Monthly Cybersecurity Newsletter

December 2022 Issue

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

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

Five Top Scams to Watch Out for This Holiday Season

The holiday season is a time when people are especially vulnerable to scams. This is because they are busy and often have their guard down. Criminals take advantage of this by circulating fake e-gift cards, posing as charities, targeting specific demographics and other deceptive actions. In this three-minute article, we will discuss Google's five most popular scams circulating this holiday season.

1. **E-gift card scams**
2. **Charities**
3. **Demographic targeting**
4. **Subscription renewals**
5. **Crypto scams**

With the holiday season in full swing, so are gift card and prize scams. These scammers will often lie about being a known contact of yours to try and get you to buy them a gift card, or they may offer an amazing prize in exchange for your credit card information. If you receive any suspicious emails like this from someone claiming to be your friend, make sure to confirm it with them through another method before doing anything further. And as always, if something seems too good to be true, it probably is.

Be wary of scammers and phishing attempts; they worsen during the holiday season. This hurts not only those who fall for the scams but also charities that could have benefited from donations. For example, an attacker might pretend to be associated with a charity related to current events or one with a familiar name. If someone contacts you asking for money via personal email or another method, beware that it might be fraudulent.

With more people shopping online and sharing personal information this holiday season, scammers are taking advantage by targeting consumers with frauds that seem more realistic. For example, you might get an email from what looks like your child's school PTA about a holiday fundraiser. But if you click on the link in the email, it could take you to a fake website where you are asked to enter sensitive information like your credit card number or Social Security number.

These types of scams can be difficult to identify because they seem so personalized. But if you are aware of potential threats and know what to look for, you can help protect yourself against them.

Scammers love to target people at the end of the year, and one particularly nasty version of these emails spoofs antivirus services. They lure victims with promises of improved security, but if you take a closer look at the sender's email address, you can usually spot these scams pretty easily.

Cryptocurrency-based scammers are more prevalent during these times of high crypto usage. They often use a cryptocurrency wallet to collect payments and might threaten their victims if they do not receive the funds. Gmail usually sends a warning about these kinds of emails, but it is helpful to know how to spot them on your own too. Some key elements found in fraudulent emails include typos, strange email addresses and demands for payment.

By being aware of these five popular scams circulating this holiday season, you can protect yourself and your loved ones from potential fraud. Learn more about the social engineering dangers lurking online.

This article is redistributed with permission from KnowBe4.

Safe Online Holiday Shopping

Now that holiday shopping is in full swing, the National Cybersecurity Alliance is listing a few online shopping trends they have noticed and giving a few tips about how to stay safe online while buying gifts. Review these tips for more information.

Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks

The U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and Multi-State Information Sharing and Analysis Center have released guidance, Understanding and Responding to Distributed Denial-of-Service Attacks, to provide organizations with proactive steps to reduce the likelihood and impact of DDoS attacks. The guidance is for both network defenders and leaders to help them understand and respond to DDoS attacks, which can cost an organization time, money and reputational damage.

Concurrently, CISA has released the Capacity Enhancement Guide (CEG): Additional DDoS Guidance for Federal Agencies, which provides federal civilian executive-branch agencies additional DDoS guidance, including recommended contract vehicles and services that provide DDoS protection and mitigations. CISA encourages all network defenders and leaders to review:

- Joint Guidance: Understanding and Responding to Distributed Denial-of-Service Attacks
  - https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

- CEG: Additional DDoS Guidance for Federal Agencies
  - https://www.cisa.gov/sites/default/files/publications/ceg-additional-ddos-guidance-for-federal-agencies_508c.pdf

- Tip: Understanding Denial-of-Service Attacks
  - https://www.cisa.gov/uscert/ncas/tips/ST04-015

Let's Have Cyber-Safe Holidays!

Don't let cybercriminals ruin your holiday fun!

Whether you are traveling or buying or selling items online this holiday season, keep the following tips in mind.

Online Threat Prevention

Keep an eye out for fake coupons, unbelievable promotional deals, or even fake shipping notices.

Cybercriminals will repeatedly spam you with notifications this season, don't let your guard down. Never assume notifications are safe.

Only purchase and use gift cards with the authorized retailer.

Travel Threat Protection

Use verified, secure Wi-Fi connections and avoid connecting to free public Wi-Fi.

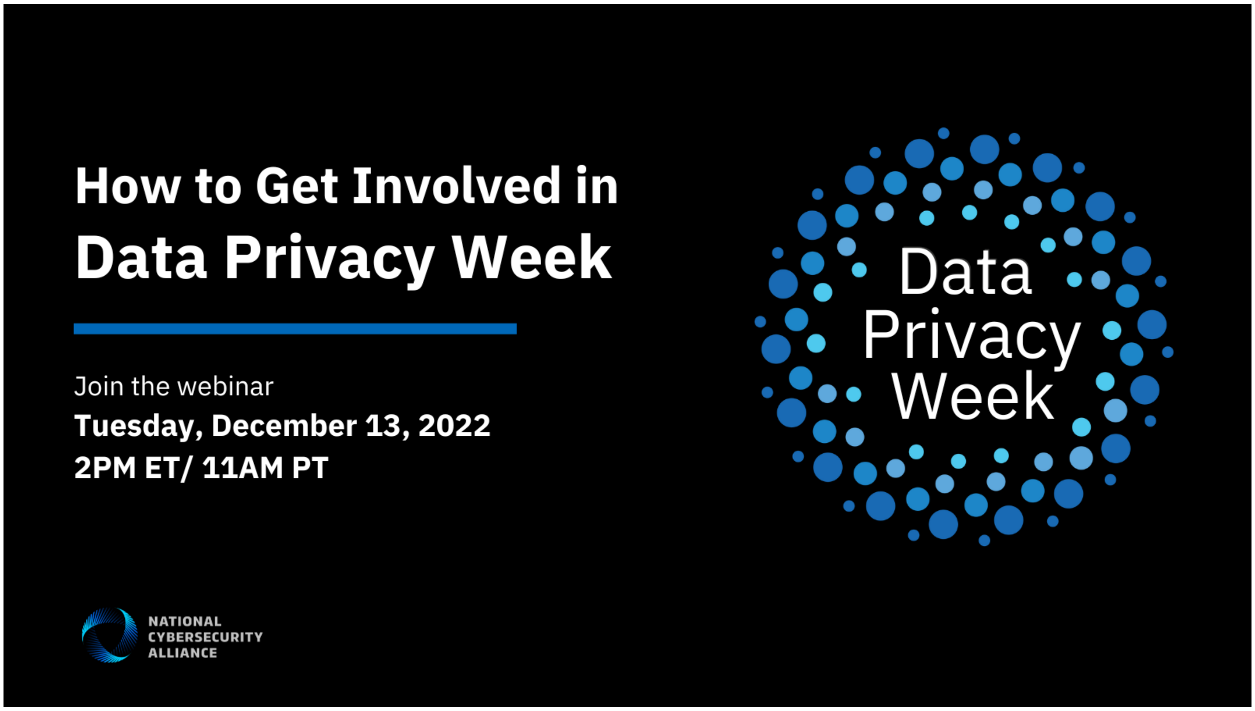
Never leave your devices unattended and always secure them with strong passwords.

Research the legitimacy of booking sites before making travel arrangements.

Cybercriminals will always try to trick you.
Remember to **stop**, **look**, and **think** before taking any action!

Have a safe, fun holiday season from KnowBe4

| www.KnowBe4.com



How to Get Involved in Data Privacy Week

Join the webinar
Tuesday, December 13, 2022
2PM ET/ 11AM PT

NATIONAL CYBERSECURITY ALLIANCE

Data
Privacy
Week

Data Privacy Week (Jan. 22-28, 2023) is an annual campaign with the goal of educating individuals and businesses about the importance of online privacy.

Learn how you and your organization can get involved in 2023’s campaign by registering for a special webinar at 2 p.m. on Tuesday, Dec. 13. Presented by the National Cybersecurity Alliance, the event will take an in-depth dive into 2023’s theme and messages, review materials in this year’s toolkit and share tips and advice for launching your own initiatives.

KnowBe4
Human error. Conquered.

ON-DEMAND WEBINAR

Discover 5 Major Threats to Your Digital Supply Chain and How to Reduce Your Vendor Risk

WATCH NOW »

In this webinar, **Discover 5 Major Threats to Your Digital Supply Chain and How to Reduce Your Vendor Risk**, James McQuiggan, Security Awareness Advocate at KnowBe4, discusses why a vendor risk management program is a critical step to securing your organization from third-party services or vendor products.

Watch Now:
https://kcmgrc.knowbe4.com/5-threats-digital-supply-chain-odw

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Click here to access. ***Note**: You must have a valid state employee Microsoft 365 account*.

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

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.

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.*