NEED TO KNOW NEWSLETTER | OCTOBER 2024

Cybersecurity Awareness Month 2024

October is Cybersecurity Awareness Month. Private companies and government agencies unite to raise awareness on cybersecurity topics critical to protecting your safety online.

This year, Cybersecurity Awareness Month focuses on four topics to create the best recipe for cybersecurity success: recognizing and reporting phishing, using strong passwords and a password manager, updating software and enabling multi-factor authentication (MFA).

Strong passwords

The key to a successful password is creating something easy to remember but hard to guess. Incorporate a favorite quote, a song title or a favorite sports player into your password, and it becomes more complex.

A password manager app provides a secure vault for all your passwords. You only have to remember the password for the app itself, allowing you and your computer to access the rest of your passwords for all your logins.

Multi-factor authentication

To guard data and protect against password exploitation, many organizations and commonly used applications are implementing MFA, or multi-factor authentication.

In computer security, an authentication factor is anything that you use to authenticate yourself with a system. A password, for example. With MFA, you use two or more different factors to log in: for example, a password and a verification code sent to your smartphone.

If one of your factors is stolen, the thief still doesn't have the other factor and can't access your account. The more factors you use or the stronger the factor, the better your security.

Phishing

Phishing can be catastrophic for organizations. Phishing attacks make up 44% of social engineering incidents and Some of the most-clicked phishing emails are disguised as corporate communications, such as emails about performance reviews and approval of documents. These phishy emails have an average click rate of 10-20%! Hackers use email address spoofing to make the email look like it is being sent from an internal or trusted source.

To avoid falling for a phishing email that looks like it is from your organization, go straight to the official source to authenticate the message. For example, if it looks like an email from Human Resources, go to your organization's Human Resources page to view the information and avoid the link in the email.

Automatic updates

Hackers can exploit vulnerabilities in unpatched software. When new software updates come out, it allows everyone, especially hackers, to learn about those weaknesses and take advantage of anyone who hasn't updated yet. Public knowledge of those holes leaves you and your organization easy prey.

Updating or patching your software means you are less vulnerable to security risks. If an update becomes available on your device, update it promptly. Better yet, enable automatic updates so your phone or smart device never gets left behind!

Exciting new gadgets? Keep it on the down-low

Getting a new gadget is always exciting, but be careful how much you share about it. Hackers know about Internet of Things (IoT) devices and how to access them. Be sure to follow best practices when firing up these new toys. Change the default passwords, check all security settings and keep it up-to-date to safely enjoy your devices.