MEL CYBER TASK FORCE UPDATE

Holiday Cyber Safety

With so many people choosing to shop online this holiday season, you need to be extra vigilant about avoiding cyber scams that can not only steal your money, but also corrupt your home and/or work computer and network.

E-commerce sales are expected to rise by 25 to 35 percent as shoppers choose using their computers and smartphones over brick and mortar stores. Cyber criminals may target victims through a variety of methods, including compromised or spoofed websites, phishing emails, social media ads and messages, or unsecured Wi-Fi networks.

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) has put out a number of tips to help increase awareness of these cyber threats and help you avoid these cyber traps at home and work.

1. Do Your Online Shopping at Home and avoid using work computers - Avoid using public computers, such as those at a library or hotel, or public Wi-Fi connections to log in to personal accounts or conduct online shopping. Public computers could be infected with malware designed to steal your information and hackers can intercept network traffic traveling over unencrypted Wi-Fi signals.

TIP: If you must connect to public Wi-Fi, use a virtual private network (VPN) to secure information transmitted between your device and the internet. Refrain from using work computers to make online purchases as cyber threats could endanger company and/or customer information.

2. Look Out for Holiday-Themed eCards and Messages Meant to Install Malware - In the past, users reported being targeted with various Thanksgiving Day-related scams. In some cases, spoofed emails were sent appearing to originate from legitimate organizations and contained the subject line “Thanksgiving eCard,” and others used lures, such as the subject lines “Happy Thanksgiving Day Greeting Message” and “Thanksgiving Day Card.”

TIP: *As malicious actors commonly leverage public interest and current events to conduct financial fraud and disseminate malware, users are reminded to exercise caution with unexpected or unsolicited emails, especially those with a holiday theme.*

3. Avoid Links and Attachments in Unsolicited Emails - Be careful not to click on those enticing emails offering coupons or special “limited time offers” they may contain links or attachments that install malware to steal user credentials. Recently, the NJCCIC has observed Amazon, PayPal, and FedEx phishing emails attempting to deliver to New Jersey State Employees in order to steal users' credentials.

TIP*: Don’t click on these email links, instead navigate directly to retailer websites by typing the legitimate URL into their browser. Also refrain from entering login credentials on websites visited via links delivered in emails.*

For details, contact the MEL Underwriting Manager or your local JIF Executive Director

MEL CYBER TASK FORCE UPDATE

4. Beware of Magecart and Other Online Skimming Attacks - This is a type of web-based data skimming operation used to capture customer payment card data from the checkout pages of online stores. A malicious JavaScript code is embedded in the check-out page to skim the data which can be used to make fraudulent purchases or sold on the dark web.

TIP: *Use credit cards over debit cards when shopping online as they often have better consumer fraud protections, and consider enabling charge notifications for every card transaction. If you discover fraudulent activity notify the banking institution, lock the card and request a new card.*

5. Enable Multi-Factor Authentication (MFA) on All Accounts - This involves combining at least two of the following: something you know, something you have, and something you are - on every account that offers it, as this will greatly reduce the risk of account compromise via credential theft. Even if a cybercriminal obtains a username and password, they will be unable to access that user's account without their second factor.

TIP: *Choose authentication apps, hardware tokens, or biometrics as a second factor over SMS-based authentication due to the risk of SIM-swapping, though using any form of MFA is beneficial.*

6. Take Caution with Social Media Ads - You know the ones you see as you scroll through social media platforms or those that "pop-up" on your screens. While many of these ads link to known, legitimate vendor websites, users may also be confronted with ads that link to malicious or otherwise suspicious sites that could be used to install malware, steal credentials, or sell counterfeit goods.

TIP: *Beware of website addresses that don't seem right, some cybercriminals use URL shortening to hide the true destination of a link. Use a URL expander to reveal the true destination prior to visiting websites and verify websites are the legitimate vendor prior to making any purchases*.

7. Beware of "Secret Sister" Gift Exchange Scam - Social media posts promoting a "Secret Sister" gift exchange promise between 6 and 36 gifts in exchange for sending one gift. The scam begins with a request for the name/address of the recipient and friends. While this type of chain-letter appears innocent, it is illegal and considered a pyramid scheme.

TIP: Only participate in gift exchanges with individuals you know personally and refrain from sharing too much personal information online.

8. Avoid Connecting Devices to Public Charging Stations - These kiosks can expose devices to the risk of malware infection, and can contain concealed computers that attempt to extract data such as contact information, photos, and videos from connected devices, unbeknownst to the users.

TIP: Charge your devices at home or in your car. Even if the charging station is not malicious, the manufacturer or owner of the kiosk may require users to input their email addresses or phone numbers in order to charge their devices, potentially exposing them to unwanted marketing campaigns, phishing emails, and scam calls.

9. Verify Charities Before Donating - Users may be prompted to donate via solicitations received through email or social media; however, these may be promoting fake charities or impersonating legitimate charities.

TIP: Prior to donating, visit the FTC site to verify a charity's legitimacy and ensure you are visiting the charity's legitimate website to donate.

For more information about these tips visit the NJCIC website: www.cyber.nj.gov/informational-report/stay-cyber-safe-this-holiday-season

To learn more about Cyber Risk Control and how to best educate your employees and protect your organization against cybercrime visit: https://njmel.org/mel-safety-institute/resource-center/public-officials/public-officials-cyber-risk-control/