Cybersecurity Awareness Month

Cybersecurity Awareness Month

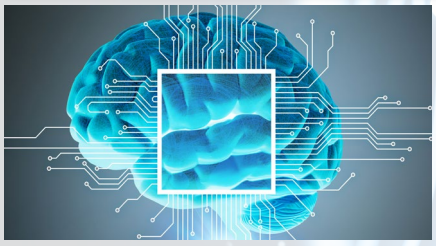
Office of Information Technology / Division of Information Security

OCTOBER 2021 **WEEK 1**

Be Cyber Smart!

Week of October 4, 2021
Be Cyber Smart!
Week of October 11, 2021
Fight the Phish!

Week of October 18, 2021
Cyber Security Career Awareness Week
Week of October 25, 2021
Cyber Security First



DID YOU KNOW?

An estimated 300 billion passwords are used by humans and machines worldwide.

Source: https://www.crn.com/news/channel-programs/log-mein-poor-or-reused-passwords-responsible-for-83-per-cent-of-breaches

What Does It Mean to be Cyber Smart?

It means you engage in behaviors to keep your information safe from attackers and other bad actors who want to do you harm. Sometimes you can measure the harm, like in financial attacks where money is stolen from your bank account or you find that your credit card information has been compromised.

Other kinds of harm can't be measured, such as if someone impersonates you online and acts in a way that could damage your reputation. Maybe they asked your friends and family for money, or found private correspondence or images and released them to your colleagues.

GOOD HABIT 1

Make your social media profiles more private. Learn more here.

GOOD HABIT 2

Back up IHS files to the network drive. Do not use unapproved offline or cloud storage for IHS data.

!!REMEMBER!!

You have to be right all the time; crooks only have to be right once!

Be Cyber Smart!

At Home

GOOD HABIT 3

Make sure your personal devices stay up to date on relevant security patches.

GOOD HABIT 4

When using GFE, only use pre-approved removable media.

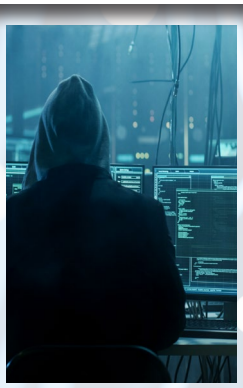
Network Smart

A well-protected home network means that your family and guests can use the Internet safely. Manage your network so you and your guests can connect to the Internet securely and reliably:

- Buy your own router; don't use the router your ISP provides.
- Update any default passwords so they are strong, easy to remember, and hard to guess.
- Use antivirus scans on a regular basis.
- Check the router manufacturer's website each month for updates.
- Turn off your network if you will not use it for an extended period, such as when on vacation.
- Check for unauthorized device connections.

DID YOU KNOW?

1 out of every 3 homes in the US with a computer is infected with malware.
Source: https://www.dhs.gov/be-cyber-smart/facts



DID YOU KNOW?

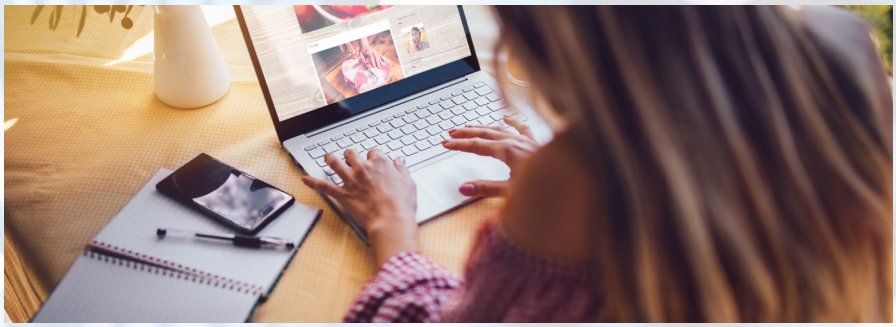
Human intelligence and comprehension is the best defense against phishing attacks.
Source: https://www.cybintsolutions.com/cyber-security-facts-stats/

!!REMEMBER!!

The IRS is specific about how it contacts you for tax purposes. Learn more here.

Be Cyber Smart!

Online



GOOD HABIT 5

Don't access sites from email links. Use your Web browser to enter the address.

GOOD HABIT 6

Disable auto-complete for online forms and don't let your browser remember passwords.

GOOD HABIT 7

Keep your antivirus software up to date!

INTERNET SMARTS

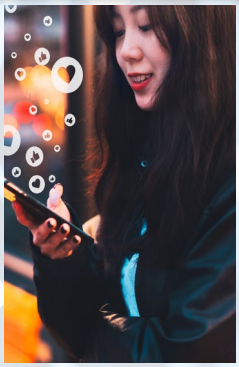
When using the Internet, you really can't be too careful; what they don't know, can't hurt you. This includes any time you make a purchase, access social media, or complete a form that requests your information.

Tips and Best Practices

DO NOT click on an enticing link when shopping.
DO visit the merchant's site by typing the Web address.
DO NOT use a debit card, if possible.
DO use a credit card, which offers much better protection for your purchases.
DO NOT share private details on social media; they can be used to guess account passwords.
DO create complex passwords that are easy for you to remember, but hard for others to guess.

DID YOU KNOW?

Every single day, 600,000 Facebook accounts are hacked.
Source: https://www.dhs.gov/be-cyber-smart/facts



DID YOU KNOW?

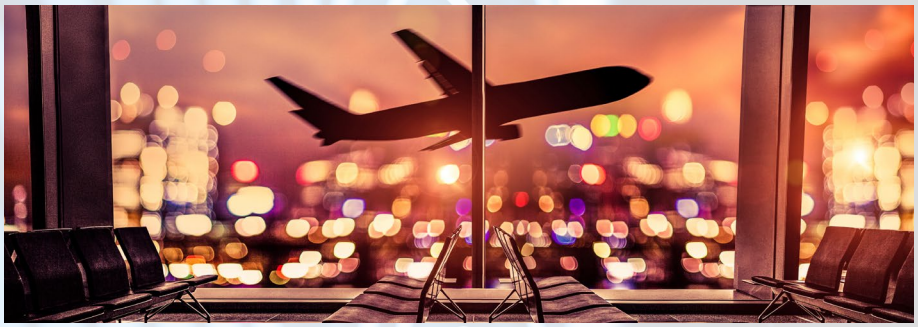
Data breaches exposed 36 billion records in the first half of 2020.
Source: https://www.itpro.com/security/357578/exposed-records-top-36-billion-in-2020-so-far

!!REMEMBER!!

IHS executives are not going to send you requests for money. Verify all requests.

Be Cyber Smart!

On Travel



GOOD HABIT 8

Keep your device from connecting automatically to wireless networks by following these steps.

GOOD HABIT 9

Do not use personal details in passwords, like names or birth dates. Don't reuse the same password across multiple accounts.

GOOD HABIT 10

Keep software versions current to protect against newly discovered vulnerabilities.

Why Practice CYBERSECURITY While Traveling?

Reasons to practice cybersecurity while traveling:

Thwart device theft - Keep devices securely on you or with people/in locations you know and trust at all times.
Avoid cyber terrorism - Prevent cyber hackers from illegally using your data and network for political use.
Evade financial attacks - Keep malicious persons from stealing credentials to financial accounts, including credit card and bank accounts.
Mitigate hacking - Make it harder for criminals to gain access to your laptop, smart phone, or other devices.
Discourage shoulder surfers - Using a privacy screen on mobile devices can keep wandering eyes from capturing information about you while you browse.

BLUETOOTH SECURITY

Cyber criminals have the ability to pair with your device's open Bluetooth connection and steal personal information.
Disable your Bluetooth connectivity!

HERE'S A TIP!

Sharing your current location and excessive details on social media makes you an easy target for criminals online and in real life. Wait until you return home to post about your travels to prevent revealing that you are away from home. Protect yourself, your loved ones, and your property.

!!REMEMBER!!

Stop and think before you connect to any public wireless network!!!