Monthly Cybersecurity Newsletter

November 2021
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

Phishing: Low, Middle and High Level

Phishing is a form of social engineering that uses authentic-looking – but false – messages to trick people into doing something they should not, such as going to a fake website, sharing sensitive information, or downloading malicious files. In an article published by ITProPortal, Mark Nicholls, from Redscan, explains that phishing attacks have varying levels of sophistication, with the lowest level being simple emails designed to lead a victim into a scam.

“The most basic phishing emails are designed to establish a relationship with the target,” Nicholls says. “There are no links or malicious attachments to open. The phish is simply a primer for future communications, such as requests for payment. Messages are typically plain text and sent via widely used email services such as Gmail, which means they are very likely to bypass mail filters rather than be marked as spam. The sender’s name used is often a senior person within an organization, such as the CEO.”

“To conduct mid-level phishing campaigns, attackers use basic hacking tactics, techniques and procedures,” Nicholls says. A very common technique among more sophisticated phishing attacks involves the purchase of a private website domain (e.g., mysite.com) to host a webpage that is cloned from a legitimate website. With a cloned website, an attacker can lure individuals to their fake page through a malicious email link and entice them to divulge sensitive information.

The most sophisticated and damaging attacks are highly targeted phishing acts that involve a great deal of preparation and intelligence gathering on specific organizations and employees. According to Nicholls: “The [professional criminals] that create and leverage advanced phishing campaigns such as business email compromise attacks conduct extensive open-source intelligence gathering on their targets. This involves profiling individuals but also the organizations they work for. Job advertisements are often a good source of information, disclosing details about the types of systems, applications and security tools organizations use.”

To help mitigate the risk of all levels of phishing, Nicholls suggests the following:

- Provide employee awareness training and ensure its content is regularly refreshed.
- Closely monitor networks and endpoints to detect threats that evade perimeter defenses.
- Conduct simulated assessments to assess the effectiveness of controls and processes.
- Leverage and act upon threat intelligence to help improve defenses.
- Enforce multi-factor authentication to protect user accounts in the event of passwords being compromised.

NORTH CAROLINA
CYBERSECURITY
AWARENESS SYMPOSIUM
#CyberSecureNC

2021 N.C. Cybersecurity Awareness Symposium Session Recordings Online

In support of National Cybersecurity Awareness Month, the N.C. Department of Information Technology hosted the 2021 N.C. Cybersecurity Awareness Symposium on Oct. 6-7. This was a virtual event that provided several learning opportunities for how to help secure an organization amid current trends. Nearly ***500 people attended*** from state and local government, boards and commissions, K-12 school systems and colleges and universities.

The symposium featured opening remarks from Gov. Roy Cooper and a keynote address from retired Gen. Keith Alexander (co-founder of IronNet Inc.). Session topics included threat intelligence, ransomware, continuity of government, cybersecurity awareness and training and managing third-party risk.

Participating presenters and vendors included the N.C. National Guard, the U.S. Cybersecurity & Infrastructure Agency, IronNet, BitSight, Crowdstrike, VMware, Amazon, Tanium, KnowBe4, Splunk, Info-Tech Research Group, Microsoft and Tenable.

The sessions are available online and may be viewed here.

Smishing Attacks and How To Avoid Them

Cybercriminals continue to launch new smishing attacks, a form of phishing that uses mobile phones as the attack platform, to steal credentials and distribute malware, according to Michael Marriott, senior strategy and research analyst at Digital Shadows. Marriott describes a new Android banking Trojan called "AbereBot" that is being sold on cybercrime forums. Since the Trojan targets mobile devices, it is distributed via text messages.

People are often prompted to download an application on their mobile device that enables an attacker to do something nefarious, such as capture banking credentials. Marriott cites advice from the UK's National Cyber Security Centre on how to avoid falling for these scams:

- Only download apps from app stores, such as the Android Play Store.
- If you suspect you have clicked on a malicious link, reset your device to factory settings and reset credentials of any accounts that you have entered since the infection.
- Even non-Android users should be cautious of clicking on links that might be attempting to capture credentials.
- Beware of unsolicited texts using high-pressure tactics that introduce urgency, such as closing accounts or transferring funds. When in doubt, go to the company's full website and check notifications for your accounts there.
- Beware of anything that forces you to log in to unrelated services, such as entering banking credentials to receive a package.
- Always treat a message offering "something for nothing," such as winning money or prizes, as suspect, especially when you need to provide financial or other sensitive information.

Two-Thirds of Organizations Have Been a Target of Ransomware

According to some recent data, ransomware is pervasive throughout every industry, size and type of organization and is the ***number one cyberthreat today***.

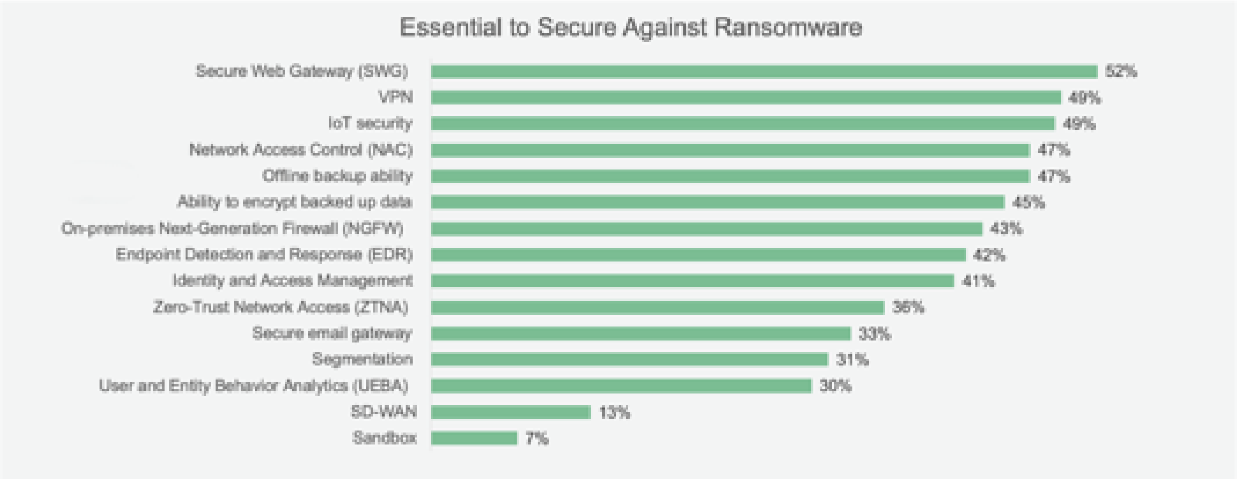
According to Fortinet, which develops and sells cybersecurity solutions such as firewalls, anti-virus protection and intrusion prevention systems, ransomware grew ***more than 1000%*** between July 2020 and June 2021. This new data from Fortinet's 2021 Ransomware Survey Report shows just how terrible ransomware attacks are today. The report found the following statistics:

- 67% of organizations have been a target of ransomware attacks
- 16% have been hit three or more times
- 96% feel at least moderately prepared (despite the percent of attacks indicating otherwise)

Organizations might not be making the connection between user awareness and cyberattacks. For instance, look at the following stats:

- Nearly a third (32%) say there is a ***lack*** of security awareness training.
- Sixty-one percent have user training – but as part of an incident response plan (***after*** an incident has occurred and not before).
- Fifty-eight% of ransomware attacks in North America ***start*** with phishing a user.

The statistics from the report support the need for increased cybersecurity awarness and securing the human firewall. However, in the list of measures essential to secure against ransomware, security awareness training is ***not*** mentioned. This begs the question, why?



Source: Fortinet

Individual end users play a crucial part in either helping or stopping ransomware attacks. Since phishing is still the number one vector of attack, it is incumbent upon everyone to be vigilent and aware of cyberattacks. Regular and relevant cybersecurity awareness training helps create a proactive security stance that is designed to reduce the risk of cyberattacks.

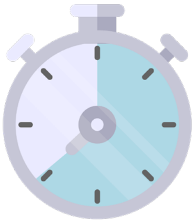
Be sure to check out NCDIT's webpage on Avoiding Phishing Attacks.

DANGER ZONE

It's a dangerous world out there, and cybercrime is happening way more than you think. Hackers want to gain access to your accounts and devices, as well as your organization's valuable resources and information.

Discover some surprising facts as well as actions you can take to lessen the threats you and your organization face.

CYBERCRIME STATISTICS & HOW TO PROTECT YOURSELF



36 seconds is the average amount of time between hacker attacks worldwide.

Follow your organization's security policies.

60% of data breaches involved vulnerabilities that had a patch, which wasn't applied.

Update your devices and applications with the latest security updates.

81% of data breaches are due to the reuse of a compromised password.

Never reuse passwords! Duplicating passwords makes you more easily hacked.

69% of IT experts are concerned about increased cybersecurity risks due to employees working from home.

Lock and **secure** your devices and documents when not in use.

94% of malicious software is delivered by email.

Don't click on links or open attachments, especially when they're unexpected.

STOP, LOOK, AND THINK
when something seems fishy.

KnowBe4

NIST Cybersecurity Framework: A Quick Start Guide

NIST
National Institute of
Standards and Technology

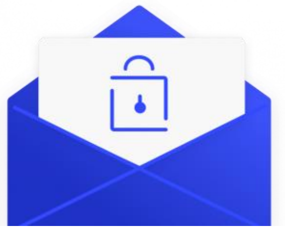
To continue providing guidance and assist in the facilitation of utilizing the NIST Cybersecurity Framework, the National Institute of Standards and Technology has finalized a new guide, NIST Special Publication (SP) 1271, *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*.

The NIST Cybersecurity Framework is organized by five key functions: identify, protect, detect, respond and recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time. This publication outlines key, high-level activities organized by Framework Function that might offer a good starting point for an organization when establishing a secure cybersecurity posture and is applicable for any sector or community seeking to improve cybersecurity risk management.

The NIST Cybersecurity Framework enables organizations – regardless of size, degree of cybersecurity risk or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. Through implementation of the NIST Cybersecurity Framework, organizations can better identify, assess and manage their cybersecurity risks in the context of their broader mission and business objectives.

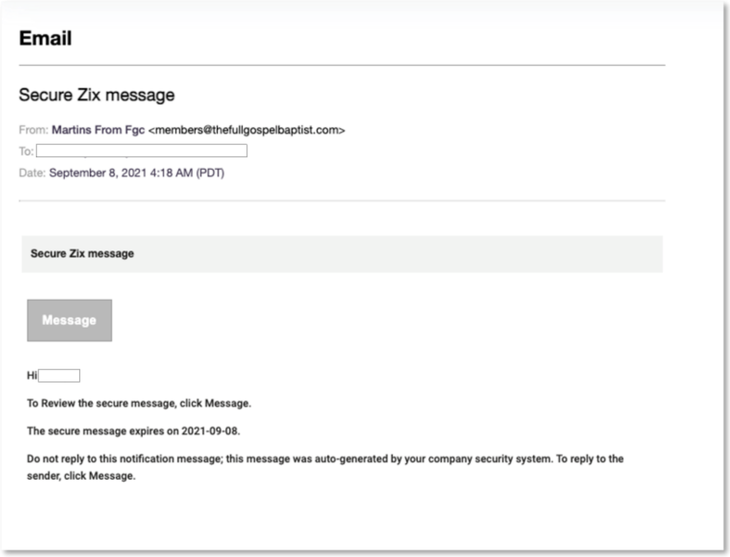
Questions and comments about this notice may be sent to cyberframework@nist.gov.

Phishing Campaign Spoofs Zix Messages



Researchers at Armorblox have discovered a phishing campaign that is impersonating encrypted messages from Zixmail, an email encryption solution that many organizations use to send email messages securely. The phishing messages contain a link to download an HTML attachment.

“This email is titled ‘Secure Zix message,’ includes a header in the email body reiterating the email title and claims that the victim has received a secure message from Zix,” the researchers write. “The email invites the victim to click on the ‘Message’ button to view the secure message.” (See image below.)



Secure Zix message

From: Martins From Fgc <members@thefullgospelbaptist.com>
To: [redacted]
Date: September 8, 2021 4:18 AM (PDT)

Secure Zix message

Hi [redacted]

To Review the secure message, click Message.

The secure message expires on 2021-09-08.

Do not reply to this notification message; this message was auto-generated by your company security system. To reply to the sender, click Message.

Although the phishing campaign was widespread, researchers observed some attacks were targeted at specific employees.

Armorblox recommends people slow down and ***think before clicking*** on unsolicited links. Always inspect the sender name, sender email address, language within the email and any logical inconsistencies within the email *(e.g. Why is a Zix link leading to an HTML download? Why is the sender email domain from a third-party organization?)*.

PCI Webinar by Coalfire

The N.C. Office of the State Controller is pleased to announce the next PCI webinar that will hosted by Coalfire, a PCI compliance validation services vendor for the state of North Carolina. The next webinar will be on **Dec. 8 from 10-11 a.m. EST**. The topic of the webinar will be "Risk Assessments – Do You Feel Lucky?"

To be notified, [sign up for PCI webinar announcements via the eCommerce listserv](), which also provides updates about products and services on the merchant card and enhanced file transfer (EFT) master service agreements, annual PCI compliance, self-assessment questionnaires and quarterly scans.

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/2021

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 9: SANS Webinar: Cybersecurity Standards Scorecard

November 11: Veteran's Day

November 18: SANS Webinar: The Truth about Ransomware: It's not Complicated!

November 25-26: Thanksgiving

December 8: Coalfire Webinar: Risk Assessments – Do You Feel Lucky?

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.*