DECEMBER 8, 2021 // WEDNESDAY // ISSUE 4

SECURITY NEWS

HOLIDAY SAFETY

Merry Christmas!!!

CHRIS MCDANIEL
DECEMBER 2021

The Yadkin County Information Technology Department would like to wish everyone a Safe and Merry Christmas. It is finally that time of year again when we get to start planning our holiday traveling, shopping, and giving plans. We would like to remind everyone to stay security smart when traveling, giving, and shopping this year.

The newsletter I have put together this month will focus on Holiday Safety. Please take some time to read over the tips provided that will help keep you safe this holiday season. Remember there are cybercriminals out there constantly looking to ruin our holiday and make our lives difficult. Let's not fall prey to their tricks and always remember to think before you click. Hope Y'all have a great holiday this year and we look forward to seeing you next year.

Be Aware of Charity Scammers

NCDIT
DECEMBER 1, 2021

As this year comes to a close during the holiday season, donating to your favorite charities is a 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 you 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 is not 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.

The information for this article provided by the North Carolina Department of Information Technology and may be found via the link provided here: NCDIT.

SECURITY TIPS FOR VACATIONS

Princess Young, SANS, December 1, 2021

Overview

As the holiday season approaches, millions of people will be traveling. If you are one of the many, here are tips to help you stay cyber savvy and safe.

Mobile Devices

Bring as few devices as possible. The fewer devices you bring when traveling, the fewer devices that can be lost or stolen? Whenever you leave a hotel room, restaurant, taxi cab, train or airplane, do a quick device check and make sure that you have all your devices. Don't forget to also have your friends or family traveling with you to double check for their devices as well, especially children who may leave a device behind on a seat or in a restaurant. As for devices you choose to bring, make sure they are updated so they are running the latest operating system and apps. Always keep the screen lock enabled. If possible, ensure you have a way to remotely track your devices if they are lost. In addition, you may want the option to remotely wipe the device. This way if a device is lost or stolen, you can remotely track and/or wipe all sensitive data and accounts from the device. Finally, backup all your devices you choose to take with you, so if one is lost or stolen, you can easily recover your data.

Wi-Fi Connections

When traveling, you may need to connect to a public Wi-Fi network. Keep in mind you often have no clue who configured that Wi-Fi network, who is monitoring it or how, also who else is connected to it. Instead of connecting to a public Wi-Fi network, if possible connect to and use the personal hotspot feature of your smartphone. This way you will know you have a trusted Wi-Fi connection. If that is not available and you need to connect to a public Wi-Fi network (such as at an airport, hotel, of café), use a Virtual Private Network, often called a VPN. This is software you install on your laptop or mobile devices to help protect your Wi-Fi connection. Some VPN solutions include settings to automatically enable the VPN when connecting to non-trusted Wi-Fi networks.

Public Computers

Avoid using public computers, such as the ones in hotel lobbies or at coffee shops, to log into any accounts of access sensitive information. You don't know who used the computer before you, and they could have infected it accidentally or intentional with malware, such as a keystroke logger. Stick to devices you control and trust.

Social Media

We love to update others about our travels and adventures through social media, but we may not always know who every friend of viewer is online. Remember to avoid oversharing while on vacation as much as possible and consider waiting to share your trip until you're home. In addition, don't post pictures of boarding passes, driver's licenses, or passports as this could possible lead to identity theft.

Work

If you will be working while you're on vacation make sure you check what your travel policies are ahead of time, including what devices or data you can bring with you and how to remotely connect to work systems safely.

Vacation should be a time for relaxing, exploring, and having fun. These simple steps will help ensure you do so safely and securely.

The information for this article from SANS may be found via the link provided here: SANS OUCH! Newsletter.

SHOPPING TIPS FOR THE HOLIDAY SEASON

NCDIT, December 1, 2021

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)

'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.

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