating folks - our interconnected world will be safer and more secure for everyone.

Cybersecurity Responsibility

It's everyone's job to know and perform basic cyber best practices.

- Use long and unique passphrases for all accounts.
- Don't use the same password everywhere.
- Never share your password with anyone
- Don't put passwords on sticky notes, use a password manager instead.

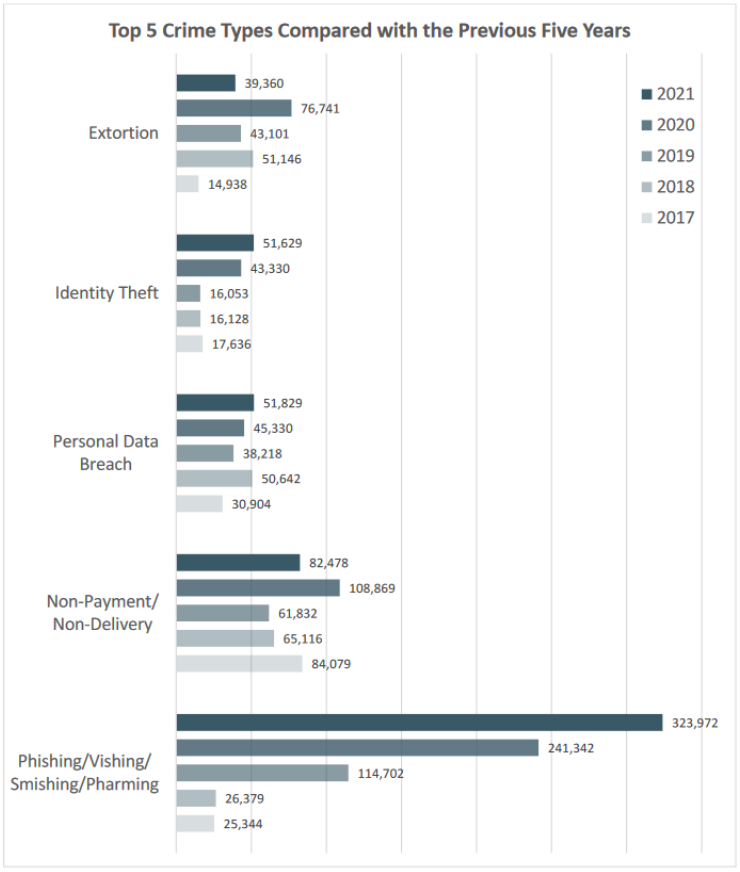
- Enable multi-factor authentication wherever possible.
- Ensure that security software updates are being done to the computing platforms and applications you are using.
- Ensure that backup copies of your data both on and offsite are validated.

Make cybersecurity a priority no matter where you are:

AT WORK	AT HOME
• Build security into your products and processes	• Consider security when purchasing internet-connected devices
• Train employees on security during onboarding and equip them with the tools they need to keep the organization safe	• Update seucurity/privacy settings and change the default passwords as soon as you turn on a new connected device

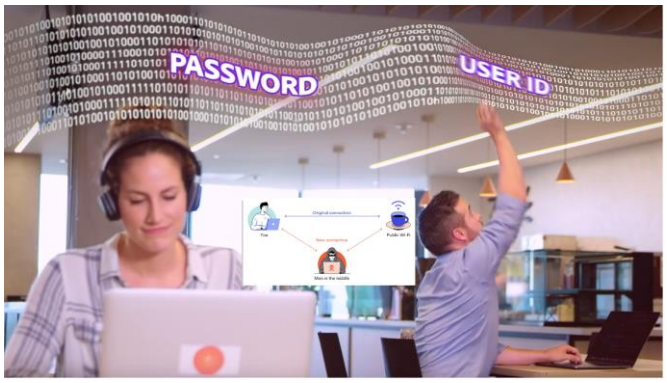
- Only use technology from trusted sources
- Share sensitive information only with those who have a need to know
- Don’t share personal or company information with unknown, unfamiliar, or untrusted sources
- Always Report suspicious e-mails or suspicious calls to security
- Encrypt e-mails that have sensitive information with #encrypt at the start of a subject line.
- Think before you click – e-mails, tweets, texts, posts, social media messages and online advertising are gateways for revealing sensitive information.

FBI Statistics

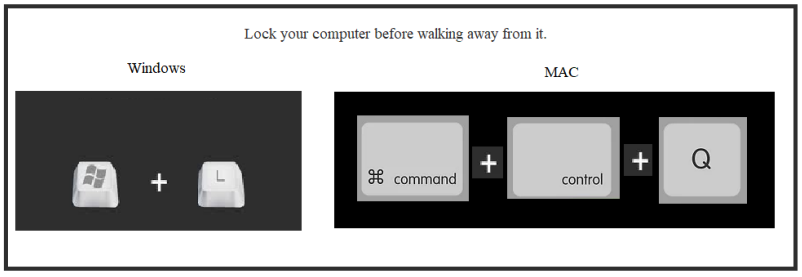


- Report lost or stolen computers immediately to security@bsd.uchicago.edu
- Never turn off or uninstall security tools
- Never leave your computer unattended in public places
- Ensure you have antivirus software installed [The BSD uses CrowdStrike]

- Only download files from verified trusted source
- Never send sensitive information over an unsecure free Wi-Fi.



- Check your configuration, privacy, and security settings whenever you sign up for any services, download a new app or get a new device.
- Always lock your computer before walking away from it.



We want our everyday technology to be reliable, predictable and worry free from interruption and issues as much as possible. Following security best practices can help prevent incidents that throw a wrench into our daily lives. If you have any questions about any of the best practices above, please contact security@bsd.uchicago.edu We are more than happy to help.