Monthly Cybersecurity Newsletter

August 2022 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 *Still* Tops the List as Initial Attack Vector for Ransomware

Ransomware is a large threat. A report published by the Institute for Security and Technology's Ransomware Task Force states that last year there were more than 4,000 documented ransomware attacks involving varieties of extortion malware that targeted organizations across every sector in 109 countries. More concerning, the latest data on ransomware trends from backup vendor Veeam shows the impact these attacks have on backups and an organization's ability to recover.

Current and reliable backups are a crucial step for an organization to be be operationally resilient to ransomware attacks. But, according to Veeam's 2022 Ransomware Trends Report, organizations are not prepared for the sophisticated attacks they are facing. These attacks target backups, seeking to remove an organization's ability to recover without first paying the ransom. According to the report:

- Backup repositories are targeted in 94% of attacks.
- These same repositories were impacted in some way in 68% of attacks.
- Attackers targeted specific systems and platforms (i.e., Windows, VMware, NAS, etc.) in 80% of attacks.
- On average, 47% of all data was encrypted.
- Of those organizations that paid the ransom, 31% still could not recover their data.

Although most organizations are able to begin recovery efforts within minutes to hours, 93% of organizations report that it took between ***a week to four months*** to be completely operational again.

How do these very impactful attacks gain entrance into an organization's network? According to the report, initial attack vectors in ***44% of ransomware attacks*** were phishing emails, malicious links, etc.

To combat threats such as ransomware, an organization's cybersecurity strategy needs to include both technical controls as well as raising awareness among its users. Network security solutions do little to address the threat that ends up in an individual's inbox or the webpage that contains a malicious link. Individuals who receive regular and relevant security awareness training will be far more likely to spot a phishing attack and stop it before it gains traction.

Be sure to view Janus Associates post on How to Minimize the Risk of a Ransomware Attack. For more information and tips on avoid phishing, visit NCDIT's Avoid Phishing Attacks webpage.

LinkedIn Remains a Leading Platform for Social Engineering

LinkedIn is a widely used professional networking platform. With more than 810 million members, it offers a large pool of potential victims – working, connected and, in some cases, wealthy. LinkedIn member profiles usually have a lot of personal information, and their connections offer opportunities for scammers to pivot to other potential victims.

A study by researchers at Check Point found that 45% of all the email phishing attempts observed during the second quarter of 2022 mimicked LinkedIn's "style of communication," as scammers sought to direct their victims to a spoofed LinkedIn login page to harvest account credentials.

That is a big jump from the fourth quarter of 2021, when Check Point found that only 8% of the brand phishing attacks sought to take advantage of LinkedIn's reach and reputation. Researchers at Vade Secure reached a similar conclusion: In 2021, LinkedIn trailed both Facebook and WhatsApp in the rate of attempted impersonation. Other brands that phishers loved to impersonate during Q2 2022 are Microsoft (13%), DHL (12%) and Amazon (9%).

Things appear to have changed. Social engineers impersonating communications from LinkedIn dangle phish bait that is likely to attract the attention of the platform's professionally minded clientele. The scam message might indicate that another LinkedIn user is interested in doing business with the victim, that their profile has "appeared in X searches this week," or even something as simple as a note that a message is waiting for them.

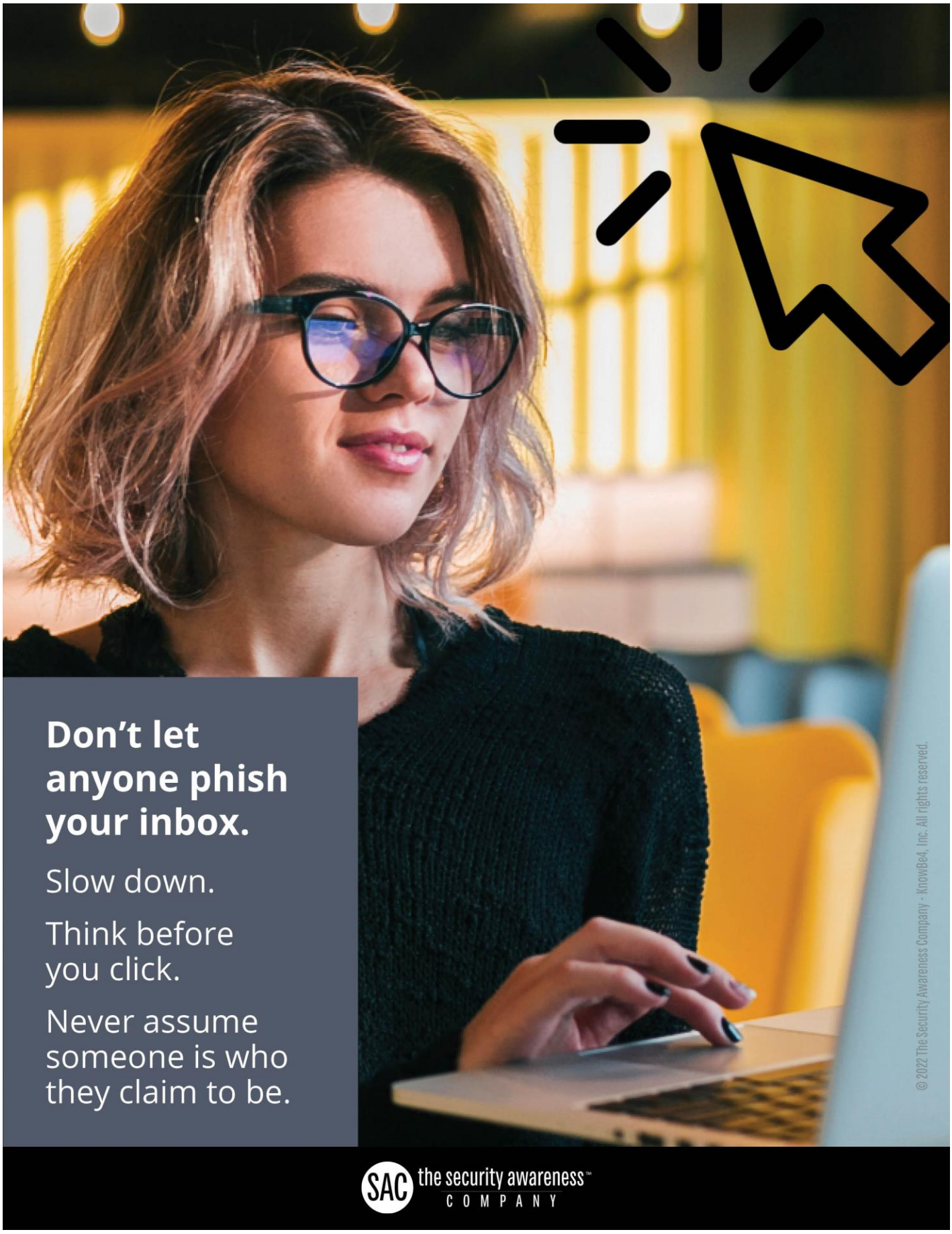
These approaches are particularly effective when the labor market is fluid and people are moving between jobs and looking for better opportunities. But scammers do not stop there. One of their common goals, the FBI warns, is to lure people into speculative (and bogus) investments in cryptocurrencies. One Florida benefits manager says she lost $288,000 – her entire life savings – to a scammer on LinkedIn. The FBI reports that they have seen an increase in this particular investment fraud, which is different from a long-running scam in which the criminal pretends to show a romantic interest in the subject to persuade them to part with their money.

LinkedIn says it removed more than 32 million fake accounts from its platform in 2021, according to its semiannual report on fraud. LinkedIn members reported 127,000 fake profiles that were also removed.

The company offers some sound advice for its users: "Be wary of and consider reporting" the following three common problems:

- People you do not know in real life who ask you for money. This can include people asking you to send them money, cryptocurrency, or gift cards to receive a loan, prize, or other winnings.
- Job postings that sound too good to be true or that ask you to pay anything upfront. These opportunities can include mystery shopper, company impersonator or personal assistant posts.
- Romantic messages or gestures, which are out of place on LinkedIn – can be indicators of a potential fraud attempt. This can include people using fake accounts to develop a personal relationship with the intent of encouraging financial requests.

If you have been the victim of a scam, report it to your local law enforcement. If you have received a scam message on LinkedIn, contact LinkedIn Support.


Don’t let anyone phish your inbox.
Slow down.
Think before you click.
Never assume someone is who they claim to be.
© 2022 The Security Awareness Company - KnowBe4, Inc. All rights reserved.
SAC
the security awareness™ COMPANY

Monthly Privacy Meeting – Aug. 30, 10–11 a.m.

NCDIT Chief Privacy Officer Cherie Givens will hold the department's monthly privacy meeting from 10-11 a.m. on **August 30**. All privacy points of contact and other state employees working on privacy matters or interested in privacy are invited.

If you have been identified by your agency as the privacy point of contact, you should be receiving an invitation. If you are a state employee with an interest in privacy, please send your name and contact information to ditprivacy@nc.gov to be added to the meeting invitation list

Look Out for HR Phishing!

HR-targeted attacks are a trending global threat, experts said at a recent keynote at the 2022 RSA Conference. Threat actors are targeting HR employees who are looking to hire new people, according to Lisa Vaas at Contrast Security. As part of their job, HR employees frequently interact with people outside of the organization and are *more likely to open external files*. Attackers frequently take advantage of this by hiding malware within fake resumé files.

Attackers use job-listing and networking sites such as LinkedIn to identify potential targets. Vaas states, "One example: In April, eSentire research showed that new phishing attacks, targeting corporate hiring managers, were delivering the more eggs malware, tucked into bogus CVs. These campaigns sprang up a year after potential candidates looking for work on LinkedIn were lured with weaponized job offers: The offers dangled malicious ZIP archive files with the same name as that of the victims' job titles, as lifted from their LinkedIn profiles."

HR personnel must be careful when viewing and responding to potential job applicants. One click or download could render you vulnerable to scams and cons. Everyone should be careful to never click the "Enable content" button in a Microsoft Office document.

On-Demand Webinar: A Master Class on IT Security: Roger Grimes Teaches You Ransomware Mitigation

Roger Grimes, KnowBe4's data-driven defense evangelist, explains how to prevent, detect and mitigate ransomware. In this session you will learn:

- How to detect ransomware programs, even those that are highly stealthy
- Official recommendations from the Cybersecurity & Infrastructure Security Agency
- The policies, technical controls and education you need to stop ransomware in its tracks
- Why good backups (even offline backups) no longer save you from ransomware
- How to identify and stop these attacks before they wreak havoc on your network

Watch it now!

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Click here to access. ***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/

- August 10: SANS Webinar: Combating Ransomware with Cyber Deception: How to Save $4.62 Million (11 a.m.)
- August 16: Diving Deep on Data Governance in Local Government Webinar (2 p.m.)
- August 17: SANS 2022 Report: Moving to a State of Zero Trust (1 p.m.)
- August 17: Managing Cyber Risks: Understanding New Risks and How to Prepare Webinar (1 p.m.)
- August 18: Detect Possible Ransomware and Blackmail Attacks Before They Strike Webinar (1 p.m.)
- August 25: SANS 2022 Cloud Security Exchange (11 a.m.)
- August 30: Privacy Monthly Meeting (10 a.m.)

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.*