A YEAR IN REVIEW

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

THIS MONTH'S TOPICS:

Cookies & The SLAM Method - pg. 2

A Scammer's Carol - pg. 3

Scam of the Month - pg. 4

A Bright Future Ahead - pg. 5

2020 was a year we may all want to forget. Despite the frustrations felt by many, cybercriminals enjoyed a prosperous year, shattering multiple records.

What becomes clear as we look back on 2020 is that cybercrime and scams will continue and advance, no matter what the global climate looks like. The only step forward we can take is to be aware of the threats and continue to educate ourselves and remain diligent.

A New Year means new personal goals. Although cybersecurity may not be at the top of your list of resolutions, you should find a place for it! There is always more we can learn and improve upon to advance our cyber-aware culture.

What's the Deal With Cookies?

An internet cookie is a website's way of keeping track of its visitors and their activity. As they collect data, cookies can help the website optimize the user's experience with login assistance, advertisement management and preference settings.

Generally, there are no security concerns with these internet cookies BUT their issues relate more to privacy concerns. The good news is, there are ways that you can manage your cookies from your internet browser. Here are some options:

Block Cookies - Your internet browser should have options available to block cookies altogether or block certain types of cookies.

Set Cookie Permissions - Other permissions can be set to reduce and control how cookies are used during your browsing session including restricting specific sites from using cookies.

Clear Cookies - Cookies and other site data can be cleared in your internet browser at any time, or preferences can be set to automatically clear cookies for you when you close your browser.

THE SLAM METHOD

Creating a list of New Year's resolutions? Try adding some cybersecurity resolutions to your list. To better protect yourself from phishing emails and text messages, follow the SLAM method whenever you are unsure of a message's legitimacy.

S **Sender** - Carefully analyze the sender of the email. Look for misspellings or irregularities within the email address.

L **Links** - Watch for deceptive or hidden links. Hover over any link before clicking to see where it truly leads.

A **Attachments** - Treat all attachments with caution. These documents or files could be malicious.

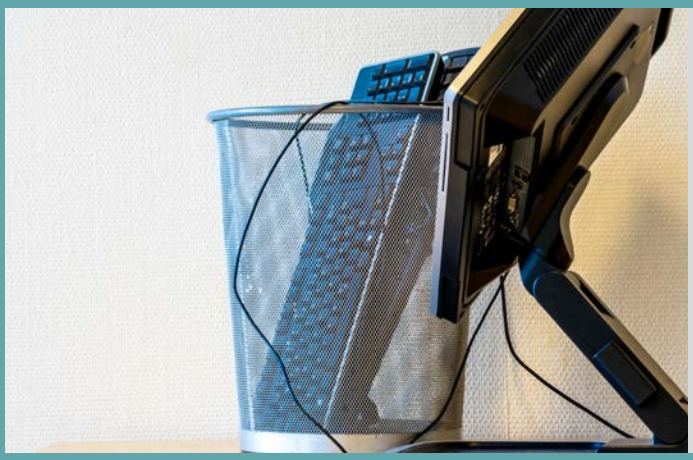
M **Message** - Read the message carefully and think about any action requested. Look for misspellings, poor grammar and threatening language.

A SCAMMER'S CAROL

Charlie was always a bit naïve when it came to cybersecurity. He knew that cyber attacks were occurring but never saw himself ever becoming a victim. To help prove to Charlie that his cybersecurity actions from the past and present can help shape the events yet to come, he is visited by three spirits one cold December night.

The Ghost of Scams Past

This spirit shows Charlie an event three years prior. An amateur scammer is compiling a list of email accounts and passwords gathered from a breach. Charlie learns that his credentials were exposed in this breach and posted online. Although he changed his password for the compromised account, he had used this same or similar password on other accounts. This leaves Charlie exposed and vulnerable to a breach of his account and information.



The Ghost of Scams Present

This next ghost shows Charlie a more familiar scene. They appear at Charlie's office and watch as Charlie proceeds to skirt company policies such as not disposing of company equipment properly and browsing social media sites on his lunch break. His lack of awareness is putting the company and its data at risk of exposure.

The Ghost of Scams Yet to Come

The final apparition has appeared to show Charlie his potential fate if he continues down his current path. Charlie learns that breaches have severe consequences including termination of employment and personal issues such as financial losses and identity theft.

Charlie has learned a lot from his visitors. With a new lease on life, he returns to his present and vows to take cybersecurity more seriously in order to avoid the many painful consequences.

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.

"Kevin" got a great holiday bonus in his last paycheck. He's been doing well financially and wants to donate some of this bonus to charity. Kevin's home town of Littleville was recently hit with a devastating flood and he wanted his funds to go towards the relief efforts. With a quick internet search Kevin clicked on the first link he saw titled www.littleville_floods.com. Kevin clicked on the "Donate" button on the webpage and began filling in the requested information to make the donation including his government identification number and bank routing number. Unfortunately for Kevin, this was a fake charity page set up by a scammer to look legitimate.

Did you spot the red flags?

- The site Kevin visited had the addition of the underscore (_) in the web address, a slight difference from the real site.
- When attempting to donate, the site requested additional information such as identification numbers and banking information. These would be unnecessary in a standard donation process.

Scammers prey on our generosity, especially during crises and natural disasters. Being aware of events on a global level along with local issues in their area, they craft their fake website and URL. Often scammers will set their site to an almost identical name as the real charity they are looking to copy.

Do your research on any charity before donating. Before donating, know that the charity you are giving to is legitimate and how your donation is going to be spent. There are many online tools available to verify if the charity is registered or if there have been any complaints issued against the charity.

Quick Tips

- Don't feel rushed or pressured into donating. A common tactic used by scammers is to force their victims into irrational decisions.
- Never give out sensitive and personal information that is beyond what would typically be required for an online purchase.

A BRIGHT FUTURE AHEAD

Key Takeaways

With a tumultuous year behind us, set goals for your future cybersecurity success. We all have lessons to learn and skills to improve so let's make this next year a success.

Internet cookies are generally not to be feared, but if you are worried about privacy, take the time to manage how cookies are used on your web browser.

We all can become victims of cybersecurity incidents, so don't let your past or present behavior have a negative impact on your future.

Don't rush your generosity; donate securely. Watch for suspicious fake charities designed to line the pockets of scammers.

Cybersecurity Cryptogram

A Cryptogram takes each letter of the alphabet and replaces it with a number. Using the key at the top, find the appropriate letters that correspond with the phrase below. We gave you a few to start, can you find the hidden phrase below in this month's puzzle?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
				22								10													

4 23 26 22 23 4 23 15 15 18 23 14 20 25 17 23 10

7 6 22 22 14 22 24 18 22 23 6 !

Answer: Have a Happy and Scam Free New Year!