Monthly Cybersecurity Newsletter

February 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 – Maria Thompson

---

2020 Has Record of Highest Reported Phishing Sites

2020 was an extraordinary year that presented many challenges. The global COVID-19 pandemic forced organizations to shift business to more remote work, and cybercriminals took advantage of this opportunity.

According to VPN service provider AtlasVPN, the search giant Google detected a record number of phishing websites – **2.1 million phishing domains** – last year – 25% more than the previous year and the highest number in a decade. While there is evidence that phishing sites were increasing even before the pandemic and the shift to more remote working, the COVID-19 has given cybercrminals additional vectors of attack. On average, Google detected over ***40,000 phishing sites*** every week in 2020.

"These websites pretend to be legitimate so that they can trick users into typing in their usernames and passwords or sharing other private information. Webpages that impersonate legitimate bank websites or online stores are common examples of phishing sites," according to Atlas in a Jan. 13 blog post.

The bottom line is you must be careful of the sites you visit online. They might be malicious. The following advice can help you avoid falling victim to phishing scams:

- **Pay attention to the URL.** If the URL (website address) has errors or unusual symbols, then that is a red flag. Fraudsters typically use domain names that look similar to legitimate sites, but they are not the same. For example: amazn.com instead of amazon.com.
- **Look for an SSL certificate.** Be sure the URL address starts with HTTPS, not with HTTP. A site should also have a padlock symbol before the web address. This means the website connection is encrypted. Never enter sensitive information on a website that is not encrypted. **WARNING:** Even if the website is secure, it might not be legitimate or safe. Fraudsters use SSL certificates to make their malicious sites seem safe, so proceed with caution.
- **Look for spelling and grammatical mistakes.** If you find a spelling error, proceed with caution. You can use URL checkers to see if a website has been flagged already. You can find many such tools by searching "Check URL safety" in Google.
- **Pay attention to internet ads.** Fraudsters can use internet Ads, such as Google Ads, to appear at the top of internet searches. This may not be a common occurrence but worth knowing nonetheless.

AtlasVPN's full article can be found here.

Workplace Communication Tools Prone to Phishing Hazards

The increased usage of online collaboration platforms, such as Microsoft Teams, Slack and Google Hangouts, has also increased the likelihood that more cybercriminals will attempt to take advantage of these workplace tools and the inherent trust individuals place on them.

Because people tend to believe these tools are more secure than email, they often share sensitive information too freely or click links and open attachments from these platforms that they might otherwise ignore. And that could be an advantage for a hacker.

For example, if an attacker successfully compromises a user's Office 365 credentials, not only do they have access to the user's email, but they can also access the user's Teams account and message others. Attackers who gain access to an organization's Teams environment can also gather sensitive information from a chat or channel conversation, send malicious files to other people and possibly gain access to protected information. Many organizations have third-party partners who are connected into their Teams environment, which increases the level of risk.

Cybercriminals are also utilizing fake email messages and notifications that look like legitimate Teams communications. These fake messages include a link that directs the end user to a malicious site that in some cases looks like a Microsoft login page. If victims enter their Microsoft credentials, their account is compromised, and the attacker can then use the compromised credentials for other malicious purposes.

As in all circumstances, you need to be careful what data you share, what links you click and what type of files you download, regardless of the communications tool you are using.

FBI Warns of Vishing Attacks

The FBI recently issued a Private Industry Notification to warn of ongoing vishing attacks attempting to steal corporate accounts and credentials. This is the second such warning since the start of the COVID-19 pandemic.

Vishing (also known as voice phishing) is a social engineering attack where attackers impersonate a trusted entity during a voice call to persuade the victim to reveal sensitive information, such as banking or login credentials. The cybercriminal tricks the targeted individual into logging into a phishing webpage they control to capture usernames and passwords. In many cases, once the attacker gained access to a company's network, they have gained greater network access than they expected, allowing them to increase their privileges using the compromised employees' accounts.

Be suspicious of unsolicited phone calls or email messages from individuals asking about employees or other internal information. Do not provide personal information or information about your organization, unless you are certain of a person's identity and their authority to have the information.

Learn more at the N.C. Department of Information Technology's website about vishing and other social engineering attacks and what you can do to avoid becoming a victim.

The following are a few resources that can help you protect your identity and be safer and more secure online this tax season – and year-round:

- STOP. THINK. CONNECT.™ Tips and Advice
- Identity Theft Resource Center
- The Federal Trade Commission's IdentityTheft.gov
- The Internal Revenue Service's Tax Scams and Consumer Alerts

If you believe you are a victim of identity theft or identity fraud, the following are some steps to take:

- File a report with your local law enforcement agency.
- File a report with the Federal Trade Commission (FTC).
- File a report with the three major credit bureaus (Equifax, Experian, and TransUnion) and request a "fraud alert" for your account.

If you receive spam or a phishing email about your taxes, do not click on the links or open any attachments. Instead, forward the email to phishing@irs.gov. Other tax scams or frauds can be reported by following this IRS guide.

PCI Webinars by Coalfire

The N.C. Office of the State Controller is pleased to announce that Coalfire, a PCI Compliance Validation Services vendor for the state of North Carolina will be presenting four webinars in 2021. The scheduled dates are as follows:

Date	Topic (tentative)
March 9, 2021	Policies, Procedures, Standards and Guidelines, What Are They?
June 15, 2021	Vulnerability Scanning and Penetration Testing – What is the Difference?
Sept. 7, 2021	Authentication and Access Control – Who Are You?
Dec. 7, 2021	Risk Assessments – Do you Feel Lucky?

All webinars will begin at 10 a.m. EST and will be approximately 1 hour.

Additional details (including registration information) will be sent out in advance of each webinar. For the current list of webinars being provided by the Office of the State Controller, please visit here.

Please Note: The PCI webinar announcements are distributed through the eCommerce listserv. If you are interested in receiving this information directly, please register online. The eCommerce listserv communications also provides updates for products and services on the Merchant Card and EFT Master Services Agreements, as well as webpage and enrollment form updates and reminders regarding annual PCI Compliance, SAQs and Quarterly Scans.

Red Flags!

Red flags are signs of danger or a problem. Protect yourself and your organization from cybercriminals by being aware of these warning signs and knowing actions to stay safe.

Common Red Flags	Actions to Stay Safe
Someone you don't know following you or your co-workers inside the office.	Contact security about unknown individuals.
Someone looking at your screen or watching what you type.	Pay attention to your surroundings and safeguard organizational information.
Someone you don't recognize looking through a desk.	Keep confidential information and devices locked-up/secured when not in use.
Social media connection requests from someone you don't recognize.	Don't accept unsolicited requests; report them to the service.
Receiving an unusual request from someone you know.	Contact the person directly to verify it's legitimate.
Requests that offer you something in exchange for private organizational information.	Be cautious before sharing any personal or organizational information.
Unexpected emails, phone calls, and voice or text messages.	Follow your organization's security policies for handling suspicious correspondences.
Urgent requests to take an action.	Never act on emotion and take the time to verify the request is legitimate.

Always stop, look, and think before you click on a link, open an attachment, or take any action!

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 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

Feb. 10, 2021: A Master Class on IT Security: Roger Grimes Teaches Ransomware Mitigation

Feb.17, 2021: The Cyber-Threat Landscape in 2020 and Bracing for 2021 Webinar

Feb.23, 2021: Security Culture - How it Helps Better Manage Risk webinar

March 9, 2021: *Policies, Procedures, Standards and Guidelines, What Are They?* PCI Webinar by Coalfire

April 2, 2021: Good Friday (State Holiday)

April 15, 2021: Tax Day

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.*

***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.*