Monthly Cybersecurity Newsletter

May 2022 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Rob Main

Human Error Ranked as the Top Cybersecurity Threat

A recent report provides new insights into the state of data security by showing a clear focus on the weakest part – the end users – and organizations doing little to address it. Within Thales' 2022 Data Threat Report, the following oberservations are made:

- Human error is seen as the highest threat to organizational security, with 38% of organizations ranking it as the top threat. Nation states was only a top concern for 28% of organizations.
- 29% of organizations ranked "accidental human error" as the top threat (and again for reference, only 17% ranked external attackers with financial motivation as a top threat).
- 79% of organizations are concerned about the security risks with an increasingly remote work force.

Users play a significant role in making an organization insecure. According to Alan Suderman at Fortune, organizations in the U.S. lost $2.4 billion due to business email compromise (BEC) scams (also known as CEO fraud) last year. "BEC scammers use a variety of techniques to hack into legitimate business email accounts and trick employees to send wire payments or make purchases they shouldn't," Suderman writes. Organizations of all sizes need to be wary of BEC scams. "Almost every enterprise is vulnerable to BEC scams, from Fortune 500 companies to small towns," Suderman writes.

"Targeted phishing emails are a common type of attack, but experts say the scammers have been quick to adopt new technologies, such as 'deep fake' audio generated by artificial intelligence to pretend to be executives at a company and fool subordinates into sending money."

With the significance in end user security, we might expect to see effort spent on ways to secure the user. But according to the Thales' report, organizations are prioritizing network security (e.g., intrusion prevention solutions, gateways, firewalls), key management, cloud security and zero trust solutions.

It seems like the focus is way too much on trying to prevent data from leaving, instead of stopping attackers from ever getting in. More focus on security awareness training is needed to reduce the threat of phishing, a primary attack vector in nearly every kind of cyber attack. This kind of training helps to establish good cyber hygiene, a sense of vigilance, and has been shown to reduce the risk of users falling for social engineering tactics employed within phishing attacks.

Remember … cybersecurity is everyone's responsibility..

FBI Warns of Bank Fraud Smishing Campaign

The FBI has warned of a smishing campaign that is targeting people in the U.S. with phony bank fraud notifications. The text messages inform users that someone has attempted to initiate a money transfer on their account.

"The actors – who typically speak English without a discernible accent – then call the victim from a number which appears to match the financial institution's legitimate 1-800 support number and claim to represent the institution's fraud department," the FBI says. "Once the actor establishes credibility, they walk the victim through the various steps needed to 'reverse' the fake instant payment transaction referenced in the text message."

"In these schemes, background information on the victims appears to have been well researched. In addition to knowing the victim's financial institution, the actors often had further information such as the victim's past addresses, Social Security number and the last four digits of their bank accounts." This information is used to convince customers that the request is legitimate.

The FBI offers the following advice to help people avoid falling for this scam:

- Do not respond directly to calls or texts regarding possible fraud or unauthorized transfers. Be wary of unsolicited requests to verify account information. Cyber actors can use email addresses and phone numbers that might appear to be from a legitimate financial institution.
- If you receive an unsolicited request to verify account information, contact the financial institution's fraud department through verified telephone numbers and email addresses on official bank websites or documentation – not through those provided in texts or emails.
- Enable multi-factor authentication for all financial accounts, and do not provide MFA codes or passwords to anyone over the phone.
- Understand that financial institutions will not ask customers to transfer funds between accounts to help prevent fraud.
- Be skeptical of callers who provide you with your personally identifiable information, such as Social Security numbers and past addresses, as proof of their legitimacy. The proliferation of large-scale data breaches over the last decade has supplied criminals with enormous amounts of personal data, which may be used repeatedly in a variety of scams and frauds.

Privacy Monthly Meeting – May 31 Kick-off

NCDIT Chief Privacy Officer Cherie Givens will hold the department's first Privacy Monthly Meeting from 10-11 a.m. on May 31. All privacy points of contact and other state employees working on privacy matters, or interested in privacy, are invited. If you have been identified by your agency as their privacy point of contact, you should be receiving an invitation in early May.

If you are a state employee with an interest in privacy, please send your name and contact information to ditprivacy@nc.gov to be added to the invite list. The chief privacy officer looks forward to meeting each of you and learning about your privacy needs.

Save the date for the North Carolina Cybersecurity Symposium on May 12-13. The symposium will be an exciting new venue for deepening knowledge of critical cybersecurity issues and opportunities, featuring business and government professionals, academic leaders, researchers and students. The event will be hosted by the Partnership for Cybersecurity Excellence (NC-PaCE) and will take place on the North Carolina State University campus in Raleigh.

The symposium will feature keynotes from industry leaders, lectures and panels with cybersecurity expertise in technical, legal and compliance fields, classroom training and tutorial sessions. It will also showcase business solutions, academic research and student poster sessions. This forum will focus on today's most critical and pressing cybersecurity issues, enabling participants to share and exchange ideas and knowledge, explore emerging opportunities in research, education, training, certification and talk with leading products and services providers.

For more infromation about the symposium and to register for the event, click here.

Business Continuity Awareness Week 2022

Business Continuity Awareness Week (BCAW) 2022 will be May 16-20. The theme this year is **Building Resilience in the Hybrid World**. In addition to the new theme, BCAW will include even more resources, webinars, content and competitions.

In the last 24 months, the world has seen a rise in the adoption of hybrid work models – where employees have the flexibility to work part in the office and part remote. This new work environment has compelled organizations to rethink the way they embed, validate and raise awareness among their staff of business continuity plans. The aim of BCAW 2022's theme is to equip organizations and business continuity professionals with the necessary tools to embed and improve awareness of business continuity in this new workplace reality.

More information about BCAW 2022 may be found here.

How to avoid **Social Engineering**

WENDY'S TIPS

1 Think before you Click!

Is the story really plausible?
Make sure that information is actually genuine, for example by calling back.

2 Don't let them pressure you!

Does something have to be done very quickly or are you being threatened with severe consequences?
Then be particularly wary!

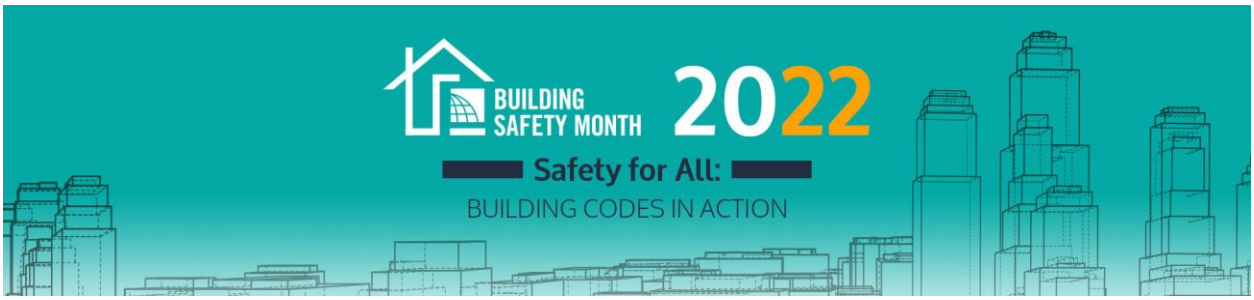
3 Speak to others!

When something unusual happens, talk to members of your team. Ask again, especially for unexpected messages or phone calls.

4 Report incidents!

Even if you've spotted the scam, report it immediately. You might not be the only one being targeted by attackers.

exploqii



May is Building Safety Month, so set your calendar reminders, and do your part to support building safety. This international campaign reinforces the need for the adoption of modern, regularly updated building codes and helps individuals, families and businesses understand what it takes to create safe and sustainable structures. The following are some things you can do to support this effort.

- **Educate your community** with materials from buildingsafetymonth.org. There are numerous helpful resources, such as the International Code Council's campaign toolkit, safety tip sheets, and kids' corner materials.
- Work with your local city officials to **issue a proclamation.** Find out how with ICC's Proclamation Guide.
- **Promote Building Safety Month** through social media and word of mouth. Tag your posts with #BuildingSafety365.

FEMA Offers Online Train-the-Trainer for CERT Basics Course

FEMA's Emergency Management Institute is offering for free an online version of its K0428 CERT Train-the-Trainer course, which prepares participants to deliver FEMA's Community Emergency Response Team (CERT) Basic Training course.

2022 Course Dates:

- June 7, 8, 9, 14, 15 and 16 (12-4 p.m. EST)
- July 12, 13, 14, 19, 20 and 21 (1-5 p.m. EST)
- Sept. 6, 7, 8, 13, 14 and 15 (12-4 p.m. EST)

Each class is limited to 20 students and meets four hours a day three days a week for two weeks. Students must attend all sessions. These courses will be delivered via Adobe Connect, and participants should familiarize themselves with it beforehand. No Adobe Connect account or downloads are required. Students must have a FEMA student identification number, computer with microphone, speaker and stable access to the internet. Visit the FEMA Student Identification System to obtain a SID.

Prerequisites:

- A referral from a CERT-sponsoring agency, typically a local, regional, or state government agency.
- If you are not a first responder, the CERT Basic Training is required.
- For current first responders, IS-317: Introduction to CERT will familiarize you with the CERT Program.

Prospective students should apply through the Emergency Management Institute's online admissions system. The course offers 1.3 continuing education units. Please refer to the FEMA Emergency Management Institute for course date availability.

CYBERSECURITY NEWSLETTERS

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

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/resources/?type=newsletter

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

May

- National Building Safety Month
- May 1: National Hurricane Preparedness Week
- May 11: You Are the Help Until Help Arrives Webinar (1-3 p.m. ET)
- May 12-13: North Carolina Cybersecurity Symposium
- May 12: SANS Webinar: DevSecOps Automation for Cloud Native Security
- May 18: Selfcare for Disaster Responders and Healthcare Workers Webinar (1-2 p.m. EST)
- May 25: Special offering of: You Are the Help Until Help Arrives Webinar, in honor of Stop the Bleed Month (5-7:30 p.m. EST)
- May 16: Business Continuity Awareness Week
- May 18: SANS Webinar: SANS 2022 SOC Survey
- May 25: SANS Webinar: Best Practices for Incident Preparedness in a Serverless World
- May 30: Memorial Day
- May 31: Privacy Monthly Meeting (10-11 a.m. EST)
- May 31: Heat Safety Awareness Day

June

- June 8: Organizations Preparing for Emergency Needs (OPEN) Part 1 Webinar (1-2:30 p.m. EST)
- June 15: Organizations Preparing for Emergency Needs (OPEN) Part 2 Webinar (1-2:30 p.m. EST)
- June 19: National Lighting Safety Awareness Week
- June 22: Psychological First Aid Webinar (1-2 p.m. EST)

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on 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.*