Monthly Cybersecurity Newsletter

December 2021 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Rob Main

---

Shopping Tips for the Holiday Season

It is that time of year again – festivities, family gatherings and holiday shopping. Many consumers will avoid brick and mortar stores and choose to shop online instead. 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. Be careful not to fall prey to them.

Here are 10 cybersecurity tips to make your online shopping experience less risky, help keep you in the spirit of the season and help you stay safe from those who are on the "naughty list."

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

2. Make sure shopping sites are legitimate and secure. Shop at well-known retailers you trust and where you have previously done business. Before entering your personal or financial information into an online commerce site, be sure it 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 at 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." Scams run rampant during the holiday season. Use a service, such as ResellerRatings.com, to make sure the vendor is legitimate. Such sites allow users to review online companies and share experiences.

4. Do not use debit cards. Use credit cards or payment services, such as PayPal. They offer more consumer protections and less liability if your information is compromised. With a debit card, you are at a much greater risk because it is linked directly to a bank account. In a debit card dispute, you are in a weaker position because the merchant already has your money, and it could take weeks to get it back. With a credit card, you have time to dispute a charge before money is paid.

5. Keep systems up to date. Be sure to keep your devices up to date. This includes your device operating system, 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 marketing emails 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 and unique 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 with 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.

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. Avoid saving 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. If the site has the option, check out as "guest" to avoid giving personal/payment information online.

9. Don't share more than is needed. Be alert to the kind 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. Monitor your financial accounts. Even with good cyber hygiene and best practices, you might 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:

- CISA: Online Holiday Shopping Scams
- National Cybersecurity Alliance: Tips for Safe Online Holiday Shopping (PDF)

Social Account Phishing in Top Three

New data from CheckPoint's Q3 Brand Phishing Report on the use of impersonation in phishing attacks focused on social media accounts shows some very realistic and worrisome websites and emails that could definitely fool you. Microsoft has nearly always dominated the list of the most impersonated brands. CheckPoint's report shows threat actors are shifting their focus – Microsoft's share of impersonated brands dropped from 45% in Q2 to just 29% in Q3.

The new report shows social media has become of great interest – specifically WhatsApp, LinkedIn, and Facebook – in the top 10 imitated brands. What is truly concerning about attacks using these brands is how real they appear to be. It used to be that social engineering attacks consisted of poorly worded and poorly designed webpages and emails. However, today's impersonation is nearly perfect.

Users should be cautious when divulging personal data and credentials to business applications or websites and to think twice before opening email attachments or links – especially emails that claim to be from companies such as Amazon, Microsoft or DHL, as they are the most likely to be impersonated. Read the full report and see examples of these impersonation attacks.

Protect Yourself from Cybercriminals This Holiday Season

***Verify** information before sharing on social media.*

*Only shop from **trusted retailer websites.***

***Confirm** purchases before opening delivery notification links.*

*Only download apps from your device's **certified app store.***

***Monitor** bank account and credit card activity.*

Happy Holidays from KnowBe4

'Tis the Season for the Wayward Package Phish

The holiday shopping season means big business for phishers and other attackers. With the increase in online shopping, attackers find more success with a lure of fake shopping confirmations and shipping notifications. One kind of a scam is a SMS-based phishing that spoofs a FedEx shipping notification and site page in an attempt to extract personal and financial information from unsuspecting recipients.

With the increase in phishing and other cyberattacks, it is a good time to remember the following tips from KrebsonSecurity:

- Avoid clicking on links or attachments in emails, text messages and other mediums.
- Avoid responding to "urgent" requests or notifications. Most phishing scams invoke a sense of emergency that threatens negative consequences if you fail to respond or act quickly.
- Rather than responding to an email or text message, visit the site or service in question manually by typing in the legitimate URL or by using a pre-saved bookmark to the site.

Read KrebsonSecuritys full article. For more information on holiday scams, visit the FBI's holiday scams page.

Be Aware of Charity Scammers

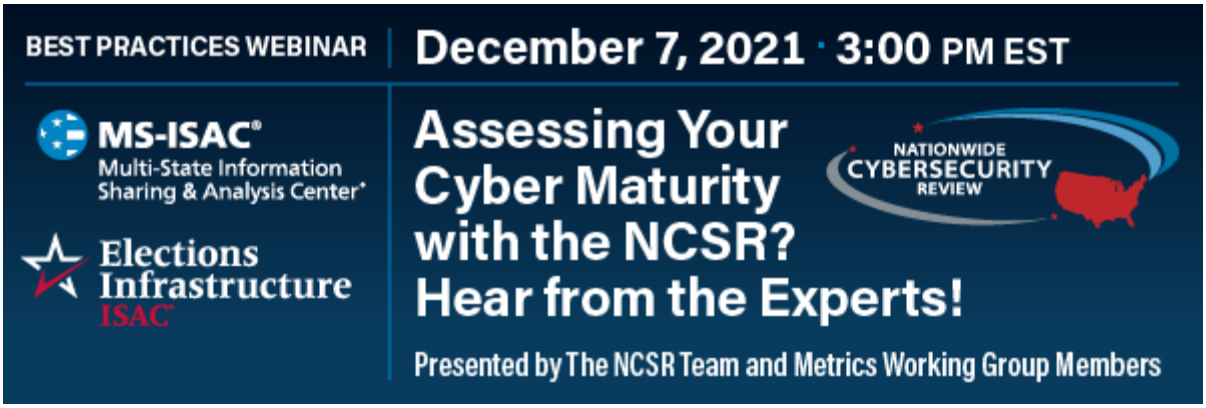
As the year comes to close during the holiday season, donating to your favorite charities is great way to help these organizations further their mission. However, this also gives cybercriminals opportunities to take advantage of you with charity scams. The Federal Trade Commission has provided the following tips to help you donate safely this holiday season and all year round:

- **Do some research online**. Start by searching for causes you care about along with phrases such as "best charity" or "top rated charity." When you consider giving to a specific charity, search its name, plus "complaint," "review," "rating" or "scam." You can use resources such as Charity Navigator or CharityWatch to verify your search.

- **Be careful how you pay**. If someone wants donations in cash, by gift card or by wiring money, don't do it. That's a trap for scammers to take your money. Be on the safe side and pay by credit card or check, and keep records of your donations. Before you click on a donation link, check out this FTC article to help you make sure your money is going where you think it is.

- **Keep scammers' tricks in mind.** Some cybercriminals try to trick you into paying them by thanking you for a donation that you never made, or using a local area code when making a call. Make sure to watch out for red flags, such as guaranteeing sweepstakes winnings in exchange for a donation (it's illegal) or claims that your donation is tax-deductible when it's not. If you're feeling rushed or pressured to make a donation, that should also be a red flag that something isn't quite right.

Every year cybercriminals take advantage of honest, charitable individuals. Be aware of their attacks. For more information, please visit the FTC page on charity scams.



Nationwide Cybersecurity Review (NCSR), a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs, is now open through February 28, 2022. A best practices webinar on the NCSR will be held on **Tuesday, Dec. 7, 2021, at 3 p.m.** Hear from Metrics Working Group members who have participated in the NCSR for multiple years and used it as a tool to drive improvements in their cyber program. They will review their experience with the NCSR and provide best practices to approach the assessment.

What to Expect

- Learn about approaching the NCSR as an organization and taking the assessment.
- Learn about resources available to assist with evaluating and communicating results.
- Ask the experts. Use the Q&A to connect with peers and ask NCSR related questions.

Register today for the NCSR webinar. Please direct any questions to info@cisecurity.org.

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/:f:/r/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News?csf=1&web=1&e=LZkrj8

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/newsletters/ouch/

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.*