Monthly Cybersecurity Newsletter

November 2024

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

AI Intersects with Cybersecurity, Privacy at Two-Day NCDIT Symposium

The N.C. Department of Information Technology has partnered with Government Technology to host the N.C. Cybersecurity and Privacy Symposium – a two-day event focused on artificial intelligence and innovation and how AI intersects with cybersecurity and privacy.

"As state government's primary information technology service provider, one of NCDIT's foremost responsibilities is to stay on the cutting edge of emerging technologies such as generative AI, and the ways they can be used for both good and harm," Secretary and State Chief Information Officer Jim Weaver said. "This important event examines AI, cybersecurity and privacy, and their implications for state and local government and the people we serve."

The free, in-person event will be Dec. 4-5 at the Raleigh Convention Center and is open to all who work in the public sector. For more information and to register, visit https://it.nc.gov/symposium.

Cybersecurity and the protection of sensitive information are becoming increasingly complex with the rapidly growing popularity of new technologies such as generative AI.

While this evolution in North Carolina's technology landscape offers exciting ways to innovate like never before, it also introduces concerns about data privacy, integrity and security that must be addressed to safeguard the state and promote its best interest.

Day 1 of the symposium is AI Day, focused on demystifying AI and showcasing government solutions and innovations using AI. Day 1 is aimed at a nontechnical audience with technical attendees also encouraged to participate.

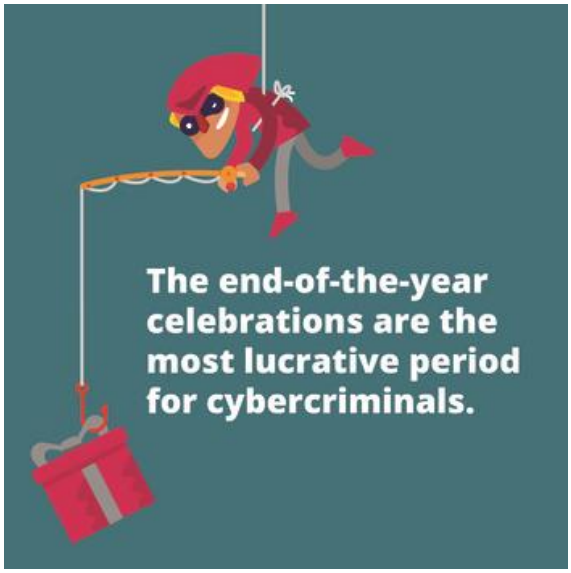
Day 2 is focused on cybersecurity and privacy and the role they play in the future of our state, including where they intersect with AI.

Information security expert and adviser Jeff Man is the scheduled keynote speaker on Day 2. A 37-year veteran in IT and information security, including cryptography and risk management, Man is also co-host of two podcasts – Paul's Security Weekly and Tribe of Hackers.

State Chief Risk Officer Torry Crass and Chief Privacy Officer Cherie Givens are also among those scheduled to speak. Stay tuned to it.nc.gov/symposium for more updates to the agenda.

Smart Shopping: Protect Yourself Online This Holiday Season

The holiday season is a time for celebration, gift-giving and often a significant amount of online shopping. Online shopping is a huge time-saver, especially for those juggling busy work schedules with little time to spare.



With this convenience, however, also comes the potential for security risks, including fraud, identity theft and scams. Cybercriminals are particularly active during the holidays, targeting shoppers with phishing emails, fake websites and other schemes.

The first line of defense is to shop from reputable websites with a proven track record, such as major retailers or well-known local businesses. By choosing websites with “https” instead of “http,” you can ensure a secure connection. You should also avoid clicking on links in unsolicited emails or ads. Typing the store’s website URL into the browser will guarantee that you are on the official site.

Phishing scams are also at an all-time high. Phishing emails can look like they are from a legitimate company, but they often contain subtle clues, such as misspelled words, poor grammar or slightly altered email addresses. Be very wary of emails or messages that ask for sensitive information or urge you to act immediately. Legitimate companies rarely ask for sensitive information. And remember, do not click on links of unsolicited emails or messages. If a deal sounds too good to be true, it probably is.

One of the most important things you can do while online shopping is to protect your passwords. Use strong, unique passwords – no repeats. Reusing passwords can make it easier for hackers to access multiple accounts linked to your name. Remember to also use multifactor authentication for double protection on your shopping accounts.

Always check your bank accounts for unauthorized transactions. The sooner a problem is identified, the quicker it can be resolved. Opting for secure payment methods enhances fraud protection on these accounts. Try to avoid using debit cards or wire transfers because they could leave you more vulnerable.

Staying safe while shopping online during the holiday season requires a proactive approach to cybersecurity. A little caution can go a long way. By staying sharp and following these tips, you can keep your data safe and focus more on the fun of the holiday season.

Happy safe shopping, everyone!

Humans: The Unexpected Weak Link in Cybersecurity

With all of the high-tech defenses that surrounded us (e.g., firewalls, encryption and AI), one would think that we would be bulletproof against cyberattacks. But there is one flaw that even the smartest systems cannot fix: human error.

If you receive a link from your bank or a coworker asking you to click for more information, what is the probability you will click the link? Is the link legitimate or is it a trap? Cybercriminals are masters of deception, using phishing scams to outsmart even the most cautious of us. One wrong click, and boom – your data is theirs.

Let's be honest. How many of us reuse the same password across different accounts? Guilty as charged. Hackers love it when we're lazy with passwords. One weak password can unlock an entire chain of accounts, making their job way too easy.

You would be surprised to know how many cyberattacks are caused by simple mistakes. Most employees are not cybersecurity pros, and without proper training, they can unintentionally invite hackers in. One employee might download an untrustworthy file or click on a risky link, setting off a chain reaction that compromises a whole network. Here, proper employee training could eliminate some of these errors.

Here is the silver lining. While humans are most often the weakest link, they can also be the strongest defense. With the right training, people can learn to spot phishing scams, create strong passwords and avoid risky behaviors. Teaching humans to be cyber savvy is the key to closing the human gap in security.

Public Wi-Fi Networks: Why They're More Dangerous Than You Think

Public Wi-Fi networks may seem like a great way to stay connected on the go, but they come with significant security risks. Here's why.

Most public Wi-Fi networks lack strong encryption. This means that when you are connected, your data isn't protected as it travels between your device and the network, leaving it vulnerable to interception. Hackers can "sniff" traffic on these networks, capturing information such as your passwords, banking details and other sensitive information.

One of the most common threats on public Wi-Fi is a man-in-the-middle attack. In this scenario, a hacker positions themselves between your device and the network, eavesdropping on the information being sent and received. This can lead to stolen credentials or the installation of malware on your device.

Hackers also create fake Wi-Fi networks that appear legitimate. These rogue hotspots are designed to trick users into connecting and giving the attacker direct access to any data shared over the network. Once connected, anything from email to online banking credentials could be stolen.

Another issue with public Wi-Fi networks is the use of outdated security protocols like wired equivalent privacy (WEP), which are easy to crack.

Some hackers use public Wi-Fi networks as a vehicle to distribute malware. They can inject malicious software into the files and websites you access while connected. Once malware is installed, it can give the attacker control of your device, enabling them to steal data, track your keystrokes or spy on you.

To protect yourself, avoid entering sensitive information when connected to public Wi-Fi. Use a virtual private network (VPN) for secure browsing, and if possible, rely on your phone's data connection for task involving personal data.

Is Disabling Clickable URL Links Enough?

Is disabling clickable URL links in emails enough protection by itself to potentially not need security awareness training and simulated phishing?

It is understandable why this misperception might exist. Many anti-phishing educational lessons discuss the need for people to evaluate all URL links before clicking on them. This is why it is best to “Think Before You Click!”

But no, disabling URL links alone is not enough. This article will discuss why.

Disabling all URL links in all emails by default is a good way to decrease cybersecurity risk. Essentially, what this control does is remove the included “hyperlinking” property of the URL and render the URL in plaintext, so it cannot be clicked on by a mouse or easily selected from the keyboard to automatically open in an Internet browser at the provided location address.

There are many organizations (including the U.S. Department of Defense) and cybersecurity guides that recommend rendering all URLs as plaintext. For that reason, Microsoft Outlook and many other email applications have had that option for well over two decades.

And, yes, disabling clickable URLs by default will decrease cybersecurity risk. It makes it harder for someone to see a link, quickly click on it and launch the content associated with it. At the very least, the user will have to manually copy the link and insert it into a browser address bar. Requiring manual action to launch a link is proven to decrease the percentage of people who will go to the URL. Phishers hate it.

Of course, plaintext links are a huge inconvenience to everyone who simply wants to click on a legitimate link and get taken immediately to the correct place. If most of the emails ending up in someone’s inbox are not malicious, then this means it’s a huge amount of inconvenience for most people in most scenarios. This makes it less likely that an organization will implement it. But for those who do and suffer the inconvenient consequences, it does reduce cybersecurity risk from email social engineering.
But not all risk.

People Will Just Copy the Links

People appropriately motivated will simply copy the links into their browser and go there anyway. Disabling hyperlinks does decrease the chance that someone will click on a particular link, but not everyone. We all know how to copy and paste something. It will slow the average user down by less than 10 seconds.

Users should be trained in how to recognize rogue URLs.

KnowBe4 even recently covered “clickjacking” in its blog, in which a hacker goes beyond merely convincing a victim to type in a URL but also gets the user to run more complex commands or PowerShell scripting at the user’s command line.

It Doesn’t Stop All Email-Based Social Engineering

Most email-based social engineering does include a URL link that the phisher is hoping the potential victim clicks on, but many don’t. Emails that include a (QR) code instead of a link are on the rise. Callback phishing, which is a phishing email that induces potential victims to call a phone number, often doesn't include a URL link. Or the link is included as part of a graphic that the user has to re-type anyway.

Email Isn’t the Only Phishing Medium

Social engineering and phishing can occur across any communication medium, including in-person, phone, SMS message, social media, chat apps and channels, QR codes and even TV. If you stop anti-social engineering training, you’re increasing the risk that someone will be compromised on non-email channels.

It Doesn’t Stop Users at Home

Many users are compromised at home, on their home devices, where URL blocking isn’t likely to be enabled. A personally compromised employee (e.g., dealing with a phishing attack, stolen money) is a less productive employee. And many employees are compromised at home, with the attacker using the personal compromise as a starting off point to attack their employer.

Good Security Awareness Training

Good security awareness training shouldn’t just include education on email phishing and simulated email phishing campaigns. It should also include training about all types of phishing and how they occur on all types of devices and mediums. You don’t want your employee being tricked by a phone call any more than an email attack.

Your training and testing should include all sorts of things to improve human risk management, beyond simply phishing education and testing. For example, you should be including education on a variety of topics, including compliance topics, such as password policy, following company policies, securing company devices when traveling or in your car and not leaving confidential information out in the open or discussing in public. It should include videos, posters, games and in-person meetings. And all of that is improved and facilitated by security awareness training that is hosted in email.

If you're doing it right, you're trying to change the organization's culture to be more cybersecurity-aware, and if you aren't training and doing simulated phishing exercises that mimic real-world events, you aren't doing that as efficiently as you might otherwise be doing it.

So go ahead, and disable URL hyperlinks if that’s what you and management want to do. But don’t stop training and simulated email phishing. There’s a whole lot more involved in creating a great cybersecurity culture than just hyperlinks and email.

Hurricane Deepfakes Flood Social Media

Since Hurricane Helene caused major damage and Hurricane Milton left a path of destruction across Florida, deepfakes have been spreading misinformation on social media.

Platforms like Instagram, Facebook and X are seeing an influx of these manipulated images, confusing users and distorting the reality of the situation.

According to Forbes, one of the most viral images – a young girl stranded in floodwaters clutching a drenched puppy – has garnered more than a million views on X alone.

Kevin Guo, chief executive officer of the content moderation platform Hive, confirmed the image was AI-generated and is being used to sow misinformation about the federal government's response to the hurricane.

Other false images include a man wading through water with a dog, law enforcement officers engaged in relief efforts and even a doctored photo of Donald Trump in a life jacket navigating muddy waters. While these AI-generated images may seem harmless at first glance, you should understand that they pose a threat. A raft of scams is possible with this type of social engineering.

Crooks are impersonating the Federal Emergency Management Agency and other disaster relief organizations in order to trick people into sending money or handing over personal information. Cybercriminals always attempt to exploit natural disasters with social engineering attacks, and similar scams should be expected in the aftermath of Hurricane Milton.

One particularly cruel scam is directly targeting victims of Hurricane Helene who are seeking financial assistance. "One of the first major threats we observed is FEMA claim scamming, where cybercriminals pose as legitimate FEMA assistance providers to steal personal information and funds," researchers at Veriti say. "A VIP member on a hackers forum, under the alias 'brokedegenerate,' recently posted about a new scam targeting Florida residents affected by the hurricane.

"On the forum, the scammer shares tactics for creating fake FEMA assistance claims, with detailed instructions on how to deceive victims and siphon off funds intended for disaster relief. This kind of scam is particularly dangerous, as victims are already in a vulnerable position due to the natural disaster."

The researchers have also observed a surge in hurricane-related phishing domains, such as "hurricane-helene-relief[.]com."

"By using hurricane-related terms and associating themselves with disaster relief, these domains aim to create a sense of urgency, making it more likely that victims will fall for the phishing schemes," the researchers write. "Attackers will likely send phishing emails directing recipients to these websites, claiming to offer relief services or grant applications. Once victims input their personal details, the attackers can use or sell the data for financial gain."

During times of crisis, it's crucial to verify the information you encounter online. Sharing false or misleading images can divert attention away from real needs. As AI technology continues to advance, so does its potential to mislead – and staying vigilant in the face of these tactics is more important than ever.

Training & Continued 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://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

SANS OUCH. Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

- **Nov. 8:** SANS Webinar: Fall Cyber Solutions Fest 2024: Threat Hunting and Intelligence Track
- **Nov. 8:** SANS Webinar: Fall Cyber Solutions Fest 2024: Zero Trust Track
- **Nov. 11:** SANS Webinar: Offensive Security Operations – Penetration Testing of the Future
- **Nov. 12:** SANS Webinar: Understanding the Risk Management Mandates in 2024 Cybersecurity Regulations
- **Nov. 20** SANS Webinar: Clearing the Fog: Detection and Defense Against AWS Persistence Techniques

View a list of upcoming SANS webcasts.

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.
