# MONTHLY CYBERSECURITY NEWSLETTER MARCH 2025

## Bernice Bond Named NCDIT Chief Information Security Officer

The N.C. Department of Information Technology welcomed Bernice Bond as the new chief information security officer (formerly the chief risk officer role), beginning Monday, March 3.

Bond is a cybersecurity leader with more than 25 years of experience. She owned and ran her own IT risk management consulting firm for nearly 20 years in the private sector, and she has held a variety of executive-leadership roles focused on cybersecurity operations, risk management, IT governance, incident management and auditing. She was named the NC TECH Association's 2024 CISO of the Year and serves on the association's advisory board.

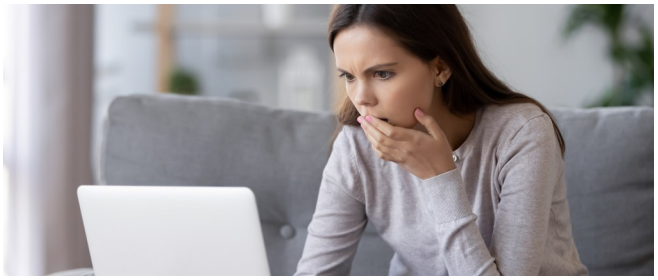
Bond enjoys leading teams to empower all staff in fostering an effective cybersecurity culture. She holds a Bachelor of Science in accounting from Hampton University and a Master of Business Administration for the University of Phoenix in addition to CISSP, PMP and ITIL v3 Foundations certifications.

## Protect Yourself from Job Termination Scams

A wave of phishing attacks is tricking employees by informing that they've been fired or let go, warns ESET, a cybersecurity company. These emails are designed to make the user panic and act quickly to see if they've actually lost their job.

If a user falls for the attack, they'll be tricked into downloading malware or handing over their login credentials. "Social engineering tactics used in phishing aim to create a sense of urgency in the victim, so that they act without thinking things through first," the researchers write. "And you can't get more urgent than a notice informing you that you have been dismissed. It could arrive in the form of an email from HR or an authoritative third party outside the company.

"It may tell you that your services are no longer required. Or it may claim to include details about your colleagues that are too hard to resist reading. The end goal is to persuade you to click on a malicious link or open an attachment, perhaps by claiming that it in-



cludes details of severance payments and termination dates."

ESET says users should be on the lookout for the following red flags associated with phishing attacks:

· An unusual sender address that doesn't match the stated sender. Hover your mouse over the "from" address to see what pops up. It may be something completely different, or it could be an attempt to mimic the impersonated company's domain, using typos and other characters (e.g., m1crosoft[.]com, @microsfot[.]com).

· A generic greeting (e.g., "dear employee/user"), which is certainly not the tone a legitimate termination letter would take.

· Links embedded in the email or attachments to open. These are often a tell-tale sign of a phishing attempt. If you hover over the link, and it doesn't look right, all the more reason not to click.

· Links or attachments that don't open immediately but request you to enter logins. Never do so in response to an unsolicited message.

· Urgent language. Phishing messages will always try to rush you into making a rash decision.

· Misspellings, grammatical or other mistakes in the letter. These are becoming rarer as cybercriminals adopt generative AI tools to write their phishing emails, but they're still worth looking out for.

· Going forward, be on your guard for AI-aided schemes where scammers could use deepfake audio and video likenesses of actual people (that of your boss, perhaps) to trick you into giving up confidential corporate information.

*This article is redistributed with permission from KnowBe4.*

## Protect Your Devices: Mobile Phishing Attacks Bypass Desktop Security Measures

Phishing attack specifically tailored for mobile devices are surging, warns Zimperium, a mobile security platform provider. These attacks are designed to evade desktop security measures in order to breach organizations through employees' smartphones.

Mobile phishing includes SMS phishing (smishing), QR code phishing (quishing), voice phishing (vishing) and mobile-targeted email phishing.

"When the same link is accessed from a desktop environment, the attack chain is terminated, making detection and analysis significantly more challenging. This is a unique and clever tactic for bypassing standard email and network security solutions, as few enterprises and users employ security on the mobile device."

Threat actors are also using links that redirect to different destinations depending on whether the user is on a mobile device or desktop.

"Our analysis of verified phishing sites reveals a sophisticated pattern of desktop redirection to legitimate services as an evasion technique, with Google and Facebook being the primary destinations," the researchers write. When accessed from desktop devices, these malicious sites redirect users to legitimate platforms – a technique that significantly complicates automated analysis and detection. This evasion tactic allows attackers to maintain prolonged campaign effectiveness by appearing benign to security tools while still targeting mobile users with malicious content.

New-school security awareness training can give your organization an essential layer of defense against evolving social engineering attacks.

"As organizations increasingly rely on mobile devices for business operations, including multifactor authentication and mobile-first applications, mobile phishing poses a severe risk to enterprise security," Zimperium says.

"Attackers are exploiting security gaps in cloud and mobile business applications, expanding the attack surface and increasing exposure to credential theft and data compromise. Traditional anti-phishing measures designed for desktops are proving inadequate, requiring a shift to mobile threat defense solutions on the mobile device."

*This article is redistributed with permission from KnowBe4.*

## 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

## 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.*