MONTHLY CYBERSECURITY NEWSLETTER JUNE 2025

Martha Wewer Named Chief Privacy Officer

Martha Wewer, a lawyer and experienced privacy leader in the public and private sectors, has been named NCDIT's new Chief Privacy Officer.

She oversees the Office of Privacy and Data Protection, within NCDIT's Enterprise Security and Risk Management Office, under State Chief Information Security Officer Bernice Russell-Bond. Wewer leads the office's mission to manage the state's privacy program, provide guidance and support to state agencies protecting the privacy of residents' data, and ensure transparency in the use of data.

Previously, she served as the global privacy officer at RTI International for 10 years and privacy officer at the State Health Plan for five years in addition to practicing law privately.

She is a Certified Information Privacy Professional and holds a law degree and bachelor's in political science from the University of San Diego.

Mike Long Named NCDIT Agency CISO

NCDIT welcomes Mike Long as agency chief information security officer. A Raleigh native, he looks forward to strengthening cybersecurity for NCDIT and the state and local agencies we serve.

Long brings more than 15 years of cybersecurity leadership for the federal government, military and the energy, consulting and financial services sectors. His breadth of expertise ranges from governance, risk and compliance to testing enterprise security at security operations centers.

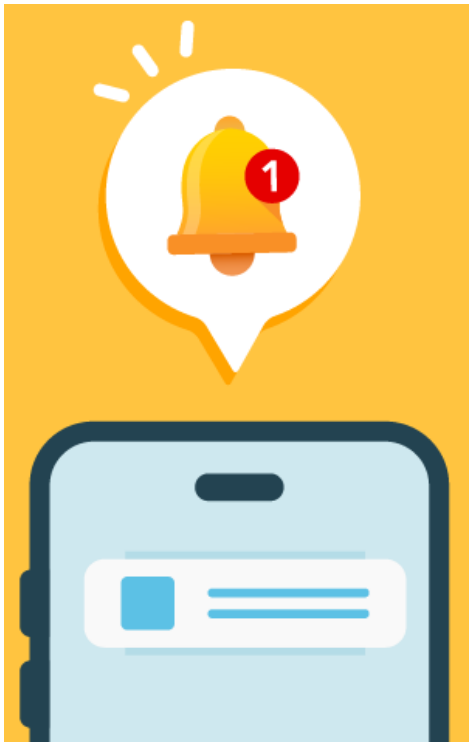
Long holds bachelor's and master's degrees in computer science from North Carolina Agricultural and Technical State University and a master's degree in business administration from the University of Virginia.

JaJuan Garvin Joins NCDIT's Security Operations Center as an Analyst

JaJuan Garvin joins NCDIT as an analyst in the Security Operations Center, which plays a critical role in responding to cybersecurity incidents across the state.

Before becoming a full-time employee, Garvin completed a six-month apprenticeship at the NCDIT Security Operations Center through the ISG Cybersecurity Apprentice Program for veterans. He served in the U.S. Army for seven years as a signal support specialist, delivering IT in various capacities.

Garvin also worked as an IT analyst at Duke University School of Nursing. He holds a bachelor's degree in cybersecurity from Purdue University.



Scam Alert: NCDMV Warns of Fraudulent Text Scams

The N.C. Division of Motor Vehicles is alerting the public about a surge in fraudulent text message scams targeting residents.

These scams falsely claim to request payment for fees, fines or tolls and may appear to come from the NCDMV. Other fraudulent text scams have attempted to collect tolls from North Carolina residents.

NCDMV does not and will never request payments via text message.

Anyone who receives any suspicious texts are encouraged to report them as spam and delete them immediately. Do not click on any links or provide personal information in response to these messages.

Protect yourself from scams:

- Be cautious of unsolicited texts requesting payment or personal information.
- Verify any NCDMV-related inquiries through official channels.
- Report suspicious texts to your mobile carrier or the Federal Trade Commission.
- Learn more about how to identify phishing texts and scams.

Five Scams to Avoid This Summer Travel Season

These days, you can't let your electronic guard down when traveling on either business or vacation. As the summer travel season begins, here are a few popular scams to watch out for.

Fake Free Wi-Fi Network – You find these when looking for access to your business account while staying at hotels and other public places. A network might have the hotel's name, but scammers are listening in to your confidential communication and online activity. Verify with the hotel or other locations before you log on to any free Wi-Fi.

Fake Software Update – A traveler attempting to set up a hotel internet connection sees an update pop-up for a popular software product. But click on it, and malware will install on your device. Always update your laptop before you leave home or work, and never do updates while you are traveling.

Pizza Delivery – In this scam, you find a flyer for a deal on food slipped under your hotel door. When you call to order, they'll take your card data but never deliver your order because the flyer was a scam. Get food recommendations from the concierge.

An ATM Security Team – ATM skimmers are almost impossible to detect with the naked eye. Thanks to a slimmed-down profile, these devices sit within the throat of an ATM card slot, capturing data when you slide your card inside. A spy camera then tapes as you enter your personal identification number (PIN) on the keypad. Especially when on the road, cover your hand when typing in your PIN.

Late Night Hotel Front Desk Call – You get a call alerting you that there is a problem with your credit card and requesting that you verify the number. Except it's a scammer, who now has your number or perhaps just skimmed your card at the ATM and needs some more info to make a fake duplicate card so they can grab the maximum cash. Especially when you travel, never give out credit card information if you did not initiate the call.

This article is redistributed with permission from KnowBe4.

ICYMI: Business Continuity and Resilience Awareness Week Webinar Recordings

During Business Continuity and Resilience Awareness Week on May 19-23, NCDIT experts explored how AI is being leveraged to predict and handle potential disruptions to an organization.

Catch all the recorded webinars featuring NCDIT experts: AI Policy and Governance Executive I-Sah Hsieh, State Chief Information Security Officer Bernice Russell-Bond, Chief Architecture and Innovation Director Keith Briggs and AI architect Justin Vargas.

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.*