CYBERSECURITY AWARENESS MONTH 2021

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

October is Cybersecurity Awareness Month. A time to focus on defending ourselves and our company from cybercrime and vampires. This year's theme is focused on being #CyberSmart, which means having the know-how to make smart decisions when it comes to cybersecurity.

Being cyber smart isn't just the responsibility of our IT providers and shouldn't be a challenging goal to achieve. Completing simple daily habits with an emphasis on putting cybersecurity first can help keep our lives scam-free.

So don't let cybersecurity scare you! Building a strong foundation of knowledge and keeping your wits about you can help anyone claim the title of being #cybersmart.

Help Samantha swipe right to find her a cyber-smart date to the company's Fall Formal.

TUCKER

Anti-virus Status:
Unsure?

Password habits:
I have one strong passphrase set for each of my accounts.

Who protects a company from cybercrime?
The Government.

Tucker shines with a strong password, but he does reuse this password across all accounts. That's a big no-no! He's also is unaware about his devices' anti-virus status.

Mario thinks it's only IT's job to protect the company from cybercrime. He also shared his password on a dating platform. Not cool, Mario.

MARIO

Anti-virus Status:
All of my devices have anti-virus

Password habits:
I've got the best password. It's MarioCart8!

Who protects a company from cybercrime?
The IT department

Cyber Swipes

FRANK

Anti-virus Status:
Only set up on work devices.

Password habits:
I use unique passwords and phrases for all accounts.

Who protects a company from cybercrime?
I'm responsible for myself.

Frank doesn't protect the devices he uses outside of the office. Personal devices work-from-home devices should have the same protection, as well.

Gary uses a password manager, has anti-virus protections on all his devices and takes the protection of data seriously. What a dreamboat!

GARY

Anti-virus Status:
All set up and ready to go.

Password habits:
My password manager handles everything for me.

Who protects a company from cybercrime?
It's everyone's responsibility to protect data!

Samantha wants to be cyber smart in picking a date. Who do you think she should go with?

MAKING A #CYBERSMART DECISION BY PUTTING CYBERSECURITY FIRST

Without the know-how to make smart decisions when it come to cybersecurity you could potentially find yourself in some pretty scary situations! So to avoid taking the lead role in your own Cyber Horror Picture Show, review theses SPOOKY cyber scenes, and their correlating #CYBERSMART action points.

SCENE 1: THE CALL IS COMING FROM INSIDE THE HOUSE

Your phone rings. The caller ID display shows a number eerily similar to your own. Is the call coming from inside the house? You pick up on the third ring... The line is silent... Suddenly, you hear "Your car's warranty has expired..."

#CYBERSMART ACTION PLAN:

You hang up! Chills running down your spine, as you worry about the safety of your four door hatchback. You quickly call your provider directly using a verified number.

SCENE 2: MEAT PIES AND WI-FI

You and your co-worker have lunch together at a local restaurant renowned for their splendid meat pies. Your co-worker wanted information about the upcoming company holiday party, so you take out your phone, and see that you can connect to "Sweeny's Wi-fi Service".

#CYBERSMART ACTION PLAN:

Avoid connecting to the restaurant's free Wi-Fi or any other unsecured hotspots you may see. Use your own trusted hotspot or VPN, or try saving your searching activities until you return to work.

SCENE 3: JASON'S WORK STATION

It's 3:00pm on Friday the 13th. Your Co-worker, Jason, is leaving early for a hockey game. You notice he is downloading information onto a USB hard drive before heading out. "It's just so I can catch up on work this weekend. It's no big deal."

#CYBERSMART ACTION PLAN:

Inform Jason that he needs approval first before downloading onto an unapproved personal device. If he refuses, inform your supervisor yourself as this may be a violation of company policy. Approach these situations delicately and avoid confrontation if you don't feel safe.

ARE YOU AFRAID OF THE DARK ... WEB?

There are many dangers out there on the Dark Web, don't get us wrong. But, there are still some good things that occur on the dark web as well. Let's run through some of the good, the bad and the ugly when it comes to the Dark Web.

The Dark Web has many legitimate, non-nefarious uses. Many users from foreign countries use the tool to communicate when free speech and internet use is heavily scrutinized by their government.

Breached data is commonly put up for sale on the dark web following an attack. Using the built in privacy features of the Dark Web, cybercriminals can buy and sell your data to be used against you in future scams.

Ransomware as a Service and Phishing-as-a-Service have appeared more recently on the Dark Web. These solutions offer pre-made kits designed to make any newbie scammer initiate ransomware like a veteran.

SCAM OF THE MONTH

Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Katie turned on the television one morning and saw the devastating news about an earthquake that affected a foreign country. Katie wanted to help and donate to the relief efforts. She searched "Earthquake Donation" on her favorite social media site and clicked on a crowdfunding page that asked her to provide her credit card information, address, and other personal details. **The page then mentioned she could be eligible for tax credits but needed to enter her government identification number, which she did.** The next day her bank called to report the suspicious activity. They were able to reverse her original donation, but her exposed government identification number put her in grave danger of future scams. She needed to put a credit freeze on her account which inhibited her from purchasing her dream home.

Did you spot the red flags?

- Katie searched for a charity on social media and selected a crowdfunding page.
- Katie gave out far too much information in the online form.
- Katie failed to do any research to determine if this charity was reputable or not.

Charity scams have become very common, especially after natural disasters that make the news or during the holiday season when the giving spirit is in full swing. Be cautious with crowdfunding pages and do your research. While there are many reputable charities that are responsible with their donations, there are others that were created by scammers with the sole purpose of stealing information and funds from generous givers.

Along with fake web pages, watch for unsolicited phone calls, as well. Scammers commonly pose as reputable charities in an effort to collect your donation quickly over the phone. Beware of pressure tactics by the caller encouraging you to act now. Try hanging up and visiting the charity's website directly to donate securely or use a charity verification resource that may be provided by your government.

Make sure your money gets to the people that need it the most. Be diligent about researching reputable charities to make sure you are donating securely.

Key Takeaways

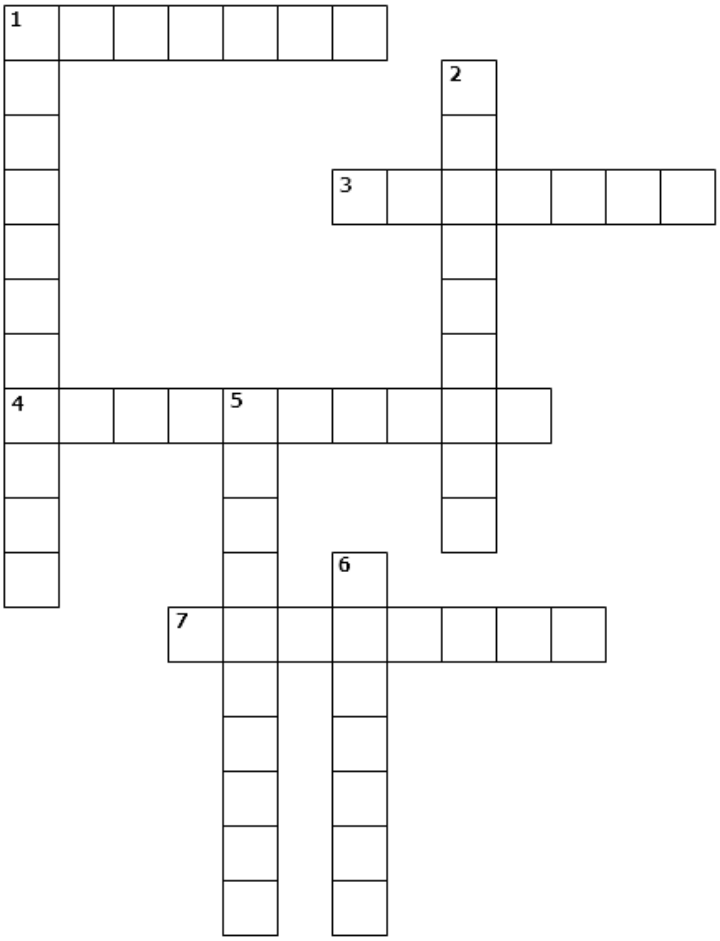
It doesn't take a genius to be cyber-smart. Taking the time to think through your daily actions can have a major impact on keeping your company data, and your own personal information, safe and secure.

Do your part, #becybersmart. When you make cybersecurity a priority, it becomes easier to see where others can make smarter decisions in their own cyber life.

The Dark Web gets a bad rap for being a community where cybercrime can thrive. But many good-intentioned people use the tool for communication purposes outside of their controlling countries.

Charity scams increase in volume after natural disasters and during holiday seasons. Do your homework on any charity before dipping into your wallet for a donation.

A Cybersmart Crossword



ACROSS

1. Many scammers try to set up fake ones of these to steal from giving people.
3. Use this instead of public Wi-Fi to keep your data safe.
4. Being this, means having the know-how to make smart decisions when it comes to cybersecurity.
7. Katie tried making one of these to a charity after the recent earthquake.

DOWN

1. Many individuals use the Dark Web to do this positive purpose to let their voices be heard.
2. To best protect your computer from feeling sick, make sure you have this up and running to block security threats.
5. This is being sold as a service for anyone to purchase on the Dark Web.
6. A platform built for privacy, this seedy corner of the internet still has some non-nefarious uses.

Across: 1. Charity 3. Hotspot 4. Cybersmart 7. Donation Down: 1. Communicate 2. Antivirus 5. Ransomware 6. DarkWeb