Monthly Cybersecurity Newsletter

December 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

---

Holiday Shopping Scams

It is that time of year again, festivities, family gatherings and holiday shopping! Even though Black Friday and Cyber Monday have come and gone, holiday shopping is still in full swing. Due to the pandemic and many consumers avoiding brick and mortar stores, online sales are rapidly on the rise. As such, it is important to remain vigilant and be aware of the cyber risks to online shopping. While legitimate businesses are after your money, so are cybercriminals. When it comes to holiday shopping, you need to be careful that you do not fall prey to criminals. The following are ***10 cybersecurity tips*** to make your online shopping experience less risky and help keep you in the spirit of the season and off the "naughty list".

1. **Do not use public Wi-Fi for shopping activity.**

Public Wi-Fi networks can be very dangerous. While they can be convenient to use, they are not usually secure, and can potentially grant hackers access to your personal information. Never log in to banking/financial sites on a public Wi-Fi network and make sure you are logged out of those sites before connecting. However, it is best to avoid public Wi-Fi networks altogether.

2. **Make sure shopping sites are legitimate and secure.**

Before entering your personal or financial information into an online commerce site, you need to ensure that the site you are on is legitimate and can be trusted. Verify the site is the one you intended to visit by checking the URL. Also, look for the "lock" symbol in the URL bar and make sure "https" is in the beginning. These indicate the site uses encryption to protect your data.

3. **Know what the product should cost.**

The adage goes, if it is too good to be true, then it probably is. These kinds of scams run rampant during the holiday season! Make sure the company/vendor is legitimate, such as using a service like ResellerRatings.com. This site allows users to review online companies to share their experiences purchasing from those companies.

4. **Do not use debit cards for payment.**

When you are shopping online remember that it is best to rely on your credit cards or payment services such as PayPal. Credit cards offer more consumer protections and less liability if your information were to be compromised. On the contrary, debit cards are linked directly to a bank account, thus, you are at a much greater risk if a criminal were to obtain this information.

5. **Keep systems up-to-date.**

Be sure to keep your devices up-to-date. This includes your device operating system (OS), installed applications, and anti-virus software. This is one of the most important and easiest things you can do to help prevent criminals from accessing your information. Most software updates improve security by patching vulnerabilities and preventing new exploitation attempts.

6. **Think before you click.**

Scammers take advantage of the surge in holiday deals and communication to send out their own viruses and malware. Scams have evolved to the point they are depicted as legitimate discounts or special offers. Also, be careful with messages regarding shipping confirmations and changes. Phishing scams include cleverly crafted messages that look like official shipping notifications. Always use official channels to stay updated. As always, NEVER open an email from someone you do not know, did not expect to receive, or from a site you have not visited.

7. **Use strong, unique, and regularly changed passwords.**

Creating strong and unique passwords is still the best security practice for protecting your personal and financial information. Make sure your passwords are sufficiently long and complex utilizing a combination of upper- and lower-case letters, numbers, and special characters. Better yet, create a cryptic passphrase that is longer than the typical password, but easy for you to remember and difficult to crack. Be sure to not reuse passwords for multiple sites, particularly between work and personal resources. Lastly, update your passwords regularly.

8. **Avoid saving your information while shopping.**

Never save usernames, passwords or credit card information in your browser and periodically clear your offline content, cookies, and history. Also, you should avoid saving your payment information in your account profile when completing an online transaction. If the site autosaves your payment information, go in after the purchase and delete the stored payment details.

9. **Don't share more than is needed.**

Be alert to the kinds of information being collected to complete your transaction. If the site is requesting more data than you feel comfortable sharing, cancel the transaction. You only need to fill out required fields at checkout.

10. **Keep an eye on your financial accounts.**

Even with good cyber hygiene and best practices, you may still find yourself a victim of a cyber scam. Pay close attention to bank and credit card accounts, and be sure to monitor your credit report, to ensure there is nothing out of the ordinary.

For more information on holiday shopping safety, visit the following resources. Also, for those traveling out of the country during the holidays, be sure to review the State's International Travel policy.

- https://us-cert.cisa.gov/ncas/current-activity/2020/11/24/online-holiday-shopping-scams
- https://staysafeonline.org/wp-content/uploads/2020/11/Online-Holiday-Shopping-1.pdf

Employee Stress and Remote Work Are Leading Causes of Data Breaches

Stressed employees and remote working conditions are the two most common causes of email-related data breaches, according to a survey commissioned by data security company Egress. Based on interviews with hundreds of senior IT security employees in the US and UK, the survey found the following:

- 93% had experienced data breaches via outbound email in the past 12 months.
- Organizations reported at least an average of 180 incidents per year when sensitive data was put at risk, equating to approximately one every 12 working hours.
- The most common breach types were replying to spear-phishing emails (80%); emails sent to the wrong recipients (80%); incorrect file attachments (80%).
- 62% rely on people-led reporting to identify outbound email data breaches.
- 94% of surveyed organizations have seen outbound email volume increase during COVID-19. 68% say they have seen increases of between 26 and 75%.
- 70% believe that remote working raises the risk of sensitive data being put at risk from outbound email data breaches.

The survey determined that employee stress and remote work were the two most frequently cited causes of serious breaches. In terms of the impact of the most serious breach incident, on an individual-level, employees received a formal warning in 46% of incidents, were fired in 27% and legal action was brought against them in 28%.

At an organizational-level, 33% said it had caused financial damage and more than one-quarter said it had led to an investigation by a regulatory body.

These sobering statistics reveal the importance of ***regular cybersecurity awareness training for all employees and contractors***. Awareness training can help minimize the risk of social engineering attacks and accidental breaches by teaching individuals to follow security best practices. Ongoing security awareness training is also an important component of the cybersecurity best practices known as the CIS Controls. These offer prioritized and prescriptive actions that protect organizations from known cyber-attack vectors. A top priority is the ability to identify social engineering attacks such as phishing, phone scams, and impersonation calls.

For the full story from Egress, visit the following:

https://www.egress.com/en-us/news/2020-outbound-email-security-report

The end-of-the-year celebrations are the most lucrative period for cybercriminals.

Beware of email phishing attacks! Think and analyze before clicking on any sales link.

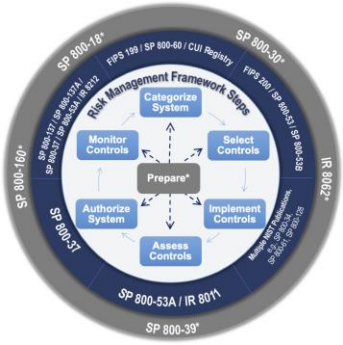
Advertisements that appear on the screen can bring malicious programs or throw you at fake sites. Do not click!

Before you shop online, make sure that the site in question is safe and reliable.

Use secure payment methods and research the reputation of the site or seller.

Be wary of big discounts on products and other advantages offered by unfamiliar sites on social networks.

El Pescador
a KnowBe4 company



Risk Management Framework Online Training

The National Institute of Standards and Technology (NIST) has released an updated Risk Management Framework for Systems and Organizations Introductory Course to reflect guidance from NIST Special Publication (SP) 800-37, Revision 2. The Risk Management Framework (RMF) was developed by NIST to help organizations manage information security and privacy risks to and from Information Technology (IT) systems more easily, efficiently, and effectively.

This three-hour online course provides individuals **new to risk management** an overview of a flexible methodology for organizational and system risk, the Risk Management Framework (RMF). For individuals with experience with NIST SP 800-37, Revision 1, this course explains **updates** to the RMF in Revision 2, including the integration of privacy and supply chain risk management into this holistic process.

The RMF Introductory Course describes ***at a high-level*** the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step. The course can be launched through your internet browser and upon completion, individuals may print a certificate of completion. The training is also available for organizations who wish to include it as a module in their Learning Management Systems (LMS) in the following LMS standards: SCORM, AICC, xAPI, and cmi5.

Please contact sec-cert@nist.gov with questions or comments.

PCI-DSS 4.0 Webinar

Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **December 9, 2020 at 10:00am**. The title of the webinar will be ***PCI 4.0 - Merchant and Service Provider Responsibilities***. Join Bill Franklin, Senior Director Payments, for a discussion about the timeline for PCI DSS 4.0 and what is expected of merchants and service providers in the new PCI DSS 4.0.

Bill is responsible for client engagements focused on projects and advisory services regarding the Payment Card Industry Data Security Standards. He has over 25 years of experience conducting and managing IT Governance, Risk, and Compliance assessment and audits in the areas of PCI, HIPAA, FFIEC, NIST 800-53, ISO and COBIT. Bill's areas of expertise include IT compliance regulations and frameworks, IT security, technology risk assessment & audit, project management, and System Development Life Cycle (SDLC). You may join the meeting from your device via the following link: https://global.gotomeeting.com/join/165648389

You can also dial in using your phone by dialing 1-877 309 2073. Access Code: 165-648-389.

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

December 3: 5 things you need to know to future-proof your data security today SANS webinar.

December 9: *PCI 4.0 - Merchant and Service Provider Responsibilities* webinar by Coalfire.

December 15: It's Been A Hard Year - 2020 Security Operations Center (SOC) Survey - SANS@Mic Keynote SANS webinar.

December 24, 25 & 28: State of NC Christmas Holiday

January 1, 2021: New Years Day Holiday

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.*