Monthly Cybersecurity Newsletter

May 2023

**Enterprise Security and
Risk Management Office (ESRMO)**

From the Desk of Interim State Chief Risk Officer Keith Briggs

Large Language Models Will Change How ChatGPT and Other AI Tools Revolutionize Email Scams

The use of large language models (LLMs) is the fine-tuning that AI engines, like ChatGPT, need to focus the scam email output to only effective content that results in a wave of new email scams.

These tools are revolutionizing the content used in phishing emails. In short, gone are the days of poorly written scam emails, because ChatGPT wrote them.

This single effort addressed the bottleneck in any threat group's phishing activities – the writing of the persuasive email designed to elicit a response from the potential victim. With well-written influential emails comes larger percentages of tricked victims. But the challenge with ChatGPT is that it is not perfect. Even an AI engine can spout out nonsense, and with scammers often being non-native speakers to those they are attacking, the possibility exists that even a ChatGPT-created emails can fail.

Enter LLM.

TechTarget defines large language models as "a type of artificial intelligence (AI) algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate and predict new content." Facebook recently had its LLM leaked online. These LLMs are compact enough, the entire AI can run on a single laptop. And when focus is placed on writing compelling phishing emails, the likelihood that users will fall prey to the phishing content increases, leaving the attackers asking *"ChatGPT who?"*

These kinds of advancements will quickly become commonplace for phishing scammers, making it absolutely necessary to elevate the state of users' vigilance when they interact with email and the web. Literally, any content that seems even the slightest bit suspect or out of the norm will need to be treated as hostile until proven otherwise.

This article is redistributed with permission from KnowBe4.

One in 8 Email Threats Now Make It Past Security Solutions

Phishing attacks that can evade detection by email scanners are improving their chances of reaching the inbox, thanks to an increase in the use of one specific attachment type.

According to new data found in HP Wolf Security's latest Security Threat Insights Report for Q4 of 2022, 13% of all email threats being sent make their way past layered email security defenses to reach the user's inbox. This number is up from the previously published finding by Acronis of 11.7%. While a little more than 1% may not seem like much, with approximately 3.4 billion malicious emails sent daily, that accounts for an additional 44 million messages.

So, why the increase? According to HP Wolf, one of the reasons is the continued use of PDF files containing malicious links. It also mentions the use of archive files (e.g., ZIP files) as the most popular malicious file type used (in 42% of the cases) for its inability to be scanned easily – something HP Wolf first covered late last year.

This rise in malicious emails getting to the inbox means you have one of two paths to take. The first is that you assume the user is going to unwittingly fall for the likely social engineering tactics used in the malicious email and your endpoint protection is going to need to do the work of hopefully stopping the attack. Or you educate users through security awareness training so they can easily spot an attack and, by failing to interact with the malicious links or attachments, stop the attack before it has an ability to arm itself in the first place.

This article is redistributed with permission from KnowBe4.

Cyberattacks Increase as a Result of the Russia-Ukraine War

The ongoing Russia-Ukraine conflict has seen a rise in cyberattacks aimed at disrupting critical infrastructure in both Ukraine and Russia. Cyberattacks have been used as a weapon of war to gain a foothold in enemy territory and to compromise their communication systems. These systems and assets are essential for the country's society and economy to function properly. The attack surfaces include power grid networks, water supply systems, transportation systems, email and phone systems, as well as attacks on medical facilities, causing significant damage.

The use of cyberattacks as a weapon of war is not a new concept. In December 2015, the first major attack on Ukraine's power grid took place in the city of Ivano-Frankivsk. The attack was conducted using BlackEnergy malware, which was used to infiltrate the network and gain control of the systems. The attackers were able to cause a power outage that lasted for several hours, affecting more than 200,000 people. After this attack, a series of similar attacks followed, affecting several regions of Ukraine.

The Federal Security Service of the Russian Federation recently announced that it has recorded more than 5,000 hacker attacks on Russia's critical infrastructure. This announcement has raised concerns about the security of Russia's critical infrastructure and the potential consequences of these attacks.

Cyber warfare has become one of the most pressing security concerns of the 21st century. With the increasing reliance on technology and the internet, cyberattacks have become more sophisticated and more frequent. These attacks can cause significant damage to critical infrastructure, government agencies and private companies.

Cyberattacks can come in many forms, including viruses, malware, phishing attacks, denial of service attacks and ransomware. These attacks can be launched by state-sponsored hackers, criminal groups or even individuals looking for financial or political gain. But in this case, it is the result of cyber warfare.

The Russia-Ukraine war highlights the growing threat of hacker attacks. It is important for all countries to take steps to enhance their cybersecurity measures to protect against these economically crippling attacks. It is also essential for global cooperation in addressing these threats to ensure the safety and security of all countries and their citizens.

We all must take extra measures to protect our personal data from these threats by using strong passwords, updating and patching security software and being vigilant of suspicious online activities.

Should We Opt out of Sharing Data with Mobile Providers?

So many times, we willingly share our personal information with our mobile provider not knowing they are collecting or using it. Most of us feel like this information is a requirement to continue using the service. The question is, should we opt out of sharing this information to protect our personal privacy?

Recently, news of an AT&T customer data breach has sent shockwaves across the industry. According to reports, the breach potentially affected the personal information of millions of AT&T customers, including Social Security numbers, names and dates of birth.

AT&T has assured customers that it has taken immediate steps to rectify the situation and is investigating the matter. The company has also offered credit monitoring services to affected customers.

The issue of data breaches is not new, and companies must learn from such incidents and take concrete efforts to bolster their cybersecurity measures. This includes implementing strict access controls, conducting regular risk assessments and educating employees about the importance of maintaining security at all levels.

There are a few reasons why you might opt out of data sharing with their mobile provider:

- **Privacy concerns.** Opting out of data sharing means that the mobile provider will not have access to your personal data and usage information, which can help protect your privacy.

- **Avoiding targeted advertisements.** Mobile providers might use your data to show you targeted advertisements. By opting out, you can avoid being targeted with ads based on your usage habits.

- **Control over your data.** Opting out of data sharing can give you more control over your data and how it is being used by third-party apps or services.

Ultimately, the decision to opt out of data sharing with your mobile provider will depend on your individual needs and preferences. It is important to carefully read and understand the terms of service before deciding.

Utilizing Mobile Threat Defense

Mobile devices, especially smartphones, have become an integral part of our daily lives. We use them for communication, entertainment and work.

The rise of mobile threats, such as malware, phishing attacks and ransomware, highlights the need for mobile threat defense solutions, which are becoming more and more commonplace as the need to protect and secure mobile devices becomes more dynamic.

Mobile threat defense (MTD) is a security technology designed to protect mobile devices from a variety of threats. MTD applications detect and prevent attacks and provide early warning to users if their device is compromised. These applications use a combination of signature-based detection, behavioral analysis and machine learning to identify malicious activity on a mobile device.

MTD applications offer a wide range of features and capabilities to protect mobile devices. These include anti-virus and anti-malware protection, web protection, network security, app scanning and device management. MTD applications can also help identify vulnerabilities in the device's operating system and installed applications before they become an issue.

MTD applications come with advanced monitoring capabilities that help in detecting any suspicious activity on the device. This includes monitoring network traffic, file activity, system logs and other critical parameters. By analyzing this data, MTD applications can identify any anomalies and flag them as potential threats.

Another crucial feature of MTD applications is their ability to perform vulnerability scans on the device's operating system. These scans help in identifying any weaknesses or loopholes that could be exploited by attackers to gain unauthorized access to the device or steal sensitive data.

Once the vulnerabilities are identified, the MTD application provides remediation suggestions to the user to patch or fix the security loopholes.

To maximize mobile threat detection, here are some steps that you can take:

- Ensure that your application is up to date with the latest patches and security updates.
- Use the most advanced threat detection techniques, such as artificial intelligence and machine learning, to detect anomalies and threats that traditional security measures might not identify.
- Regularly test and assess the application's performance to ensure that it is accurately detecting threats and minimizing false positives.
- Provide adequate training and resources to your security team to effectively manage the application, investigate and respond to threats, and continuously improve the application's performance.
- Consolidate your security tools to ensure that your threat detection application is integrated with your other security tools, such as firewalls and intrusion detection systems, to provide comprehensive security and threat remediation.

Business Continuity Awareness Week Is May 15-19

Business Continuity Awareness Week is the Business Continuity Institute’s most popular campaign that raises awareness of business continuity and resilience. The campaign offers free access to professionals and organizations across all industry sectors to a wide range of resources covering business continuity and resilience, as well as related disciplines.

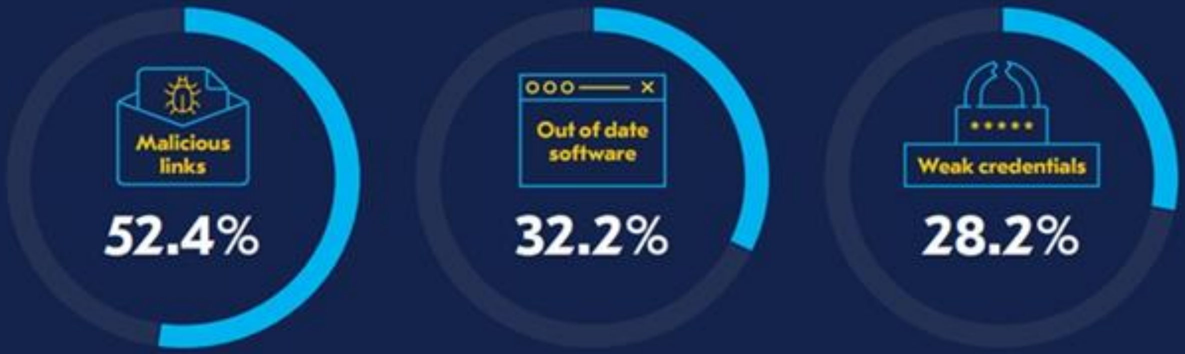
BCAW 2023 will feature the theme *“Embracing the Challenge of Resilience”* and it will cover different areas of the resilience discipline, which are also key focuses on many of the disruptive events currently happening. Each day of the campaign will be dedicated to a specific topic.

- May 15: Cyber Resilience
- May 16: Supply Chain Resilience
- May 17: Operational Resilience
- May 18: Personal Resilience
- May 19: Organizational Resilience

The Enterprise Security and Risk Management Office and our North Carolina Business Continuity Team partners will be presenting a 30-minute “Business Continuity Talks” each day at 1 p.m. using Microsoft Teams.

The discussion will revolve around the resilience discipline being highlighted that day in relation to business continuity from a state government perspective. We will also be highlighting content presented each day by thebci.org and their partners.

In the past year, the main causes of cyber incidents were:



Embracing the Challenge of Resilience.

bci BCAW

Business Continuity
Awareness Week
15th - 19th May 2023

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/

May 3: SANS Webinar: Implementing Attack Surface Management

May 4: SANS Webinar: 5 Automation Trends to Scale and Modernize Your InfoSec Compliance Program

May 9: SANS Webinar: How to build a Security Awareness Program and Manage Human Risk

May 11: SANS Webinar: Building Better Cloud Detections…By Hacking? Azure Edition

May 16: SANS Webinar: Red and Purple Team: Improve the defenders' ability to stop the attackers

May 30: SANS Webinar: Using Intelligent Data as a Force Multiplier for Security and IT Ops

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.*