Monthly Cybersecurity Newsletter

December 2023 Issue

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

It's Official: Scams Via Email and Text are Inescapable as Nearly Every American Receives Fake Messages Daily

New findings show that the overwhelming majority of people have to sort through scam messages and texts.

According to McAfee's Global Scam Message Study, more than 80% of Americans say it's more difficult than ever to spot a text, email, or social media message that's a scam. The proliferation of such messages sent via email and SMS is giving the average person a real sense that even they could become a victim if they're not careful.

According to the survey, the problem of email and text-based scams is rampant.

- 95% of Americans receive fake messages or scams via email daily.
- 40% of them receive five or more fake email messages each day.
- 87% of people receive fake messages or scams via text each day.
- 30% of them receive five or more fake text messages each day.
- 75% of the people surveyed have received fake messages or scams via social media every day as well.

Now add back in that 80% of Americans can't tell the difference between a legitimate and a scam email. This has a lot to do with the massive uptick in the use of AI tools to generate content. With tools like FraudGPT making every aspect of a scam nearly completely automated, it's incredibly easy for the newbie scammer to jump into the game and have a very real-looking arsenal of websites, emails, etc. to launch their very first scam.

In the corporate environment, organizations need to consider elevating their employees' sense of cyber vigilance to help them err on the side of caution. Even when they can't tell if a message is a scam or not, this helps reduce the risk of a successful scam or possible cyber-attack.

This article is redistributed with permission from KnowBe4.

How Thinking Like a Hacker Can Better Your Defense

There's no doubt that cyber threats are advancing and becoming more persistent. Traditional defense strategies alone are no longer sufficient to protect our digital environments. To stay one step ahead of cybercriminals, defenders must adopt the mindset of a hacker. Embracing a hacker's mindset is one of the most viable ways to catch a cybercriminal in action while revolutionizing the way we approach cyber defense.

The first line of defense is understanding your adversary to effectively anticipate their tactics, techniques, and procedures used to infiltrate systems. By adopting this perspective, defenders gain valuable insights into the motivations and goals of an attacker, enabling them to develop proactive defense strategies.

Thinking like a hacker can also help you pinpoint system vulnerabilities. Cyber defenders use penetration tests to identify weaknesses in the system's security controls. These tests give the defender an inside look into what tools a hacker would use to exploit systems, further giving them ways to counter the technique. It also tests the effectiveness of security protocols that are already in place. Once these items are identified, it will be easier for defenders to develop a more efficient incident response plan.

Keeping abreast of the latest security breaches and hacking techniques will help you better understand how systems are compromised. Exploring new techniques and methodologies will guide you to take appropriate preventative measures.

Adopting a hacker's perspective and thinking creatively when assessing your system's security can definitely give you an advantage over your adversary. Always consider unconventional attack vectors or potential weaknesses that others might overlook. Regularly test the effectiveness of the systems you have in place and always think of ways to improve them through counterattack mechanisms.

Digital Skimming Increases by 50%, Just in Time for the Holiday Season

Security researchers identify growth in the use of an ongoing cyberskimming campaign that involves compromising legitimate website checkout codes.

We've all seen a video that shows someone fidgeting with a credit card terminal only to pull off a very realistic molded cover that looks identical to the actual device beneath it, complete with its own circuitry to read and store credit card swipes. Now take that very same idea and put it into the digital world.

What would a digital skimmer look like? According to security researchers at Malwarebytes earlier this year, it appears as benign code within a legitimate webstore checkout code. A recent news release from Malwarebytes states they're now seeing 50% higher instances of this mode of attack in just a single

month, “demonstrating a huge uptick in both compromised sites and the opportunity for innocent shoppers to fall victim.”

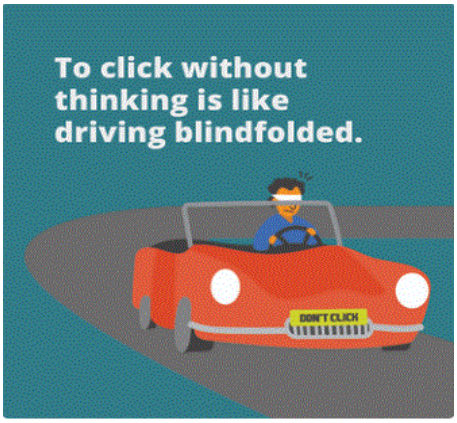
The problem here is that online shoppers, like their gas station skimmer counterparts in the real world, won’t know or suspect anything until that unauthorized charge comes through some time later. Plus, you won’t know where the breach of your credit card data occurred.

But this attack speaks to a much larger issue: that cybercriminals are getting really good at injecting code into a legitimate checkout process and can do whatever they want. That means it’s possible to see this kind of attack expand to include launching infostealers, leveraging social engineering through ads on the checkout pages, and more, all to obtain more from the potential victim buyer than just their credit card.

So, while you can’t do much to stop yourself from becoming a victim of digital skimming, you can still remain vigilant when online to reduce the likelihood of becoming a victim this holiday season.

This article is redistributed with permission from KnowBe4.

How to Help "Frequent Clickers" Become More Mindful



Within our organizations, there are those employees who consistently exhibit mindfulness, avoiding every phishing attempt. Yet, there are also those users who, despite repeated education efforts, habitually fall prey to phishing emails and simulations, neglecting the tell-tale signs of social engineering.

These individuals are known as "frequent clickers."

A question we often encounter is how to increase the mindfulness of these frequent clickers so they become less susceptible to phishing tactics. Transforming them into the always mindful "never clickers" is a challenge, but we do have some insights and approaches to offer.

In the context of cybersecurity and preventing risky behaviors such as clicking on phishing emails, "mindfulness" refers to a state of active, open attention to the present. More specifically, in this scenario, mindfulness can be broken down into:

1. **Awareness**: The individual is fully aware of their actions and the potential dangers that come with every email they encounter, demonstrating attentiveness to the unique elements of each communication.
2. **Recognition**: The ability to recognize tell-tale signs of phishing, such as suspicious links, unfamiliar sender addresses, and urgent or threatening language that requests personal information.
3. **Focus**: A mindful individual maintains focus and doesn't act on auto-pilot when navigating emails. They take the time to scrutinize each message rather than quickly clicking through without considering the consequences.

4. **Intentionality**: Actions are taken with purpose and intention. The individual deliberately chooses whether or not to engage with an email based on their assessment, rather than reacting impulsively.
5. **Responsiveness**: Instead of reactively clicking on links or attachments, a mindful person is responsive to training and best practices, using these tools as a guide for secure online behavior.

In essence, in the context of cybersecurity, mindfulness is the deliberate and attentive management of one's interactions with digital communications, with the intention of preventing security breaches and maintaining informational integrity.

Our understanding begins with an interesting observation from Dr. Matthew Canham's anti-phishing research. A renowned researcher and ally of KnowBe4, he has delved deeply into what influences people's likelihood of clicking on phishing emails. During one particular study, a significant incidental discovery was made.

Dr. Canham differentiated between those who had never responded to a phishing attempt ("never clickers") and those who frequently did ("frequent clickers"). Each participant was asked to choose a "code word" for use in later anonymous interviews, allowing survey answers to be linked without compromising anonymity.

Surprisingly, all "never clickers" showed impeccable mindfulness in remembering their code word. In stark contrast, the "frequent clickers" consistently forgot theirs. This suggests that mindfulness, or the lack thereof, may contribute to the vulnerability seen in frequent clickers. Although this is an initial finding, its implications are profound enough to warrant further exploration.

Recognizing that mindfulness may be a factor allows us to develop targeted strategies. An initial step might be to amplify the regularity of security-awareness training and simulations—monthly training is advisable, but for those less mindful, a weekly reminder may reinforce their awareness and recognition.

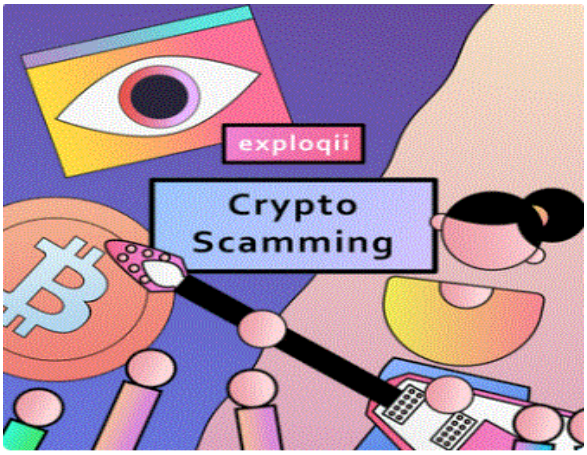
For social engineering exercises, while diversity in themes usually benefits the workforce at large, for less mindful frequent clickers, it might be beneficial to maintain a consistent theme until they demonstrate consistent recognition and reporting of phishing simulations. This focused approach can nurture their alertness and recognition and build their confidence. Once successful with one theme, they can be gradually introduced to new ones, reinforce their focus and responsiveness.

It's also useful to directly engage frequent clickers about how they can become more mindful. Many are aware of their challenges and know what learning strategies are effective for them. Insight from their own experiences may illuminate how to tailor their training for better outcomes.

Furthermore, as frequent clickers begin to show progress, encouraging them to participate in the gamification functions (reporting suspicious emails) which reinforces their learning. Being acknowledged by peers is a powerful reinforcement tactic. When they are on par or better than average, ask them to participate and become a security champion. Teaching is a powerful way to internalize knowledge, and it could inspire and foster improvement amongst the broader group of frequent clickers.

Transitioning frequent clickers into never clickers is definitely a challenge. However, by increasing training frequency, limiting subject variability, customizing education to individual needs, and reinforcing behavior with gamification, we stand a better chance of success. These measures benefit not just the individuals, but also strengthen the organization's overall security culture.

Online Scammer Poses as Skype, Swindles Victims Through Cryptocurrency Scam



Researchers at SlowMist describe a phishing campaign that's distributing a phony version of Skype in order to steal cryptocurrency, Cointelegraph reports. The malicious app was likely developed by Chinese cybercriminals.

"We noticed that the signature information of this fake app is quite simple, almost empty, and both the owner and publisher are labeled as 'CN,'" SlowMist's researchers explain.

"Based on this information, we preliminarily deduced that the phishing production gang is likely Chinese. Also, from the certificate's effective date of September 11, 2023, we inferred that this app was not created long ago. Further analysis revealed that the fake app uses version 8.87.0.403, while the latest version of Skype is 8.107.0.215. Using Baidu search, we found multiple sources of the same fake Skype version, with signature information consistent with that provided by the victim."

Cointelegraph notes that the phishing campaign is probably targeting users in China who are searching for third-party versions of apps like Skype that are banned in the country.

"Common behaviors of fake apps include uploading files and images from the phone, uploading data that may contain sensitive user information, and maliciously replacing network transmission content, like altering the destination address of wallet transfers, as seen in this case," SlowMist says. "Such tactics are not uncommon in fake Telegram and fake exchange apps."

SlowMist warns users to be wary of apps downloaded from third-party websites.

"Users need to be more cautious when downloading and using apps, sticking to official download channels to avoid downloading malicious apps and suffering financial losses," the researchers conclude. "In the blockchain's 'dark forest' world, users must continuously enhance their security awareness to avoid being deceived."

This article is redistributed with permission from KnowBe4.

Holiday Security Tips

As the holiday season approaches, many of us are excitedly making plans, shopping for gifts and booking vacations. Unfortunately, cybercriminals also see this time as an opportune moment to exploit unsuspecting individuals. It is crucial to remain vigilant and take extra precautions to protect your digital life and stay safe online during this festive period.

Check out some a few holiday tips to help keep you safe.

Training and 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/

- **Dec. 5:** SANS Webinar: **Take Sensitive Data Protection to the Next Level in 2024**
- **Dec. 7**: SANS Webinar: **Cloud Infrastructure Security for AWS**
- **Dec. 12:** SANS Webinar: **SANS First Look: Backups and Data Resiliency Made Easy**
- **Dec. 13**: SANS Webinar: **Is Your SIEM Really Doing Its Job? How to Take Cybersecurity to the Next Level**
- **Dec. 14**: SANS Webinar: **SANS Cyber Defense Initiative 2023: SANS@Night- The Industrial (ICS/OT) Cyber Threat Landscape**
- **Dec. 20**: SANS Webinar: **The Journey to Operational Security Effectiveness and Maturity: Frameworks, Tools and Techniques**
- **Jan. 10**: SANS Webinar: **Identify, Evaluate & Prioritize Industrial Cyber Risk**

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.*