MONTHLY CYBERSECURITY NEWSLETTER

FEBRUARY 2025

NCDIT Secretary Piccione Makes Cybersecurity a Priority

As the N.C. Department of Information Technology's new Secretary and State Chief Information Officer, Teena Piccione is making cybersecurity one of her top three priorities.

"Nefarious actors are coming after us fast and furious, so we must ensure that we are protecting the state's data and thinking through how we make sure that everything we have access to is secure," Piccione said at the North Carolina IT Strategy Board meeting on Jan. 31.

Piccione comes to NCDIT from Google, where she was most recently the managing director for Cloud and Customer Engineering over Telecommunications, Media, Entertainment and Gaming. She has also worked at RTI International as executive vice president and chief technology officer, at Fidelity Investments as senior vice president and chief operating officer, and at AT&T as vice president and leader of the Big Data Center of Excellence.

She has also served on the IT Strategy Board's Digital Transformation Committee where she advised NCDIT on vision, mission and goals for digital transformation and helped develop a digital transformation roadmap for the state.

Beware: Credential Phishing Attacks Increased by 703% in H2 2024

Credential phishing attacks surged by 703% in the second half of 2024, according to a report by Slash Next.

Phishing attacks overall saw a 202% increase during the same period.

"Since June, the number of attacks per 1,000 mailboxes each week has increased linearly," the researchers write.

"Currently, we are capturing close to one advanced attack per mailbox each week. As we reach the 1,000 threshold, this translates to nearly one advanced attack for every single mailbox each month. This steady increase indicates a substantial volume problem that individual efforts cannot handle effectively."

The researchers believe the increase is partially due to

the proliferation of phishing kits, which allow criminals to launch sophisticated attacks by making little effort.

“Throughout the year, we’ve shown evidence of attackers having access to unique phishing kits designed to evade detection, automate their processes, and target victims at scale,” SlashNext says.

“Our data shows that these diverse phishing methods have been consistently employed from the beginning to the end of the year .

“Since our mid-year report, there has been a remarkable 202% increase in the number of phishing messages delivered per 1,000 mailboxes. This trend underscores a significant shift in email security dynamics. We are now operating in what can be described as a ‘volume game,’ where the sheer number of attacks overwhelms traditional security measures.”

The researchers predict that these attacks will continue to increase throughout 2025, as threat actors incorporate AI tools to improve the efficiency of their attacks.

“Looking ahead to 2025, we expect this rapid evolution to accelerate, with AI-generated attacks becoming more sophisticated and harder to detect, while attackers increasingly target messaging platforms beyond email, including business collaboration tools, SMS, and social media,” SlashNext says.

“The bottom line is phishing isn’t an email-only problem anymore; it is a broader messaging security problem that requires a fundamental shift in how organizations approach threat detection and prevention.”

KnowBe4 empowers your workforce to make smarter security decisions every day. Over 70,000 organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

This article is redistributed with permission from KnowBe4.

FBI Warns of Cybercriminals Using Generative AI to Launch Phishing Attacks

The FBI warns that threat actors are increasingly using generative AI to increase the persuasiveness of social engineering attacks.

Criminals are using these tools to generate convincing text, images, and voice audio to impersonate individuals and companies.

“Generative AI reduces the time and effort criminals must expend to deceive their targets,” the FBI says. “These tools assist with content creation and can correct human errors that might otherwise serve as warning signs of fraud.”

Generative AI takes what it has learned from examples input by a user and synthesizes something entirely new based on that information.

These tools assist with content creation and can correct human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.

The FBI offers these tips following advice to help users avoid falling for these attacks:

- Create a secret word or phrase with your family to verify their identity.
- Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic teeth or eyes, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, lag time, voice matching, and unrealistic movements and unrealistic accessories such as glasses or jewelry.
- Listen closely to the tone and word choice to distinguish between a legitimate phone call from a loved one and an AI-generated vocal cloning.
- If possible, limit online content of your image or voice, make social media accounts private, and limit followers to people you know to minimize fraudsters' capabilities to use generative AI software to create fraudulent identities for social engineering.
- Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and calling the phone number directly.
- Never share sensitive information with people you have met only online or over the phone.

Do not send money, gift cards, cryptocurrency, or other assets to people you do not know or have met only online or over the phone.

This article is redistributed with permission from KnowBe4.

Data Privacy Tips for Work and Home

The N.C. Department of Information Technology joined with others from around the world Jan. 27-31 to recognize Data Privacy Week. This annual initiative focuses on increasing privacy awareness. It empowers individuals and organizations to build a culture of privacy, embedding data protection and transparency in the state's use and handling of personal information.

Everyone can take simple steps to manage their data and take more control over where it is shared.

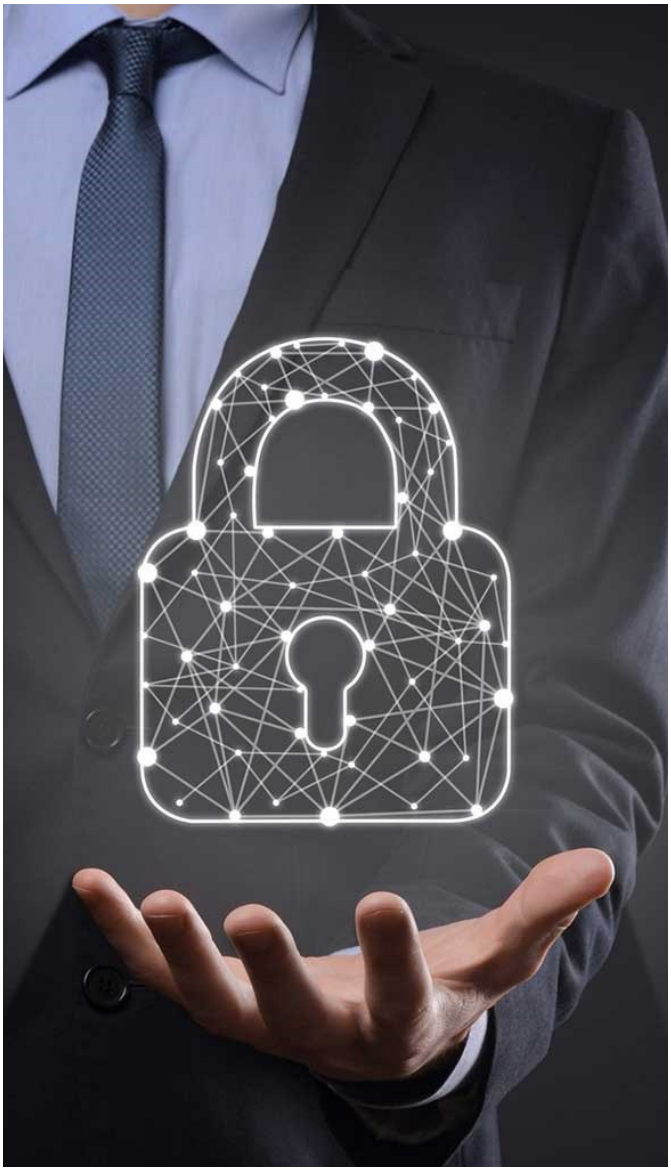
Watch the Office of Privacy and Data Protection's virtual lunch and learn on why privacy matters and how you can protect sensitive personal information at work and at home.

Check out the department's blog posts to learn about:

- Why We Value Privacy as State Employees
- Core Principles for Protecting North Carolinians' Personal Information
- The Role of Privacy in AI Governance

Learn more about why privacy matters and get useful information to help you protect privacy at work and at home.

https://it.nc.gov/privacy



Training & Continuing Learning Resources

FedVTE: Free Online Training Environment
https://fedvte.usalearning.gov/

TEEX: Texas Engineering Extension Service
https://teex.org/

NICCS: National Initiative for Cybersecurity Careers & Studies
https://niccs.cisa.gov/

ICS-CERT Training
https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Additional Cybersecurity Newsletters

SAC Security Awareness Newsletter

Monthly security awareness newsletter provided for all state employees by KnowBe4. The link to the newsletters: **Access the newsletter here.**
(Note: You must have a valid state employee Microsoft 365 account to access.)

SANS OUCH! Newsletter

Free monthly cybersecurity awareness newsletter provided by the SANS Institute. **Read the newsletter here.**

Connect with Us

Be sure to follow the N.C. Department of Information Technology on X, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness.

Remember … Stop. Think. Connect.

***Disclaimer**: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*