Monthly Cybersecurity Newsletter

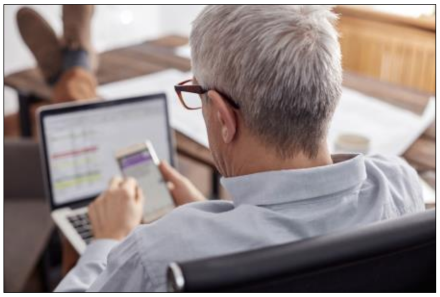
August 2020
Issue

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

Remote Working Errors Increase Risk

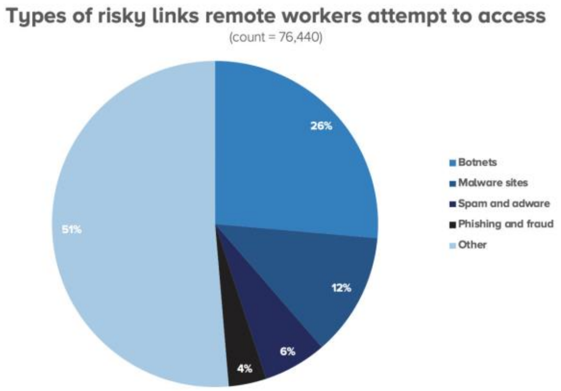


The increasing use of teleworking and reliance on the internet during the COVID-19 pandemic has created an environment that is ripe for cyber threats.

According to a study from Tessian, a technology company that focuses on email security, nearly half of employees in the United States and United Kingdom have made errors leading to cybersecurity consequences. The analysis was conducted during the COVID-19 pandemic, and it suggests that the disruption, stress and distractions of remote working make organizations more vulnerable to cyberattacks that are caused by human error.

A quarter of those surveyed admitted to clicking on a link in a phishing email while at work. Surprisingly, this most occurred in the technology sector (47%), where you might think employees would know better. Major reasons listed for clicking on phishing links were distraction, fatigue, perceived legitimacy of email and because emails supposedly came from a senior executive or well-known vendor/brand. Distraction was listed as the main reason for falling for a phishing scam ***and*** for sending an email to the wrong person. Sending email to a wrong person can result in information disclosure and can be particularly damaging if the type of data sent is restricted or highly restricted data (e.g., sensitive or confidential). Notably, 57% of workers stated they are ***more distracted*** when working from home.

According to data from another report by NetMotion, a software company that provides solution for remote workers, cybersecurity threats have risen as remote workers visit more “risky” websites outside of corporate networks. The analysis, which was also derived from data during the pandemic, revealed that employees clicked on 76,440 links that took them to potentially dangerous websites. The most common types of high-risk sites were botnets (a number of internet-connected devices that can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam and allow attackers to access the device), malware sites, spam and adware, and phishing and fraud sites. The graphic on the next page shows a breakdown of this information. Almost 1 in 5 risky links led to sites containing spam, adware, or malware.



With working from home becoming much more common, organizations must prioritize cybersecurity at the ***human layer*** and need to focus on providing more extensive user awareness training. This requires understanding employee behaviors and teaching safe cybersecurity practices to everyone. Proper education on social engineering attacks, phishing tactics and other commonly used tactics to trick users can make the difference between one unknowingly falling for a scam and one who can spot questionable, suspicious, or malicious web content.

While recent attacks have primarily revolved around COVID-19 themes, the actual tactics used have not been especially *novel*; they are just increased and more targeted. Sometimes the basic things are what will significantly reduce the risk of falling prey to a cyber threat.

- Secure all devices, including mobile computing devices.
- Keep all devices up to date with software patches.
- Have anti-malware software installed and keep it up to date.
- Use unique and complex passwords for all accounts.
- **MOST IMPORTANT**…Practice safe computing habits such as not replying to or clicking links in unsolicited texts and email messages.

New Phishing Campaign Abuses Cloud Services

A new phishing campaign uses several legitimate enterprise cloud services as part of an attempt to steal login credentials.

This new phishing campaign pretends to come from a help desk named “servicedesk.com” that mimics similar wording used by real IT helpdesk domains. Using three well-known enterprise solutions like IBM Cloud hosting, Microsoft Azure and Microsoft Dynamics to host the phishing landing pages adds legitimacy to the threat. Increasing cases of phishing campaigns abusing legitimate cloud solutions are on the rise and they add legitimacy to the phishing attacks. The increased complexity allows attackers to potentially bypass spam filters and security products.

Organizations can take several measures to better protect their remote workforce from such attacks by educating them to spot phishing tactics, requiring the use of publisher-verified apps and only allowing employees to OAuth apps trusted by the organization or provided by verified publishers.

At the end of the day, however, the best defense is to raise the awareness of phishing attacks among all individuals. The end user is the best and last line of defense of our networks and data and prevention of confidential data breach/loss. Be sure to check out STOP! THINK! CONNECT! for more information on raising cybersecurity awareness.

Collaborate Safely

Collaboration tools such as Microsoft Teams, Google Meet, Zoom and others allow you to pull together as a virtual team and securely work while being stuck at home.

There are a few security risks you need to be aware of:

01

Your account passwords are the keys to the kingdom (and to all your data). Make your passwords strong and unique. **Use Multi-Factor Authentication** - combining your username and password with something that you own, such as a One Time Password app on your phone.

02

login
Not secure agilones.com/Activate/*john@doe.com
FAKE
Microsoft
joe@doe.com
Enter Password
Password
Forgot Password
Sign in

BEWARE: scammers will try to steal your username and passwords. COVID-19 has brought about an increase in cyber attacks targeting remote workers on all platforms. Don't click on links asking you to log into a site or update details and don't trust anyone asking you for your passwords over the phone or text.

03

Who can do what with my documents? You can give other people permissions to co-author, edit or just view your files through group membership, or you by sending a link to the file. Think about the information and how sensitive it is before sharing it. Anything with personal information, financial data or intellectual property is usually classified.

04

Don't download files to personal devices. If you are working on a personal device, viewing documents in a browser is probably ok if you have the link and the approval of the owner. Refrain from downloading it to your personal and non-managed devices.

05

Public link for "Contract.docx"
Anyone will have access. Change link options
GET LINK
EMAIL LINK

Think twice before sharing files externally. External file sharing allows you to share a file with a person that is not part of your company's network. Remember that you are opening a window to your file shares or potentially sending sensitive data outside of your network so be careful about who you share your files with externally.

By Popcorn Training

Stay Safe While Working from Home

Working remotely has its benefits, ***but*** it comes with added responsibility. Click here for tips on how to stay secure while working from home.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
3RD ANNUAL NATIONAL
CYBERSECURITY
SUMMIT
SAVE THE DATES
COMING TO YOU VIRTUALLY
EVERY WEDNESDAY
9/16 | 9/23 | 9/30 | 10/7

This year will be the third year of the National Cybersecurity Summit, which is moving to a virtual format while still providing meaningful opportunities to discuss cybersecurity. Last year's summit, which drew more than 1,700 attendees, focused on providing cybersecurity strategies, policies and/or initiatives that facilitate collaboration between the full range of government, defense, civilian, intelligence and law enforcement entities.

This year, the summit will be held as a series of two-hour webinars every Wednesday for four weeks, beginning **Sept. 16 until Oct. 7**. Each week will have a different theme, highlight relevant topics and include keynote speeches and remarks from leadership across the government and private sectors.

For more information and to register, visit www.cisa.gov/cybersummit2020.

FEMA Announces 2020 National Preparedness Month Theme

FEMA's Ready Campaign promotes National Preparedness Month each **September** to encourage individual, family and community disaster and emergency planning. The 2020 theme is "Disasters Don't Wait. Make Your Plan Today."

This year the theme and national Public Service Advertisement, done in coordination the Ad Council, will follow the 2019 animation series stressing family preparedness efforts. This year's campaign will also focus on personal preparedness during the ongoing coronavirus (COVID-19) pandemic. Weekly themes and graphics for September will also be released later this month.

Earlier this year, the Ready Campaign and the Ad Council used those same animation concepts to create a series of animated videos and graphics to slow the spread of COVID-19. Videos such as "Plan Ahead for How to Deal with Disasters During Coronavirus," "Stay Home," and "Evacuate During Coronavirus" are all available at Ready.gov. The full videos can also be downloaded in broadcast quality from the Ad Council website.

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

Looking for More Training?

FedVTE
FEDERAL VIRTUAL TRAINING ENVIRONMENT

The U.S. Department of Homeland Security provides Federal Virtual Training Environment (FedVTE) courses at no cost to government personnel, including contractors and U.S. veterans. Courses include a variety of cybersecurity-related topics as well as certification preparation courses ranging from beginning to advanced levels. New courses are added or updated frequently. If you are interested in this training opportunity, more information can be found in the FedVTE course catalog.

August 7: Cleaning Up Our Cyber Hygiene Webcast

August 19: Real-World Use Cases of Metrics That Demonstrate Effective Security Practices Webcast

August 28: Zero Trust Solutions Forum

October 31: 2020 Business Continuity and Disaster Recovery Plans due!

Visit here for a list of more 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.*