SEEMS A BIT PHISHY TO ME

A review of the latest in phishing schemes and cybersecurity threats

THIS MONTH'S TOPICS:

Hook, line, and sinker:
Smishing, Vishing, and Phishing

Catch of the day:
What scammers are thankful for

Scam of the month:
Baby shark, do, do, doo, dadoo

Cyber Zen Den:
Good news on the cyber front

November is all about fishing. Ice fishing.

It's a cold, cruel, world out there, and someone's got to take the bait. Don't let it be you!

In this month's issue, we're going to tap into the different types of phishing techniques used by scammers, dive deeper into why they work, and learn more about what you can do to avoid them.

There may be some fishing puns along the way, but we're just trying to keep it reel.

In conjunction with **phishing**,
cybercriminals are also really good at **psychology**.

- In the Psych world, the psychological manipulation of people to perform desired actions is called "Social Engineering."
- Cybercriminals commonly put this social engineering concept into action with their phishing attacks against us.

THE RODFATHER

Phishing techniques

Smishing

Fraudulent text messages are sent to trick you into revealing personal information or downloading malware.

Vishing

Voice phishing or phone fraud meant to entice you to divulge sensitive data.

Email Phishing

Deceptive emails are meant to steal personal information or get you to click links to install malware.

The reason these tactics work is because they exploit human trust

Trust, **context**, and **emotion** all play a role in decision-making and can easily be manipulated.

Using these methods, attackers will draft personalized messages that pose as legitimate organizations or individuals, regarding situations you're likely to find yourself in, and create a sense of urgency around their desired action.

Hook, line, and sinker.

WHAT ARE SCAMMERS THANKFUL FOR?

"EVERY BAIT AND SWITCH IS A WORK OF ART"

"PEOPLE WHO DON'T VERIFY A LINK BEFORE CLICKING."

"OUTDATED ANTIVIRUS SOFTWARE PROGRAMS."

"OVERSHARING ON SOCIAL MEDIA PLATFORMS."

DON'T GIVE SCAMMERS A REASON TO BE THANKFUL THIS SEASON!

BLACK FRIDAY & CYBER MONDAY

(AND OTHER HIGH-VOLUME COMMERCE EVENTS)

Now is the time to remain vigilant!

The pandemic has created greater stress, as well as tighter financial and supply-and-demand pressures. Personal distress can often cloud sound judgment, so this shopping season be sure to:

- Take your time: don't panic-click unsolicited links
- Do your due diligence: research unknown vendors before purchasing products
- If the sale is too good to be true... you know the deal...

SCAM OF THE MONTH

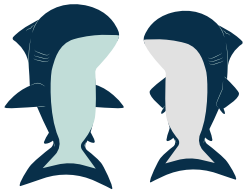
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Ariel (10) was scrolling through the newsfeed of a photo-sharing app when she noticed a glam shot of her favorite influencer wearing cute new sneakers. She took a screenshot for her birthday list and then noticed a giveaway linked in the comments section. "Turn $20 into $200 and buy these shoes now! Make real money, real fast."

Ariel knew it was unlikely she'd get the shoes from her parents, and more likely she'd get a pair of similarly colored socks, so she clicked the link to try her luck online.
This took her to an outside website. A flashing logo said to "call this number, to learn more!" When she did, a male voice answered, "All you need to do is give me the security number and pin from your reload card, and I'll add in some extra zeros." Ariel didn't feel right about the situation. Her heart was racing, and she quickly hung up.

Did you spot the red flags?

- Ariel clicked a link in the comments section. Because the link was tied to a known influencer that she liked and trusted, she was misled to believe it was vetted.
- The caller was requesting a pin or code. Never provide anyone with these numbers, or other numbers tied to your money.
- Turning $20 into $200 was too good to be true. Ariel had a gut feeling something wasn't right, and she went with it. Good for her!



As a Mamma and Daddy shark, it's important to talk with Baby sharks about scams they may encounter while surfing the web.

Social Media scams have more than tripled in the past year. These platforms are often a place to let your guard down, and surround yourself with friends. Fraudsters take advantage of this dynamic, and swoop in when you least expect it.

Make your home a no phishing zone. Stay in the know about new phishing tactics, and role-play scheming scenarios with little ones so that they'll know what to look out for and how to proceed safely.

Key Takeaways

There's a lot of different ways cybercriminals can phish for your information and ruin your life or career. But find comfort in the fact that you can take control of your cyber-space.

By taking your time and researching content that is intriguing to you before diving in (whether it be a hot new deal or a money-making opportunity), you're creating boundaries that will protect you and your information from the unknown.

Don't click that link! Whether it's in an email or a text message, know where a link is taking you before you click it.

Follow your intuition. If an encounter online doesn't feel legitimate, go with your gut, and do some further research.

Keep an eye out for all of your devices. Scamming can take place on many different platforms. It's not just emails anymore!

Mindfulness

Mindfulness is known for relieving stress, decreasing anxiety, and improving sleep.

How does this relate to cybersecurity?

Well, if you're overworked, under-rested, and a general ball of stress, you're more likely to make mistakes in areas of your life that you wouldn't normally. This includes link clicking and personal information sharing. Sometimes you don't even realize these interactions are happening until they're over.

So practice mindfulness. Take a moment right now to be present. Look at the pretty lotus flower above. Take a deep breath and check in with yourself. How are *you* doing?

Now, when those emails come rolling in, practice these mindful habits and stay in the moment to avoid accidentally clicking on those scammy links.