THE FUTURE OF FRAUD

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

THIS MONTH'S TOPICS:

We may not have a crystal ball, but there are some things we can predict about the future. Technological advancements will continue to improve our daily lives, but similar improvements will be made within the cybercrime community. Scammers know their targets are onto their tricks so they are always in search of new ways to stay one step ahead.

The good news? This future doesn't have to be scary! It all boils down to continuing our cybersecurity awareness training efforts. There will always be new scams, vulnerabilities, threats, and ways to prevent them so it's critical to keep our minds sharp. Take some time to learn about some of the cybercrimes of the future and how you can best protect your, and your company's information.

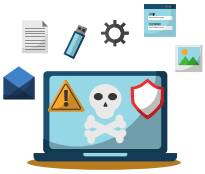
The Future of Fraud

As new technological advancements are made, new cyber threats emerge with them. Take some time to learn some of the possible threats of the future and how to best protect yourself and your company.

The Internet of Things (IoT)

More and more of our standard electronic devices used every day are becoming "smart" with internet connectivity. This popular trend can provide more technology features but allows another entry point for cybercrime.

- Be Smart!: Protect your smart devices with strong passwords and keep the devices up to date.



Ransomware as a Service

Ransomware attacks continue to grow, creating a lucrative scheme for cybercrime groups. Tools on the dark web are being sold that can help the purchaser carry out an attack from start to finish.

- Yikes!: A monthly subscription to a fully-loaded ransomware toolkit can start at just $120.

Artificial Intelligence/Machine Learning

Artificial Intelligence (AI) and machine learning are expected to drive future technological advancements. However, this advancement may be used in a malicious capacity by scammers in an effort to automate and improve their scams.

- Brutal!: AI helps power password cracking tools that rapidly guess passwords for our accounts.

Cryptojacking/Cryptomining

Cryptocurrencies like Bitcoin are at an all-time high. Cybercriminals found ways to "mine" this type of digital currency by harnessing the power of our computers through either an infected website or a malicious file.

- Stay Alert!: Tune in for poor device performance or signs your CPU is working harder than it should.

DEEPFAKES

What is a Deepfake? - Deepfakes are fabricated audio or video files designed to deceive. Sometimes they are harmless pranks, but many scammers are turning to these pieces of content to deliver a more convincing scam. Although challenging, there are ways we can spot a deepfake. Here are a few:

Inconsistent Audio
Listen for audio discrepancies like background noise or poor audio quality.

Odd looking Teeth? - Many deepfake tools struggle with generating individual teeth.

Try pausing the video, taking a screenshot and doing a reverse image search online.

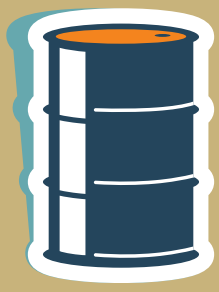
Unnatural eye movement or irregular blinking patterns.

Does the image seem blurry? - Check around the lips and the neck for subtle blurring or misalignment.

Weird lighting throughout the video, making it difficult to see the subject.

Think about the content and how you received the file. The source and subject matter may be clues to its legitimacy.

The Colonial Pipeline Ransomware Attack



Colonial Pipeline operates a 5,500-mile gas and petroleum pipeline stretching from Texas to New Jersey in the United States. **45% of the East Coast's fuel consumption relies on this pipeline.**

What happened?

On May 7, 2021, Colonial Pipeline was hit with a massive **Ransomware attack** resulting in a shutdown of operations.

Although the specifics of how this ransomware attack occurred are not yet available, similar attacks were traced back to unpatched vulnerabilities, compromised user credentials, or a simple phishing email.

Paying the Ransom?

With a crisis on their hands, the Colonial team tried to determine their options. Ultimately, the decision was made to **pay the ransom of $4.4 million in Bitcoin**. Colonial worked with a team of experts who negotiated the ransom and worked with the attackers to ensure they would keep up their end of the bargain.

What happened next?

After the ransom was paid, the pipeline resumed operation, but the damage continued. The pipeline took several days to return to running at full capacity leading to panic as consumers feared of a fuel shortage prompting **gas hoarding and high prices**.

Why should you care?

This massive shutdown impacted millions of Americans who relied on this pipeline for fuel. A longer shutdown could have resulted in major gas shortages.

Colonial stated they've previously spent 200 million dollars on IT, proving it takes more than just technology to prevent an attack. Hence why we put so much emphasis on security training!

This attack was seen around the world signaling to other cybercriminals the value in targeting similar industries and that more victims are paying the ransom.

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.

Gary is fascinated with technology and wanted the smartest house on the block. He loves buying all the latest smart gadgets and accessories such as a smart thermostat, app-controlled lights, smart washing machine, and more. In his excitement, Gary gets his devices set up and connected right away, using the pre-configured password and settings that came with the appliance. One day, Gary returns from work and finds his home is locked and he can't unlock it from his app. The smart home locks had been breached and he was unable to get in. In addition, his home thermostat was compromised and the attacker had raised the home temperature with his pets inside, creating a dire situation for Gary.

Did you spot the red flags?

- Gary didn't set these devices up securely with strong and unique passwords.
- Gary never did any security updates which left his devices vulnerable to security flaws.
- Gary put too much stock in his smart devices and failed to consider security.

IoT stands for the Internet of Things and focuses on turning everyday objects into internet-connected devices. Home appliances, watches, lightbulbs, locks, cameras, baby monitors, and more are becoming digitally enhanced. The IoT market is exploding in popularity, and while these devices are great, they do come with risk.

Examples of compromised IoT devices include:

- A hacked smart speaker allows a criminal to eavesdrop on personal situations.
- A smartwatch for children had vulnerabilities that exposed personal information and the child's GPS coordinates.

There are ways to protect these devices. Keep IoT devices regularly updated with any security patches as soon as they are released. Also, protect each individual IoT device that is controlled through an app with a strong and unique password or consider using a password manager. For advanced protection, enable two-factor authentication (2FA).

PRO TIP Protect your home Wi-Fi network. Most routers are not secured out of the box leaving your home network vulnerable. Update the standard password to a complex passphrase and consider changing the SSID (Service Set Identifier) which is the primary name of your wireless network.

The Future Starts TODAY

Key Takeaways

There is little we can do to prevent the scams of the future from being crafted, but we can stay informed and be prepared for them. Follow your instincts but check with others whenever you are unsure.

The future of fraud highlights a reliance on automation for scams. Though their efforts may ramp up, we've got the tools and knowledge to fend off many of their future attacks.

Know the signs of a deepfake video or audio file such as irregular audio, blurriness around the face, undefined teeth, and unnatural blinking or eye movement. If the content and the source of the file seem suspicious, check with IT or a supervisor.

Keep your smart devices secured. These devices are sure to continue their rapid growth in the future and will continue to be a target for cybercrime. Keep these devices updated with the latest security patches and strong password controls.

Cybersecurity Over/Under

Try to guess some of the latest cybersecurity numbers in our Over/Under game! We will give you a number in relation to a topic, you decide if the true number is "Over" the provided number, or "Under". (All data based on the Verizon 2021 Data Breach Investigations Report)

1. The median losses from a Business Email Compromise (BEC) attack were **$20,000**.

2. **90%** of incidents for Small to Medium-sized Businesses (SMB) were perpetrated by external actors.

3. **7%** of all breaches now involve ransomware.

4. **60%** of the data compromised in Social Engineering incidents were credentials.

5. For small organizations, **75%** of breaches are discovered within "days or less"

Answer: 1. Over ($30,000) 2. Under (57% External 44% Internal) 3. Over (10%) 4. Over (85%) 5. Under (47%)