NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

MONTHLY CYBERSECURITY NEWSLETTER AUGUST 2025

Jennifer Fix Named Deputy State Chief Information Security Officer

Jennifer Fix joined the N.C. Department of Information Technology as deputy state chief information security officer in July.

A cybersecurity and risk management leader with more than 20 years of IT experience, Fix has a proven ability to drive security innovation and lead high-impact teams. She has held leadership roles focused on enterprise security strategy, governance, risk and compliance.

Fix believes in fostering a culture of security awareness and an environment of effective communication and collaboration to identify and mitigate risk. She is passionate about mentoring, coaching and fostering professional growth.

She previously served as director of security and compliance at RTI International, among various other roles delivering complex enterprise-wide technology solutions over 20 years at the organization.

Fix is certified in risk and information systems control and business relationship management.

NCDIT and Carolina Cyber Network Launch New Cybersecurity Internship Program

NCDIT Secretary Teena Piccione and State Chief Information Security Officer Bernice Russell-Bond traveled to Fayetteville Technical Community College on July 7 to announce a new internship program that will provide real-world cybersecurity experience to students enrolled in Carolina Cyber Network member schools while expanding the state's information technology workforce. NCDIT is partnering with FTCC to offer the initial internships.

Starting with the upcoming fall semester, interns will work up to 25 hours a week in cybersecurity roles at NCDIT. These remote positions will focus on giving interns experiential learning opportunities in various aspects of cybersecurity and information technology.

"Cybersecurity is one of our state's top priorities, and the Carolina Cyber Network is an outstanding partner in our efforts to nurture cyber talent and strengthen our cyberdefense capabilities," said Piccione. "We're excited to establish this new program that will help us stay ahead of the rapidly evolving threat landscape while supporting important career pathways."

"On-the-job training is key to success in the cybersecurity field," said Russell-Bond. "This program will help students reinforce what they're learning in the classroom in a practical setting while also filling a critical gap in the state's workforce. It's a win-win."

"FTCC and the CCN are proud to collaborate with NCDIT to provide student interns who will work in concert with NCDIT staff to help strengthen the state's cybersecurity posture," said FTCC President and CCN Executive Director Dr. Mark Sorrells. "The initiative will also serve to expand the talent pool available to our public and private employers to further safeguard critical information and resources essential to our national defense. Through this learn-and-earn opportunity, students will gain valuable work experience to prepare them for careers in cybersecurity."

View photos from the launch event on NCDIT's Flickr account and video on YouTube.

Warning: New Phishing Campaign Targets Instagram Users

A phishing campaign is targeting Instagram users with phony notifications about failed login attempts, according to researchers at Malwarebytes.

Notably, the fraudulent emails contain "mailto" links rather than traditional URLs, which helps the phishing messages avoid being flagged by security filters.

"Instead of linking to a phishing website, which is most common with emails like this, both the ‘Report this user’ and ‘Remove your email address’ links are mailto links," the researchers write.

"Clicking on a mailto link opens your default email program with a pre-addressed message with the subject line ‘Report this user to secure your account’ or ‘Remove your email address from this account’ for the second link. The email addresses in these links all had unsuspicious looking domains, made to look similar to legitimate ones."

Malwarebytes offers the following advice to help users avoid falling for these scams:

- As with regular links, **scrutinize the destination of an email link.** Even if the domain looks legitimate, the email address should be one that belongs to Meta or Instagram.
- Remember that **legitimate companies will not ask you to mail them your account details, credentials or other sensitive information**.
- **If there’s urgency to respond to an email, pause before you do.** This is a classic scammer trick to get you to act before you can think.
- **Don’t reply if the warning looks suspicious in any way**. Sending an email will tell the phishers that your email address is active, and it will be targeted even more.
- **Do an online search about the email** you received, in case others are posting about similar scams.

This article is redistributed with permission from KnowBe4.

Google Report Outlines the Latest Scam Trends

Travel-themed scams targeting people preparing for their summer vacations are increasing, according to a Google report on the latest scam trends.

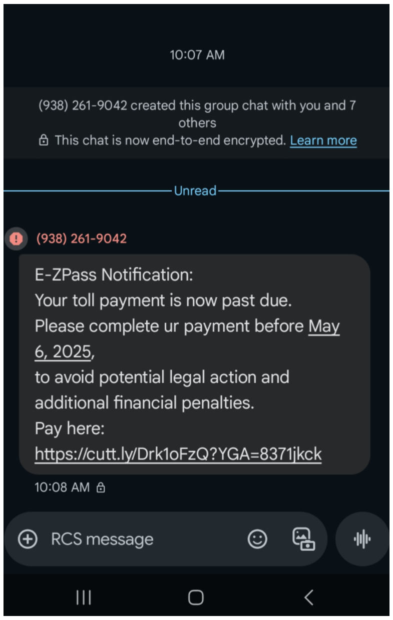
“Ahead of the summer vacation season, our teams have observed a spike in travel scams,” the researchers write. “Fake travel websites lure users into booking travel with a promise of ‘too good to be true’ prices, experiences or discounts.”

These deceptive sites often imitate well-known hotels or pose as legitimate travel agencies, a tactic particularly prevalent during holidays and major events when people book travel via messaging apps or phone.

Threat actors are also using commodity phishing kits to launch waves of package delivery scams that trick people into sending money or visiting malicious websites.

“Package tracking scams exploit the widespread use of online shopping and package delivery services by sending fraudulent messages that appear to be from legitimate delivery companies,” the researchers write. “These scams often trick users into paying additional ‘fees’ that real delivery services would never request.

“Our teams have observed these scams impersonating a wide array of global brands. A key tactic is how quickly scammers adapt their websites and messages, often changing content based on when the link is sent to a user.”



10:07 AM

(938) 261-9042 created this group chat with you and 7 others
This chat is now end-to-end encrypted. Learn more

Unread

(938) 261-9042

E-ZPass Notification:
Your toll payment is now past due.
Please complete ur payment before May 6, 2025,
to avoid potential legal action and additional financial penalties.
Pay here:
https://cutt.ly/Drk1oFzQ?YGA=8371jkck

10:08 AM

Google Report Outlines the Latest Scam Trends (cont.)

"They achieve this rapid deployment using phishing kits like Darcula and Xiu Gou, which mimic legitimate websites and brands almost instantly."

Additionally, attackers continue to bombard users with SMS phishing (smishing) messages impersonating road toll providers.

"A toll road scam involves scammers sending fraudulent text messages claiming that you owe unpaid toll fees," Google says. "These scams share patterns with package tracking schemes and are often orchestrated by the same bad actor groups."

This article is redistributed with permission from KnowBe4.

Training & Continuing Learning Resources

TEEX: Texas Engineering Extension Service:

https://teex.org

NICCS: Free Online Training Environment:

https;//niccs.gov/education-training/cisa-learning

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. Read the SAC newsletters**. 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. https://www.sans.org/newsletters/ouch

Be sure to follow the N.C. Department of Information Technology on X(formerly known as Twitter), 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.*