Monthly Cybersecurity Newsletter

June 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

Cyberattack Hits Another Major Health Care System

Nearly three months after a cyberattack on Change Healthcare, a division of United Healthcare Group, cybercriminals have targeted another major healthcare system – St. Louis-based Ascension Healthcare.

Reports within Becker's Hospital Review and The HIPPA Journal indicate that the May attack affected more than 140 hospitals and 40 senior living facilities across 19 states and the District of Columbia.

A team of network engineers detected unusual activities on Ascension systems, leading the team to identify the attack. It disrupted clinical operations throughout the system's network, prompting Ascension to recommend that its healthcare clients temporarily cut off network connections while the issue is addressed.

Ascension responded swiftly by initiating procedures to minimize the impact on patient care.

Although immediate reports did not confirm the exact nature of the attack (i.e., whether it involved ransomware), the situation was serious enough for Ascension to notify the appropriate authorities and initiate an ongoing investigation.

The incident highlights the increasing challenges and threats faced by health care systems in cybersecurity, emphasizing the importance of strong security measures and rapid response strategies to safeguard sensitive patient data and medical services.

FBI Warns of AI-Assisted Phishing Campaigns

The FBI's San Francisco division warns that threat actors are increasingly using artificial intelligence tools to improve their social engineering attacks.

"AI provides augmented and enhanced capabilities to schemes that attackers already use and increases cyber-attack speed, scale and automation," the FBI says.

“Cybercriminals are leveraging publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns, exploiting the trust of individuals and organizations alike. These AI-driven phishing attacks are characterized by their ability to craft convincing messages tailored to specific recipients and containing proper grammar and spelling, increasing the likelihood of successful deception and data theft."

Attackers are exploiting AI tools to create deepfakes that convincingly impersonate real people.

“In addition to traditional phishing tactics, malicious actors increasingly employ AI-powered voice and video cloning techniques to impersonate trusted individuals, such as family members, co-workers or business partners,” the FBI says. “By manipulating and creating audio and visual content with unprecedented realism, these adversaries seek to deceive unsuspecting victims into divulging sensitive information or authorizing fraudulent transactions.”

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

- Stay vigilant. Be aware of urgent messages asking for money or credentials. Businesses should explore various technical solutions to reduce the number of phishing and social engineering emails and text messages that make their way to their employees.

  Additionally, businesses should combine this technology with regular employee education and inform employees about the dangers of phishing and social engineering attacks and the importance of verifying the authenticity of digital communications, especially those requesting sensitive information or financial transactions.

- Implement multifactor authentication. Utilize multifactor authentication solutions to add extra layers of security, making it more difficult for cybercriminals to gain unauthorized access to accounts and systems.

This article is redistributed with permission from KnowBe4.

Scam Service Attempts to Bypass Multifactor Authentication

A scam operation called “Estate” has attempted to trick nearly 100,000 people into handing over multifactor authentication codes over the past year, according to Zack Whittaker at TechCrunch.

The scammers target users of well-known brands and banks, such as Amazon, Bank of America, Capital One, Chase, Coinbase, Instagram, Mastercard, PayPal, Venmo and Yahoo.

“Since mid-2023, an interception operation called Estate has enabled hundreds of members to carry out thousands of automated phone calls to trick victims into entering one-time passcodes,” Whittaker writes.

“Estate helps attackers defeat security features like multifactor authentication, which rely on a one-time passcode either sent to a person’s phone or email or generated from their device using an authenticator app. Stolen one-time passcodes can grant attackers access to a victim’s bank accounts, credit cards, crypto and digital wallets, and online services.”

Allison Nixon, chief research officer at Unit 221B, told TechCrunch, “These kinds of services form the backbone of the criminal economy. They make slow tasks more efficient. This means more people receive scams and threats in general. More old people lose their retirement due to crime compared to the days before these types of services existed.”

Multifactor authentication offers a crucial layer of defense against hackers, but users need to be aware that social engineering attacks can still bypass these measures.

“While services that offer one-time passcodes still provide better security to users than services that don’t, the ability for cybercriminals to circumvent these defenses shows that tech companies, banks, crypto wallets and exchanges, and telecom companies have more work to do,” Whittaker says.

This article is redistributed with permission from KnowBe4.

Use of Private Data for AI Model Development

Have you ever wondered how your favorite apps just seem to "get you"? That’s artificial intelligence (AI) working its magic.

Although AI is making our lives easier, it's also giving cybercriminals a new toolkit to manipulate. Let's dive into this wild world where efficiency and security are constantly at odds.

Businesses are all in on AI, hoping to enhance the user experience and automate repetitive tasks. Sounds great, right? But guess what? Bad actors are on it too, using AI to launch sneakier, more sophisticated attacks. It's a classic case of the double-edged sword.

AI needs a lot of data to work its wonders. This data often comes from us – our interactions, messages, and more. It’s like a giant practice session for AI to learn and improve. But here’s the kicker: all this personal and sensitive data could be at risk. Imagine if it falls into the wrong hands? Yup, that’s a potential nightmare.

One of the big issues with AI is its black-box nature. It makes decisions, but how does it get there? That is the mystery. Users assume their data is safe and private when using different apps, but AI is always watching and learning. Is this harmless optimization, or a sneaky breach of our privacy rights?

Picture this: a hacker gets their hands on all the data AI uses to learn about us. They could craft attacks that are spot-on, knowing exactly how to manipulate their targets. Scary, right? We all want efficiency, but not if it means opening the door to cyber-attacks.

Remember the attack on Slack’s platform in December 2022? Hackers managed to breach their private GitHub repositories using stolen employee tokens. Slack, one of the top communication platforms, suddenly became a goldmine for cybercriminals. According to Tech Radar, over 20 million users, including numerous businesses, were at risk. AI’s data-mining capabilities, while incredible, can also lead to terrifying scenarios like this.

Sure, private data is crucial for AI’s growth, but we need to balance this with protecting individual privacy and adhering to ethical standards. It's a tightrope walk, but one we must navigate carefully to avoid falling into a privacy pitfall.

So, next time you marvel at how an app knows you so well, remember there’s a lot going on behind the scenes. AI is powerful and impressive, but with great power comes great responsibility – for both users and developers.

The Rise of Tech Support Scams Targeting the Elderly

In recent years, we have witnessed a surge in cybercrimes exploiting older adults. Despite being faced with other forms of cyberattacks, the tech support scam remains the most prevalent and effective attack that they encounter.

These scams typically begin with a phone call or computer alert with a bogus claim about a virus or a major technical issue. The scammer, posing as a representative from reputable IT companies, uses sophisticated fear-mongering tactics to manipulate victims to take immediate action.

To “fix” the problem, the scammer frequently asks for remote access to the victim’s computer. Once connected, they can install malware, steal personal data or alter system settings to create real problems. Alternatively, they might instruct the victim to install expensive and useless software.

The financial and emotional toll on victims is substantial. Older adults are particularly vulnerable because they are often less familiar with technology and more likely to trust who they believe are authoritative figures. Furthermore, the isolation some might experience can make them more receptive to conversation, even from a stranger claiming to provide assistance. This makes social engineering easier.

The strategies employed by threat actors and others seeking to exploit technology are always changing. The dark side of this scam threatens to erode the confidence and security of our older populations.

Protecting older adults from these scams is crucial. The best lines of defense against it are education and awareness.

They need to be cautioned about accepting unsolicited tech support from unknown contacts and educated about how legitimate technical support organizations operate. It is up to families and caregivers to discuss the tactics used by scammers with them to ensure that they do not fall prey to these scams.

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.*

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

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

Upcoming Training & Events

- **Jun 3:** SANS Webinar: Exploring the Link Between Corruption and Cybercrime
- **Jun 6:** SANS Webinar: Evolution of SIEM in the Cloud
- **Jun 13:** SANS Webinar: Wings of Innovation: Transitioning to Containerization – Aviata Cloud Solo Flight Challenge Chapter 3
- **Jun 14:** SANS Webinar: AI and DFIR: A Match Made in Cyber Heaven or a Recipe for Digital Disaster
- **Jun 26:** SANS Webinar: Secure your multi-cloud environment from code to cloud with Microsoft Defender CSPM
- **Jun 27:** SANS Webinar: Is Access to Corporate Resources from any Device, Anywhere Truly Possible

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.

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.