NEW YEAR, NEW CYBER TRENDS

Keeping up with the everchanging digital landscape

THIS MONTH'S TOPICS:

Happy New Year! May 2024 bring you lots of joy and cybersecurity.

One great way to stay safe online throughout this new year is to keep up with the ways cybercriminals are changing their scams. Whether it is a completely new scam, or a twist on their tried and true, cybercriminals are always looking for ways to utilize new tools and technology.

In this month's newsletter, learn why mobile attacks are on the rise and see firsthand how social engineering attempts are getting harder to spot. Don't forget to check out our new Cyber News section!

THE RISE OF MOBILE ATTACKS

80% of phishing sites now target mobile devices.

TEXT MESSAGES

Many of these types of scamming topics are the same- reducing debt, package delivery, and fake texts from businesses. One way to verify the legitimacy of these messages is by using a reverse lookup tool. This will reveal if others have received scam messages from the number.

PHONE CALLS

2024 will likely bring political donation scams. Scammers are also using fake caller IDs to mimic businesses. It is best not to interact with these phone calls. If you say anything- even just “yes” or “no”, the scammer will know the number is active and save it for future scams.

VOICE ACTIVATED AI

Be careful when asking voice-activated AI services like Siri to call businesses or pull up websites. If a scammer has optimized their phishing page to appear at the top of search results, these tools may auto-dial the scammer's phone number or pull up their website.

WHY MOBILE?

One of the many reasons why mobile devices are targeted is because users are often using them after a long day when fatigue has set in, and they aren’t as cognizant of what they click.

87% of people surveyed receive at least one scam message via text daily.

43% of financial scams in 2023 were phone scams like robocalls or text messages.

SOCIAL ENGINEERING

With the rise of AI chatbots, social engineering attacks are easier for cybercriminals to carry out. Always be wary of unsolicited messages, no matter how specific they are.

Meet Rachel Davis.

Rachel is a mid-level executive at a marketing firm. Her job history is listed on her profile through a professional networking app. She also was recently featured in an article on prevalent alumni in Bridgeford University's online magazine.

Meet Perry.

Perry is a hacker who gained access to exposed data from a fitness app that suffered a breach. The data included names and email addresses of users. Rachel Davis was one of those users. Perry did a quick google search and used a malicious AI chatbot called WormGPT (cybercriminal's version of ChatGPT) to find more of Rachel's information and write a scam message targeting her.

In seconds Perry finds out where Rachel works, who else works there, and other personal details. He makes an email account with the address CarlosSalva5@gmail.com (her coworker) and sends her this message:

New Message

To RachelD@Bridgeford.edu

Subject Bridgeford Alumni Award

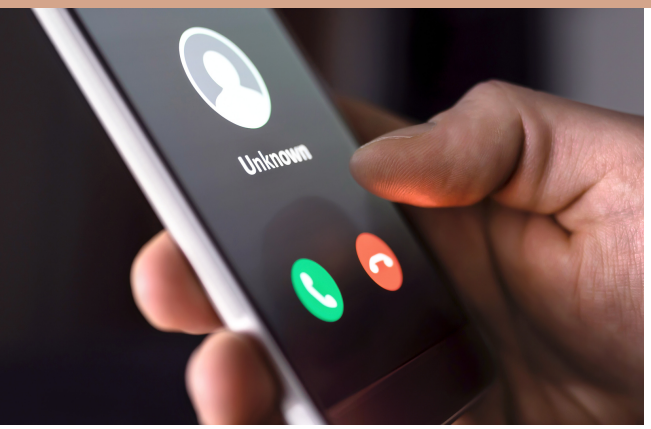
Hi Rachel,
It's Carlos from Sales. Have you seen this article about the cash award Bridgeford is offering to alumni? The details are here.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

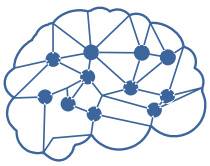
Jean was at work looking at the latest financial report when she received a phone call. The call was from an unknown number, but Jean often gets calls from potential clients, so she answered. To her surprise, it was her daughter Kenzie's voice on the other line. Kensie sounded scared and said she was in trouble. She said she needed a few thousand dollars wired to an account or else she would go to jail. She told her mom she would explain more later. Jean panicked and wanted to make sure her daughter was safe, so she wired the money immediately.

Later she tried to call the number back but there was no answer. She called Kenzie's normal phone number and Kenzie answered. When Jean asked her what happened, Kenzie was confused. She was never in any trouble and never asked for money. Jean realized it was a scam. Plus, the wallet she transferred the money into turned it to cryptocurrency, so it was not traceable.



Did you spot the red flags?

- Jean should have been more suspicious of a call from an unknown number claiming to be her daughter.
- Jean should have called Kenzie on her regular phone or called someone who would be with her before transferring the money to the unknown account.
- Cryptocurrency, wires, and gift cards are all methods of payment used by scammers. An unsolicited request for one of these forms of payment is a red flag.



Scammers use artificial intelligence to clone voices and use them for scam calls. They can do this from a small sample of a person's voice on social media or any audio of them online.

Have a family secret word that you all know to verify the legitimacy of these calls. Think about whether the person calling could be in danger or in the location mentioned by the caller.

This scam also occurs in professional settings. Scammers clone the voice of a CEO or high-up executive and call to convince employees to give away their account credentials or transfer money.

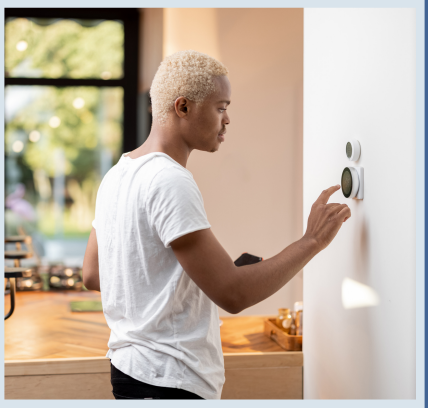
CYBER NEWS

JANUARY
2024

BOSCH THERMOSTAT VULNERABILITY

A vulnerability has been discovered in Bosch BCC100 thermostats which allows attackers to replace device firmware with a malicious update. Once infected, the thermostat can be used to listen to conversations, go through device data, steal login credentials, or infiltrate other devices on the same Wi-Fi network.

The company recommends keeping your IoT devices on a separate network and monitoring them frequently for any signs of malicious activity. Many IoT devices update automatically, but make sure all devices are up to date with the latest patches to avoid vulnerabilities like this one.



CYBER DATES

January 24th-28th: Data Privacy Week

January 29th-February 2nd: Identity Theft Awareness Week

MALICIOUS CRYPTO ADS INCREASE

Users on X (formerly Twitter) and other social media platforms are reporting an influx of malicious cryptocurrency advertisements. These ads could come from fake “verified” users who have purchased their blue check mark or from legitimate accounts that have been compromised. If the links in these posts are clicked on, the user’s crypto wallet could be drained completely. Remember to always research a company before clicking on a link in their social media ad.