# National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

Office of Information Technology / Division of Information Security

OCTOBER 2020

WEEK 1

## Cybersecurity - The Silent Threat

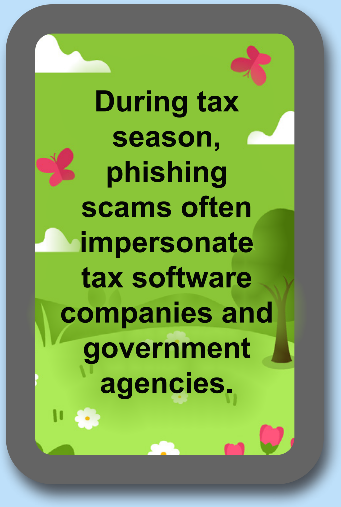
### MYTH-BUSTERS

There are many cybersecurity myths that persist that can put our personal and IHS data at risk. This article attempts to dispel some cybersecurity myths you might encounter.

**MYTH: IT staff have completely secured my computer and sensitive data. I am fully protected while at work and on my government issued computer.**

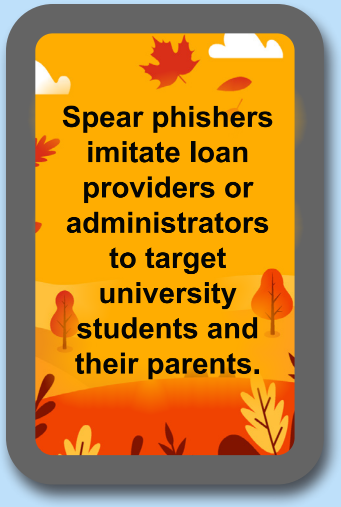
IHS IT personnel do all they can to protect IHS data, computers, and employees. They have implemented technical security safeguards such as virus scanning, firewalls, automated patching, email/web filtering and much more; however, hackers continue to target individuals through social engineering, which can bypass existing IHS technical security controls. Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of our natural tendencies to be helpful and our emotional reactions.

**REALITY:** While technical controls like anti-spam filters, intrusion detection/prevention systems, anti-virus software, and firewalls are good at keeping out some threats, they aren't designed to stop social engineering attacks. Here are some real world social engineering scams:



During tax season, phishing scams often impersonate tax software companies and government agencies.

Phishing emails frequently reference sporting events like the World Cup or the Olympics.



Spear phishers imitate loan providers or administrators to target university students and their parents.

Year after year, phishing scams exploit Black Friday and the holiday shopping season.

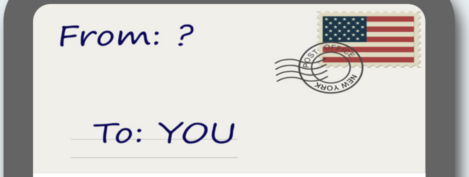
**MYTH: Phishing scams are easy to spot.**

Not long ago, phishing attacks were fairly easy for the average person to spot because they were full of grammatical and spelling errors, and linking to phony bank or email logins at unencrypted (http:// vs. https://) websites. Phishers are now certainly upping their game, polishing their language and hosting scam pages over https:// connections complete with the lock icon in the browser address bar to make the fake sites appear more legitimate.

**REALITY:** Many phishing attacks try to convince you that you need to act quickly to avoid some kind of financial loss or pain, usually by clicking a link and “verifying” your account information, username/password, etc. at a fake site. Emails that emphasize urgency should always be considered suspect. Sometimes, phishers use familiar names and actual personal details in their messages. Phishing scams are becoming more sophisticated and no topic is off limits, even COVID-19 themes.

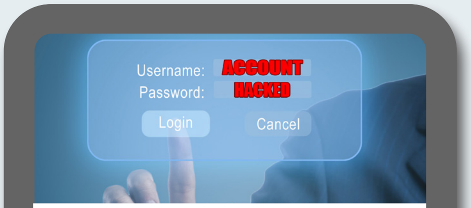
## If you receive an email that evokes strong emotion, BE CAUTIOUS!

***Look out for other characteristics that indicate this may be a phishing email.***



It’s from an unknown sender.

The email is unsolicited.



It asks to verify your password or account information.

**MYTH: The WiFi network I am on requires a password, so it is secure.**

Even if a WiFi network requires a password, it can still be dangerous. At retail establishments, the password is often available to just about anyone. An attacker on the same WiFi network could attempt to capture your account credentials and access your files and information. Wait to do more serious tasks like bill paying, accessing your bank account, or using your credit card for when you’re safely connected to your home network or tethered to your smartphone hotspot, where you’re a lot less likely to be targeted by scammers.

**REALITY:** There are plenty of free WiFi networks but unfortunately many of them are unsecure (even with a password). Although the owners of these networks have good intentions, they sometimes put their customers in harm’s way.

## Tips for Staying Safe on Public WiFi

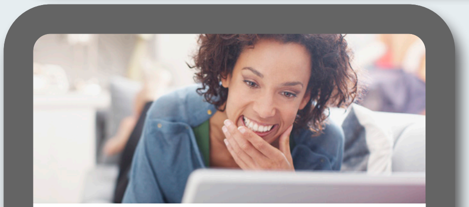
- Avoid sensitive transactions like banking.
- Maintain anti-virus protection.
- Use a VPN.
- Keep software updated.
- Have strong passwords.

**Remember, no Public WiFi is 100% secure!**

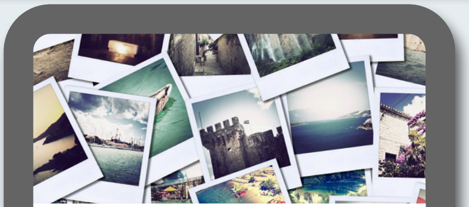
**MYTH: My friends showing up on social media won’t hurt me.**

The great thing about social media is that it connects you with your friends and relatives. Unfortunately, this web of connectivity can be a gateway for deception. Take this possible scenario - your friend has a weak password, and their account becomes breached. The hacker sends you a direct message that appears to come from your friend. The message is a link for a funny video or news article to read. Since the link appears to be coming from your friend you have known for years, you let your guard down and click the link. After all, you’re aware of phishing scams when you get a message from someone you’ve never heard of, but you don’t have that on your mind when you are contacted from a “friend.”

**REALITY:** Hackers depend on us to lower our guards so their scams work. Once they have gained our trust, they then can strengthen their foothold and use it as a jumping off point for more attacks. Here are some tips to keep your data safe:



Be cautious when you receive suspicious emails from your contacts - old or new.



Remember that information can be stolen from photos or videos you post.

DAILY NEWS
No. 48,725
THE BEST SELLING NEWSPAPER IN THE WORLD
Today's Edition
National · World · Business · Lifestyle · Travel · Technology · Sport · Weather
BREAKING NEWS

Don’t post anything that you wouldn’t want on the front page of a newspaper.

**MYTH: I use a complex password so my account is secure.**

Using a strong password is important, but even the strongest password isn’t a guarantee of your safety in today’s cyber landscape. Nowadays, there are speedy programs hackers can use to run billions of password combinations to see if they can get a username/password combination to work.

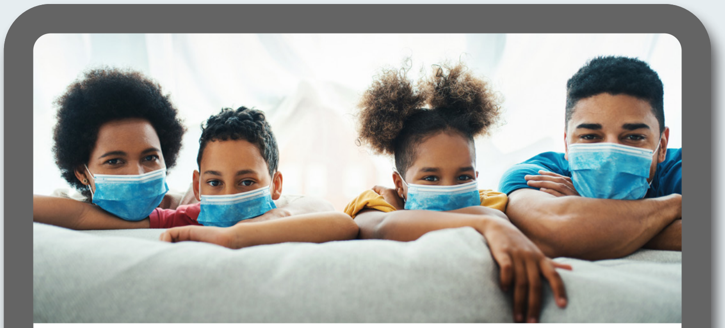
**REALITY:** Even though many cyber criminals have high-tech tools at their disposal, the stronger your password is, the more likely they are to move on to easier targets. Consider using a password manager to keep your passwords complex and secured. If the service or account offers two-factor authentication, take advantage of it whenever possible. Make sure you change your passwords regularly and do not use the same password across multiple accounts. The following table illustrates the time it takes for a hacker to break your password using brute force tactics.
(Source: https://www.hivesystems.io/blog/are-your-passwords-in-the-green)

| Number of Characters | Numbers Only | Lower Case Letters | Upper & Lower Case Letters | Numbers, Upper & Lower Case Letters | Numbers, Upper & Lower Case Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | 1 Second | 5 Seconds |
| 7 | Instantly | Instantly | 25 Seconds | 1 Minute | 6 Minutes |
| 8 | Instantly | 5 Seconds | 22 Minutes | 1 Hour | 8 Hours |
| 9 | Instantly | 2 Minutes | 19 Hours | 3 Days | 3 Weeks |
| 10 | Instantly | 58 Minutes | 1 Month | 7 Months | 5 Years |
| 11 | 2 Seconds | 1 Day | 5 Years | 41 Years | 400 Years |
| 12 | 25 Seconds | 3 weeks | 300 Years | 2,000 Years | 34,000 Years |
| 13 | 4 Minutes | 1 year | 16,000 Years | 100,000 Years | 2 Million Years |
| 14 | 41 Minutes | 51 Years | 800,000 Years | 9 Million Years | 200 Million Years |
| 15 | 6 Hours | 1000 Years | 43 Million Years | 600 Million Years | 15 Billion Years |
| 16 | 2 Days | 34,000 Years | 4 Billion Years | 37 Billion Years | 1 Trillion Years |
| 17 | 4 Weeks | 800,000 Years | 100 Billion Years | 2 Trillion Years | 93 Trillion Years |
| 18 | 9 Months | 23 Million Years | 6 Trillion Years | 100 Trillion Years | 7 Quadrillion Years |

## TOP CYBERSECURITY FACTS FOR 2020

- 94% of malware is delivered via email.
- Phishing attacks account for more than 80% of reported security incidents.
- $17,700 is  lost every minute due to phishing attacks.
- 60% of breaches involved vulnerabilities for which a patch was available but not applied.
- 63% of companies said their data was potentially compromised within the last 12 months due to a hardware or security breach.
- Data breaches cost enterprises an average of $3.92 million per year based on a 2019 report.
- Attacks on internet of things (IoT) devices tripled in the first half of 2019.
- Malicious software attacks that do not rely on files and leave no footprint to detect grew by 256% over the first half of 2019.
- 40% of IT leaders say cybersecurity jobs are the most difficult to fill.
- The Federal Bureau of Investigation reported a 300% increase in reported cybercrimes in the United States since the outbreak of COVID-19.
- More than 93% of healthcare organizations have experienced at least one data breach over the past three years.

(Source: www.csoonline.com)



## DO WE NEED CYBERSECURITY AWARENESS AT HOME?

Now more than ever, we understand the importance of safety, both online and in the real world. The coronavirus epidemic has forced millions of families across the globe to adopt social distancing and rely on their internet-enabled devices to communicate with the outside world, friends and family.

As schools now become increasingly virtual, students have turned to online classes and other means of communications with their teachers and classmates. It’s not just parents who need to adapt to the new work-from-home environment and threat landscape.

The Internet can provide a wide range of fun activities and educational materials for children but, as kids surpass their parents in tech savviness, their digital profiles can easily become a target for cyber criminals.

Learning the basics of good cyber hygiene should not have an age limit. While you monitor what apps and games your toddler accesses, it might be harder to keep an eye on teens and their online activity. More screen time can come with a price. It is important to teach your young ones about their digital profile and how they can stay safe while perusing the web. This includes what they say in the presence of passive listening devices like Alexa, Echo, and Cortana.

Teach your kids to use anonymous screen names and strong passwords, and to be aware of fishy emails. Help your kids protect their digital lives by providing them with the tools to use the Internet respectfully and responsibly as adults. It is an opportunity not only to ensure kids grow up to avoid the challenges their parents faced in the early years of the Internet, but also to be the change we want to see online.

**For more information on how you can Do Your Part, #BeCyberSmart, visit www.cisa.gov/ncsam**