APRIL 2025

PROJECT CYBERSAFE™ NEWSLETTER

A QUARTERLY PUBLICATION FOR NSSF AND SAAMI EMPLOYEES

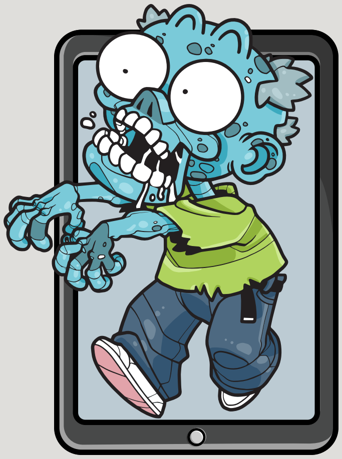
GOOGLE YOUR NAME. REMOVE THE RESULTS FOR FREE!

Google has a "newly-redesigned Results about you tool" to scan search results for the personal contact details you tell it to look for, like your phone number or address, and then it can help you quickly remove them. Once you've done this, Google's tool adds proactive monitoring, alerting you if new results are found.

Use this link to the Google results about you page to enter your information and see what publicly available information is identified. You will then be able to review and request the removal of any of the entries found. Initial results usually take 24 hours to populate.

ZOMBIE PC's

Computers that have been powered off for lengthy periods of time pose many risks to both the user and their personal/work networks when those computers are powered back on. These computers are often referred to as zombie PC's because they have been dormant for so long that they will be far behind on the system and software updates needed to keep the computer up to date. Due to the inactivity and lack of current updates, they are vulnerable to the newest cyber-attacks that have arisen since the last time your computer was powered on and updated.



If you have a work device that hasn't been power on for more than a few weeks, it makes sense to reach out to IT for guidance before powering it back on. If you have a home device that has not been powered for some time, make sure that your antivirus program is the first thing you update and then run all available system updates before using the device.

FBI ISSUES WARNING TO ALL GMAIL, OUTLOOK EMAIL USERS

The following story highlights the importance of security awareness training.

The FBI and the U.S. Cybersecurity and Infrastructure Security Agency are urging users of popular email services like Gmail and Outlook to be on the lookout for a dangerous and potentially costly ransomware scheme.
A bulletin released this week detailed a warning for the Medusa ransomware gang, a group that's been active since 2021.

As of February 2025, the ransomware attack has impacted more than 300 victims in the medical, education, legal, insurance, technology and manufacturing fields. The group uses phishing campaigns – bogus emails that prompt users to click links or provide personal information – as well as exploitation of unpatched software vulnerabilities. It then takes the computer or information "hostage" until a ransom is paid.

Roger Grimes, a data-driven defense evangelist at KnowBe4 has a slightly different take and says the governments warning continues a long tradition of "warning people about ransomware that spreads using social engineering, that then does not suggest security awareness training as a primary way to defeat it." Grimes said that, in the experience of KnowBe4, social engineering is involved in 70% - 90% of all successful hacking attacks. Yet, despite the official alert noting that social engineering is one of the primary methods of distributing the ransomware threats, awareness isn't mentioned in the 15 recommended mitigations. "It's like learning that criminals are breaking into your house all the time through the windows and then recommending more locks for the doors," Grimes said. Warning that such a continued misalignment between the ways we are most often attacked by threat actors and their malware programs and how we are told to defend ourselves enables hackers to continue to be successful, Grimes concluded that "the hackers must be laughing."

Read more from the Forbes article here.

A PROGRAM OF NSSF® The Firearm Industry Trade Association

23ANDME HAS FILED FOR BANKRUPTCY. HERE'S HOW TO DELETE ALL YOUR DATA FROM 23ANDME:

from CNBC

23andMe has officially filed for Chapter 11 bankruptcy protection, which means its assets — including its vast genetic database — will soon be up for sale.

If genetic data falls into the hands of bad actors, it could be used to facilitate identity theft, insurance fraud or other crimes. 23andMe has been plagued by privacy concerns in recent years after hackers accessed the information of nearly 7 million customers in October 2023.

23andMe said customers can still delete their account and accompanying data.

Here's how to delete your genetic data from 23andMe

- Go to 23andMe.com and sign in to your account.
- Click on your profile in the upper righthand corner of the site, then click "Settings."
- Scroll to the section at the very bottom of the page called "23andMe Data" and click the oval button that says "View."
- Check the boxes of any data you would like to download and click "Request Download." This step is optional and can take up to 30 days. Pending downloads will be canceled if you delete your account.
- Scroll to the bottom of the page and click the red button that says "Permanently Delete Data."
- You will receive an email with the subject line "23andMe Delete Account Request." Open it, and click the button that says "Permanently Delete All Records." Your data will not be deleted unless you complete this step.

At this point, your personal information and your account will be permanently deleted from 23andMe, according to the deletion email from the company. Additionally, your data will not be used in any future research projects, and any personal samples the company was storing will be discarded.

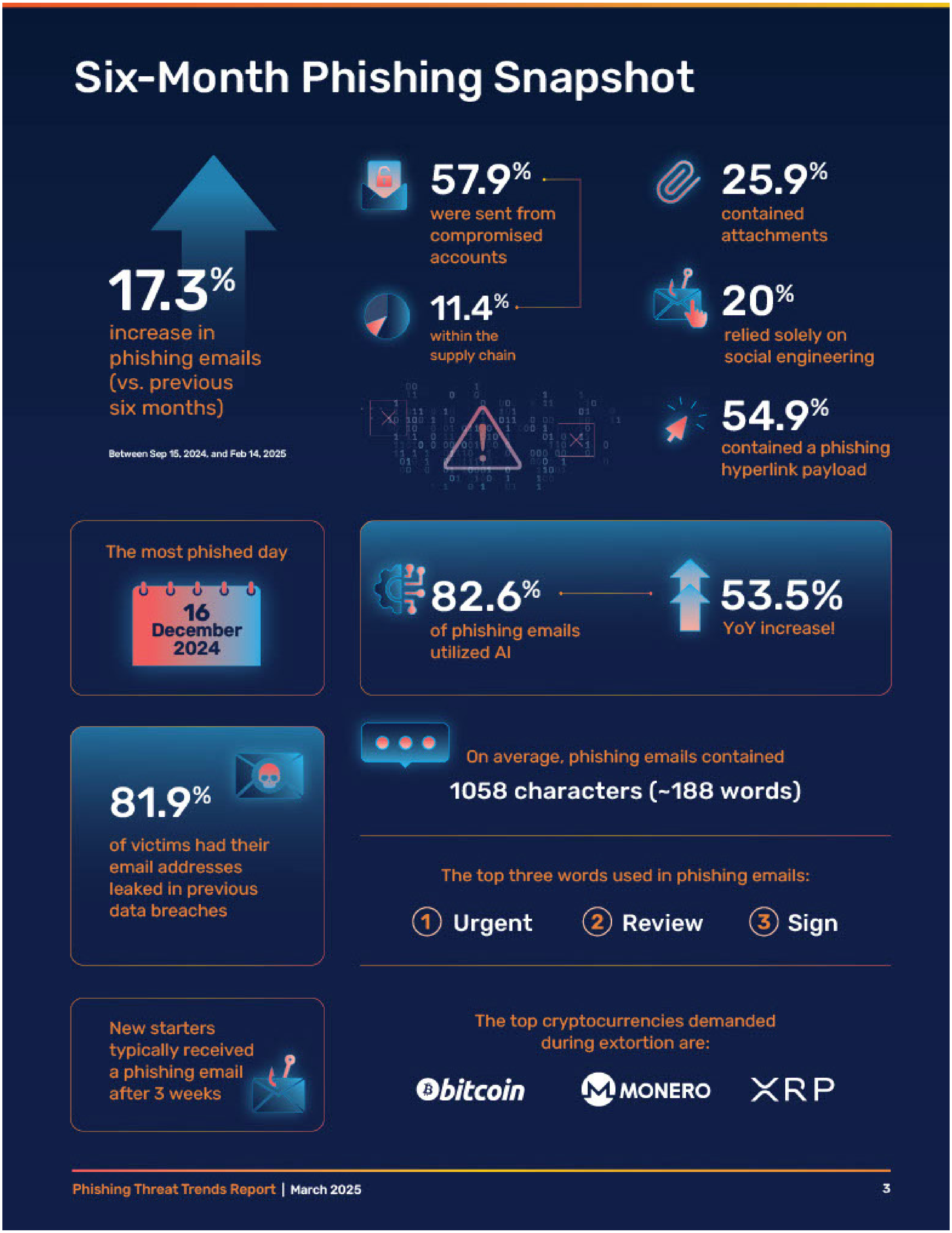
KIDS CORNER

PowerSchool systems were breached at the end of December and data was confirmed to be stolen. PowerSchool is a cloud-based software solutions provider for K-12 schools and districts that supports over 60 million students and over 18,000 customers worldwide. The company offers a full range of services to help school districts operate, including platforms for enrollment, communication, attendance, staff management, learning systems, analytics, and finance.

PowerSchool is not calling this a ransomware incident because PowerSchool reached out to the cybercriminals once they became aware of the breach and negotiated a fee with the cybercriminals for the deletion of the data with video evidence of the deletion. The investigation by CrowdStrike is still ongoing and anyone who has a child or spouse impacted should already be aware of the incident. Your schools should be keeping you updated as they receive information from PowerSchool. I thought this would be a good opportunity to share the Federal law that grants parents data and privacy rights for their children's records.

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

Infographic from the 2025 Phishing Trends Report from KnowBe4 > Download the full report here.



Six-Month Phishing Snapshot

17.3%
increase in phishing emails (vs. previous six months)

Between Sep 15, 2024, and Feb 14, 2025

57.9%
were sent from compromised accounts

11.4%
within the supply chain

25.9%
contained attachments

20%
relied solely on social engineering

54.9%
contained a phishing hyperlink payload

The most phished day

16 December 2024

82.6%
of phishing emails utilized AI

53.5%
YoY increase!

81.9%
of victims had their email addresses leaked in previous data breaches

On average, phishing emails contained

1058 characters (~188 words)

The top three words used in phishing emails:

1 Urgent 2 Review 3 Sign

New starters typically received a phishing email after 3 weeks

The top cryptocurrencies demanded during extortion are:

bitcoin MONERO XRP