National Cybersecurity Awareness Month

CYBERSECURITY AWARENESS MONTH

Every October is National Cybersecurity Awareness Month. Private companies and government agencies come together to raise awareness on cybersecurity topics critical to protecting your safety online. This year, National Cybersecurity Awareness Month focuses on four topics: recognizing and reporting phishing, using strong passwords and a password manager, updating software and enabling multi-factor authentication (MFA)

Recognizing and reporting phishing emails

Cybercriminals sent over 3.3 billion phishing messages and caused over 4,000 data breaches, exposing over 22 billion personal records. But it isn't enough to simply know that phishing emails are out there; you also need to be able to recognize and report them. Knowing the types of phishing emails will help you quickly identify and report fake and dangerous emails. Often used phishing emails are

- urgent messages
- log-in or password messages
- free gift messages
- internal messages

If you think you may have encountered a phishing email, follow your company's procedures for reporting. Whatever you do, do not click on any links, reply to the email or send it to anyone else!

Using strong passwords and a password manager

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

You always hear about creating a secure password, but how do you keep your secure passwords secure? A password manager app can help you remember (or forget) passwords.

A password manager is a secure vault for all your passwords — like a glorified password notebook but a lot more secure! You only have to remember one password, allowing you and your computer to access the rest of your passwords for all your logins.

Updating software

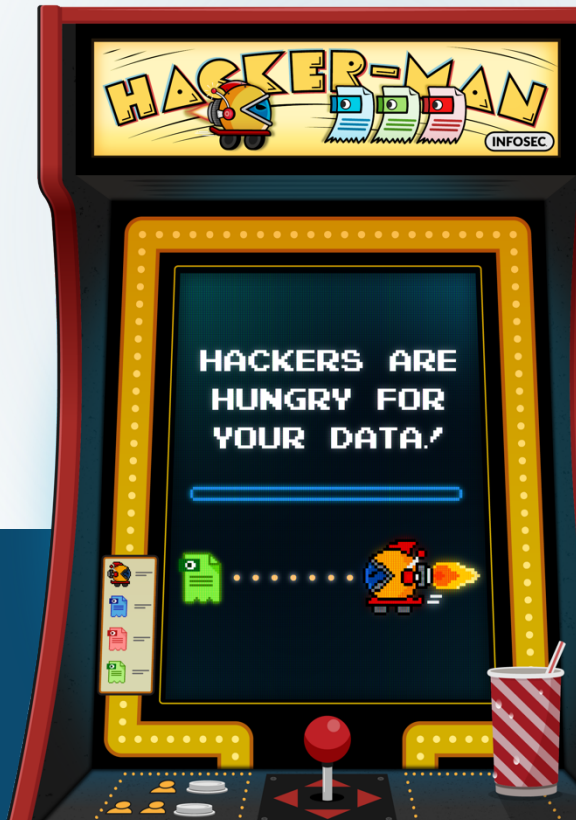
Hackers can exploit vulnerabilities in unpatched software. When new software updates come out to the public, it allows everyone, especially hackers, to learn about those weaknesses and take advantage of them. Public knowledge of those holes leaves you and your organization as easy prey.

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 your phone or any other smart device to auto-update.

Enabling multi-factor authentication

In computer security, an authentication factor is anything you use to authenticate yourself with a system. Using a password is the most common type of authentication. With multi-factor authentication (MFA), you use two or more different factors to log in.

One example is a password and a verification code sent to your smartphone. This is an extra layer of security, so even if one of your factors is stolen, the hacker doesn't have access to the other authentication factor. This stops them from accessing your account.



For more information on National Cybersecurity Awareness Month, visit https://staysafeonline.org/programs/cybersecurity-awareness-month/