October 2020 - Cyber Security Awareness Month

What is Cyber Security Awareness Month?

Cybersecurity Awareness Month is observed every October and was created as a collaborative effort between government and industry to ensure every person has the resources they need to stay safer and more secure online. This initiative was started 17 years ago by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance to raise awareness about the importance of cybersecurity.

Join the IT Department the first 4 Friday afternoons through the month of October to discuss topics on Cyber Security Awareness.

Each week, we'll be highlighting a different aspect of cyber security and answering all your questions you may on the weekly topic.

When: First 4 Friday afternoon's in October

Time: 1:00PM - 1:30PM

Where: Zoom Click here to join meeting

Why: To empower individuals and organizations to own their role in protecting their part of cyberspace.

5 Ways to be Cyber Secure at Home

Simple Tips:

1. Treat business information as personal information. Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.
2. Don't make passwords easy to guess. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches.
3. Be up to date. Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it and set your security software to run regular scans.
4. Social media is part of the fraud toolset. By searching Google and scanning your organization's social media sites, cybercriminals can gather information about your partners and vendors, as well as human resources and financial departments. Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms.
5. It only takes one time. Data breaches do not typically happen when a cybercriminal has hacked into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages immediately.

INTERESTING FACTS & FIGURES

An estimated $6 trillion will be spent globally on cybersecurity by 2021

On average after a breach, company share prices fall 7.27%

It takes companies nearly 6 months to detect a data breach

77% of organizations do not have a cybersecurity response plan

95% of cybersecurity breaches are due to human error

By 2020 there will be roughly 200 billion connected devices

95% of breached records came from only three industries in 2016

There is a hacker attack every 39 seconds

The average cost of a data breach in 2020 will exceed $150 million

The number of cellular Internet of Things (IoT) connections is expected to reach 3.5 billion in 2023 – increasing with an annual growth rate of 30%. (Ericsson)

Gartner forecasts that 25 billion connected things will be in use by 2021. (Gartner)

Once plugged into the internet, connected devices are attacked within 5 minutes and targeted by specific exploits in 24 hours. (NETSCOUT)

Weekly Topics

Week 1 - Taking Stock (October 2)

This week, we'll take stock of all our devices and remind ourselves why they're so important to us and why we need to appreciate them.

You can start by taking stock of your own cyber security knowledge by taking the following Get Cyber Safe Assessment checkup.

Get Cyber Safe Assessment Checkup.

Week 2: Phone Week (October 9)

Your precious phone! During the COVID-19 pandemic, you have probably spent even more time with your phone than you usually do. Whether you want to connect with your family, browse through photos, or scroll through social media, your phone is there when you need it. Now let's take some time making sure it's properly secured.

This week, we will give you key tips you can use to keep your phone and the information on it safe and sound, including:

- Updating your OS
- Avoiding smishing scams
- Enabling multi-factor authentication

Week 3: Computer Week (October 16)

As much as we love our phones, we still use the good old-fashioned laptop or desktop (especially if you've been working from home).

This week, we'll show you how to show your computer you care by teaching you to:

- Create complex passphrases
- Prevent against malware
- Avoid phishing scams

Week 4: Network Week (October 23)

Network devices may not be as flashy as phones or computers. Nobody is waiting in line for the latest router but they serve an important function. They connect you to everything!

This week, you'll learn all about how to:

- Set up a secure Wi-Fi network
- Use Wi-Fi safely

Resources

Global Knowledge - Cyber Security Free Training

Cyber Security Terminology - Cheat Sheet

Security Awareness Quiz - Working Remotely