# CYBERSECURITY AWARENESS MONTH

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


## THIS MONTH'S TOPICS:



October is Cybersecurity Awareness Month. The intent is to promote awareness of cybersecurity topics to consumers, small and medium-sized businesses, corporations and more.

The benefits of this global campaign are to continue to educate the community on cybersecurity threats. As this education spreads, we as a collective team become more informed and reduce our chances of becoming a victim of cybercrime.

Use the enclosed information to help reinforce the tips and skills you've learned from previous lessons while also learning some new emerging threats to be aware of. And don't be shy in spreading some of the knowledge you are gaining with friends and family - we all must be cyber-smart.

# Top Cybersecurity Myths

Cybersecurity can be a tough subject to master. To help, let's examine some of the common misconceptions that need to be debunked.



**Small & medium-sized businesses aren't targeted by cybercriminals.**

A majority of data breaches happen at small businesses. Often, small and medium-sized businesses lack the proper security measures and training to defend against cybercriminals, making them a major target.

**A strong password alone will protect your accounts.**

A strong password is important, but there are other steps that can also enhance your security. Multi-factor authentication will help protect your account a step further, along with many other necessary security measures.

**I was found on the Dark Web from a breach a few years ago, so what!?**

Any time your information is found on the Dark Web it should be taken seriously. Personal information on the Dark Web can be used for sophisticated phishing emails and you may still be using those old login credentials elsewhere.

Key Takeaways

It may be challenging to decipher fact from fiction, but use your common sense and ask questions when you are unsure of the answer.

# CYBER AWARENESS DURING ELECTIONS

Election cycles can muster up a large uptick in scams. Cybercriminals use phishing emails, phone scams and malicious fake websites to prey on the heightened political climate. Keep a level head and make sure you are applying common sense practices to avoid making a contribution to a cybercriminal's campaign.

## Cast Your Vote!

These candidates are ready to put an end to cybercrime, but they need our help!

**Candidate Name:** Sara Spoofs
**Party:** The Leave Me Aloners!
**Stance:** Sara promises to put an end to the constant spam phone calls, which are especially prominent during elections! "Scammers can spoof their phone numbers to make them look like anything," Sara explained during her latest interview. "If you're ever in doubt of who you are talking to, hang up! You can take their number and call them back on your own terms, or go directly to their website."

**Candidate Name:** Frank McFake
**Party:** The Too Good to be True Party
**Stance:** Frank is adamant about making sure the websites we visit are safe and secure. He was quoted as saying, "While I will do everything in my power to put an end to these fake and malicious websites, the risks are out there! Make sure you visit only reputable websites and avoid clicking on links with headlines that seem too good to be true!"

**Candidate Name:** Will Ustop
**Party:** The Click Cautious Party
**Stance:** Will is ambitiously declaring war on phishing emails. "Too many times I, I mean, my friends, have clicked on phishing emails and received a virus," he proclaimed during the final debate. "Phishing emails are rampant, especially during these elections. I urge my supporters to pay careful attention to emails and text messages, hover over links, and think twice before clicking anything.

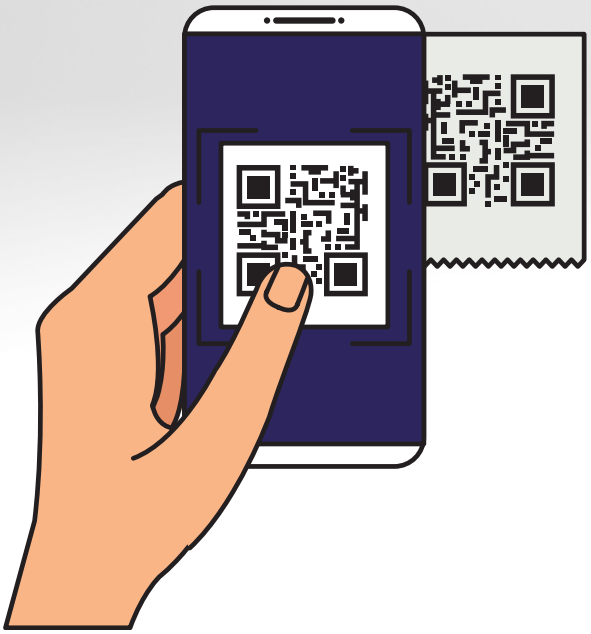
Quick Tip

Share this knowledge with your friends and family outside of work. We all must stay informed on these scams!

# SCAM OF THE MONTH

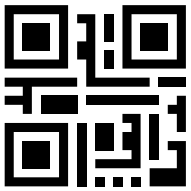
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

This month's submission comes from "Javier". Javier was walking to get his morning coffee. While walking, he spotted a telephone pole with a poster declaring "Free Couch". The poster said, "Scan the QR code for more details". Javier was intrigued and was needing a new couch, so he pulled out his phone and scanned the QR code.

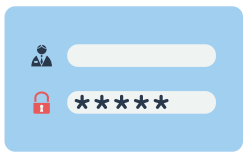


## Did you spot the red flags?

- The tease of a free couch was enough to lure Javier in for a closer look.
- The poster was placed in a public area where it could be easily seen by many.
- Javier was unaware of what a QR code was and the risks it came with.
- The QR code acts like a link that can take you wherever the code's designer wants you to go. With a quick scan, we can quickly be taken to a malicious webpage.



QR codes are becoming wildly popular. Anyone can create a QR code fast, free and easily. Scammers are using this new tool to reach new victims that may be unaware of the risks. We have been trained to hover over a link in an email to see its true path, but with scanning a QR code, the true location isn't provided until scanned.




Cybercriminals can set up a webpage to be anything they want. It could initiate the download of a virus or trick the victim into thinking they are on a legitimate page, leading them to enter in their credentials or other sensitive information. To reduce your risks, keep your personal devices updated with the latest software patches.

Not all QR codes are scams! But, since these tools are growing in popularity, it is important to be cautious. Think twice before scanning, just like you would with a suspicious link. For physical QR codes, watch for tampering, such as a new code placed over the original. Always trust your gut if something seems too good to be true.

# DON'T JUST BE SMART, BE #CYBERSMART

**Cybersecurity Awareness Month is a great time to reinforce the skills that you've learned while acquiring new skills for staying secure along the way.**

## Key Takeaways

Treat every month like it's Cybersecurity Awareness Month! Stay educated on the continuous threats that evolve every day.

Know the risks associated with QR codes and know how to protect yourself. Look for red flags and think twice before scanning anything.

Understand the reality behind many common myths. Use your common sense and ask questions to your peers when you are unsure of the answer.

Be on the lookout for election-based scams. During election cycles, we see a large uptick in phishing, phone scams and fake malicious websites.

## SECURITY MAD LIBS

Have some fun with our Security Mad Libs! Work with a co-worker or friend and ask them to select a word for each section of the speech below. Then, use the chosen words to fill in the blanks on the story below.

| | | |
|---|---|---|
| Body part: _____ | Retail store: _____ | Emotion: _____ |
| Article of clothing: _____ | Restaurant: _____ | Relative: _____ |
| Famous celebrity: _____ | Color: _____ | Noun: _____ |

John was having a really bad day! During breakfast, John's toddler stuck their _____ (body part) in John's cereal. Next, John left the house, forgetting to put on his _____ (article of clothing). When he got to work, John discovered his email was hacked and was sending hundreds of messages to _____ (famous celebrity) claiming to have free gift cards to _____ (retail store). During lunch, John left his work laptop at _____ (restaurant) and wasn't able to get it back. When he went to his car at the end of his work day, John noticed his car was spray painted _____ (color). John was not having a great day, but then he remembered it was Cybersecurity Awareness Month and he became very _____ (emotion). This month always reminded him of his _____ (relative) who always told him to avoid clicking on links in email as they may lead to _____ (noun).