Monthly Cybersecurity Newsletter

November 2020
Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and
Risk Management Office
(ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Ransomware is Still Making Demands

Ransomware is a type of malicious software (malware) that blocks access to a system, device, or file until a ransom is paid. It is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message, or website. Ransomware works by encrypting files on the infected system (crypto ransomware), threatening to erase files (wiper ransomware), or blocking system access (locker ransomware) for the victim. The ransom demand can range from as little as several hundred dollars up to and exceeding one million dollars. It is not unusual to see multi-million-dollar ransom demands in the current threat landscape.

Ransomware is a growing and expensive problem! In 2019, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed a ***153% increase*** in the number of reported State, Local, Tribal and Territorial (SLTT) government ransomware attacks from the previous year. Many of these incidents resulted in significant network downtime, delayed services to constituents, and costly remediation efforts. Ransomware has even affected the 2020 election. A Georgia county database of voter signatures was recently impacted by ransomware along with other government systems. The county announced, however, the voting process for citizens was not impacted. The effects of ransomware can be particularly harmful when it impacts emergency services and critical infrastructure, such as 911 call centers and hospitals.

What can you do to prevent a ransomware attack?

While ransomware infections are not entirely preventable, organizations can significantly reduce the risk of ransomware infections by implementing cybersecurity policies and procedures (e.g. patching software and systems, keeping up-to-date malware protection, and appropriate access control permissions), and improving ***cybersecurity awareness and practices*** of all employees. The vast majority of infections are a result of someone clicking a link from a malicious email message. Therefore, becoming more cyber aware can dramatically reduce the risk of a ransomware infection. The following are several things you can look for that may be an indicator of an email scam:

- Look for mismatched URLs – hover your mouse over the URL and compare the address
- Poor grammar and spelling
- A request for personal information, such as SSN, user IDs, passwords, banking information, etc.

- Correspondence that comes with a sense of urgency, such as your account may be disabled, or you may lose some funds
- An offer that appears too good to be true
- Unrealistic or unlikely threats
- Open communication from a perceived authority, e.g. the IRS, or a financial institution

Email scams also take advantage of current events and specific times of the year:

- Natural disasters or significant weather issues
- Global health scares (e.g. COVID-19), or even the flu season
- Financial or monetary concerns, like IRS scams
- Major political elections!!!
- Holidays and celebrating events, such as international athletic events

For those with access to the State of NC's SharePoint resource, be sure to read November's Security Awareness News newsletter for more tips on email security. If you suspect you are a victim of a ransomware infection or an email scam, it is important to follow your organization's incident response procedures and notify the appropriate information security contact within your organization as quickly as possible.

KnowBe4, a training and awareness vendor, provides cybersecurity training and awareness to individuals through a diverse library of training content. In addition to their training modules, KnowBe4 also provides a phishing simulator that organizations can use to test their employee's ability to spot a suspicious email message. Phishing simulations help decrease an organization's risk to cyber attack by simulating content that is seen in the "wild" and giving people the opportunity to learn from the simulation before they encounter a real malicious message.

KnowBe4 has produced its latest quarterly report on top-clicked phishing email subjects. These are broken down into three different categories: social media related subjects, general subjects, and "in the wild" attacks. The most common 'In-The-Wild' Emails in Q3 2020 were as follows:

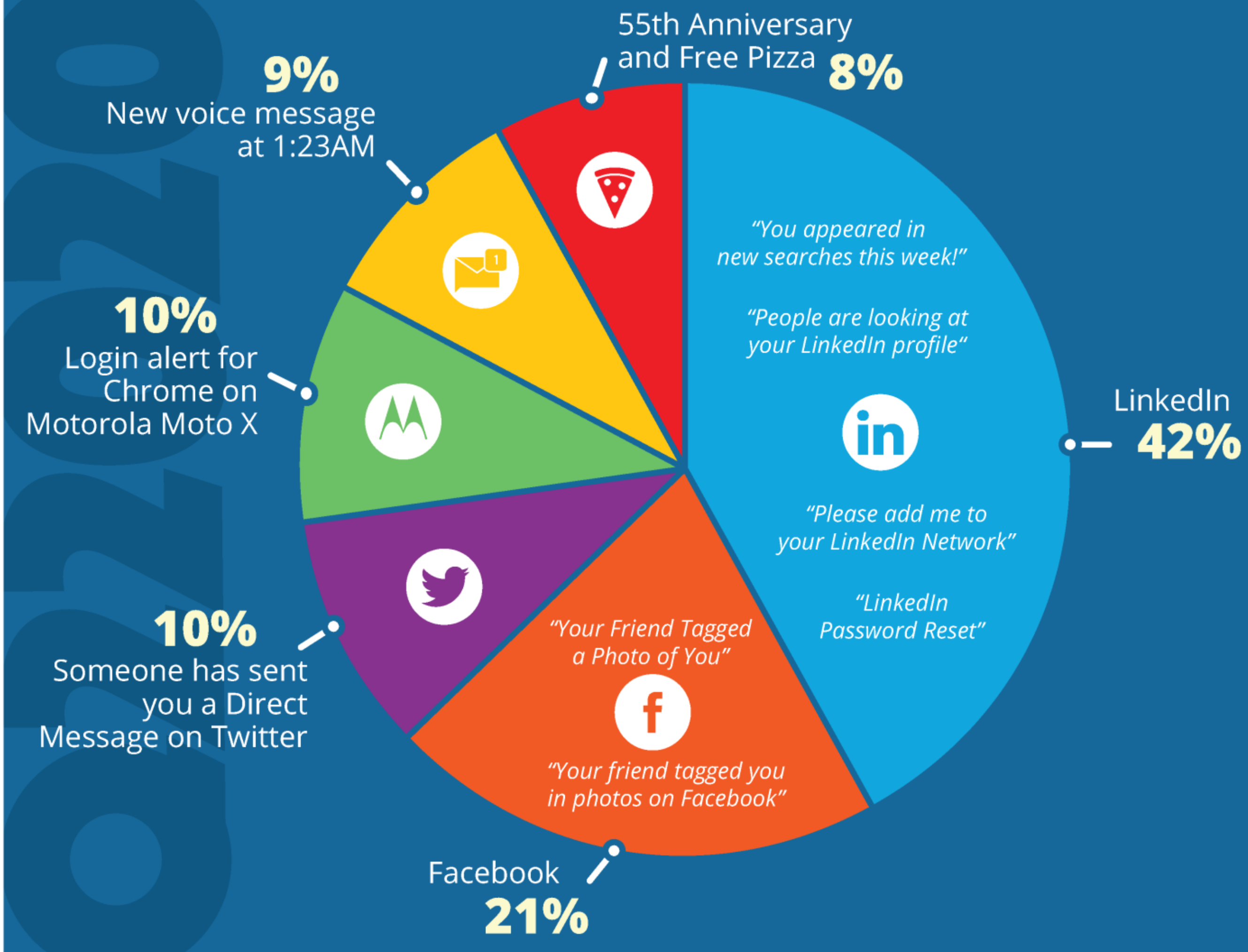
- Microsoft: View your Microsoft 365 Business Basic invoice
- HR: Pandemic Policy Update
- IT: Remote Access Infrastructure
- Facebook: Account Warning
- Check your passport expiration date
- TeleMed Appointment Reminder
- Twitter: Confirm your identity
- Apple: Take part in our iPhone 12 trial and enter for the chance to win a FREE iPhone12
- Exchange ActiveSync service disabled for [[email]]
- HR: Benefit Report

According to Stu Sjouwerman, CEO of KnowBe4, the "Q3 report confirms that coronavirus-related subject lines have remained their most promising attack type, as pandemic conditions weaken judgment, and lead to potentially detrimental clicks." The following two infographics highlight the report findings.

KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or mentioned you can make someone feel special and entice them to click. And everyone loves free pizza!

TOP 10 GENERAL EMAIL SUBJECTS

Password Check Required Immediately	20%
Vacation Policy Update	12%
Branch/Corporate Reopening Schedule	11%
COVID-19 Awareness	10%
Coronavirus Stimulus Checks	10%
List of Rescheduled Meetings Due to COVID-19	10%
Confidential Information on COVID-19	8%
COVID-19 - Now airborne, Increased community transmission	7%
Fedex Tracking	6%
Your meeting attendees are waiting!	6%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. Unsurprisingly, half of the top subjects for this quarter were around the Coronavirus pandemic. Curiosity is also piqued with security-related notifications and HR-related messages that could potentially affect their daily work.

COMMON *"IN THE WILD"* ATTACKS

- Microsoft: Abnormal log in activity on Microsoft account
- Chase: Stimulus Funds
- HR: Company Policy Notification: COVID-19 - Test & Trace Guidelines
- Zoom: Restriction Notice Alert
- Jira: [JIRA] A task was assigned to you
- HR: Vacation Policy Update
- Ring: Karen has shared a Ring Video with you
- Workplace: [[company_name]] invited you to use Workplace
- IT: ATTENTION: Security Violation
- Earn money working from home

KEY TAKEAWAY

Here again we see subjects related to the Coronavirus and working from home. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

2020 Annual Cybersecurity Awareness Symposium
Hosted by the N.C. Department of Information Technology Enterprise Security and Risk Management Office
#CyberSecureNC
NCDIT
NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY
OCT. 5 & 6

The N.C. Department of Information Technology's (DIT) Enterprise Security and Risk Management Office (ESRMO) hosted its first virtual **2020 Annual Cybersecurity Awareness Symposium** on October 5 -6. Content from the Symposium has been posted online.

The annual Symposium is an information sharing and awareness event that is hosted in support of National Cybersecurity Awareness Month (NCSAM). This year's symposium was well attended with over 500 individuals from State and local government, colleges, and K-12 school systems registered for the event. Attendees were able to learn from cyber leaders and subject matter experts in the private, public and academic sectors on various topics related to maximizing cyber spend while protecting data and systems from compromise. To view content from the 2020 Symposium, as well as from previous symposiums, please visit here.

Microsoft is Nudging People Away from Explorer to Edge

Microsoft's Internet Explorer (IE) browser has been around for 25 years, but it is nearing end of life. While IE has been a popular browser with nearly 95 percent of the market share at one time, it has also had many issues when it comes to security, privacy, and compatibility. Since 2000, there have been over 1,000 serious vulnerabilities tied to it. Today, an estimated five percent of users still rely on Internet Explorer for their web content needs.

Microsoft plans to disable support for IE in certain services starting in November. Microsoft will begin redirecting users of IE to Microsoft Edge when they browse to an incompatible web site. Whenever someone visits an incompatible web site now using IE, they get a message that tells them the site is incompatible with their browser, and they need to manually switch to a different browser. When the redirect is implemented and individuals go to a site that is incompatible with IE, they will be ***automatically*** redirected to Microsoft Edge.

Microsoft 365 apps and services will be focusing on using modern browser support over the coming year. One result of this is the Microsoft Teams web app will no longer support Internet Explorer 11 after **November 30, 2020**. Users will be unable to access the Teams web app from IE 11 and will be notified to use the desktop app or access the web app from Microsoft Edge.

If you have apps that require IE, or IE-specific plugins such as Silverlight, consider using an isolated version of Internet Explorer only for use with those applications, while moving your systems to newer browsers such as Chrome, Firefox or Edge. Internet Explorer 11 will continue to receive security updates and technical support for the lifecycle of the version of Windows on which it is installed. It is recommended to move to more current browsers as soon as possible.

State Employee Cybersecurity Town Hall

The Department of Information Technology's (DIT) held its first-ever **Cybersecurity Town Hall** for State employees on Wednesday October 28. Approximately 530 employees from 44 agencies registered for the event. Attendees learned some basics of cybersecurity, including how best to protect themselves while working from home. If you missed the Town Hall or would like to see it again, the event is available online at https://youtu.be/8v_2RvlNqCU.

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. ***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2020

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). 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

November 1-30: National Critical Infrastructure Security & Resilience Month

November 5, 10, 13, 16, 18, 20, 24, 30: FEMA's Integrated Preparedness Plan and Integrated Preparedness Planning Workshop webinars**.**

November 10: SANS 2020 Vulnerability Management Survey

November 18: Securing Your Digital Future: Merging Mobile and Security Strategies webinar by ISSA

November 19: Ransomware Prevention Special Report: How to Address a Pervasive and Unrelenting Threat webcast by SANS.

November 26 & 27: Thanksgiving Holiday!

November 30: 2020 Business Continuity and Disaster Recovery Plans due!

December 9: *How does PCI DSS 4.0 impact us? It Depends* webinar by Coalfire.

Also…for a list of upcoming SANS webcasts, visit here!

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.*