Monthly Cybersecurity Newsletter

November 2018
Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

Holiday Season, Hackers, and You!

The holiday shopping season is upon us again and people will be making their lists and checking them twice, three times or more. This is a wonderful time of year, full of joy and excitement, but it can also be a stressful and dangerous time as well. Criminals prey upon people during the holiday shopping season seeking to steal personal information, money, property, and your peace of mind. A recent study found that about 67% of shoppers will go to department stores for their holiday shopping, but about 60% plan to *only shop online*. In the United States, people are expected to spend about $151 billion online this holiday season. There is usually an uptick in fraud and phishing scams this time of year. So, it is worth taking a few moments to remind ourselves of the following tips about how we can be more secure during the holiday season.

- Stay alert for phishing emails and deals that look “too good to be true.”
- Shop at well-known retailers that you trust and where you have previously done business.
- Research items you are interested in purchasing, reading vendor/product reviews.
- Establish strong and unique passwords for each online shopping account.
- Check out as “guest” to avoid giving personal/payment information online.
- Use one credit card for all your holiday shopping, limiting damage if your info is stolen.
- Monitor your bank and credit card accounts during and after the holiday season.
- Make sure your purchases are secured with encryption.
- Keep your devices up-to-date with current and active anti-virus software.
- Avoid announcing on social media when you are away from home.

Also, when purchasing and receiving gifts this season, be aware of the risks of “smart toys” and other connected Internet of Things (IoTs). These devices can be fun, and they provide a wealth of features, but they can also be risky. For instance, children’s toys and baby monitors can be compromised, putting the privacy and safety of your children at risk. For more information on IoT toys, please review the FBI Public Service Announcement (PSA) on Internet-Connected Toys.

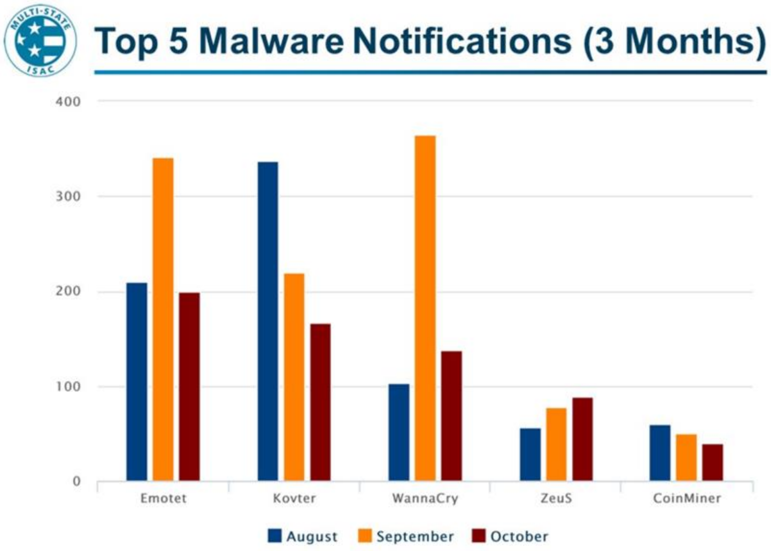
Finally, be sure to review the Holiday Shopping Scams tip sheet from the Security Awareness Company that is attached to the end of this newsletter. The National Cyber Security Alliance (NCSA) has also published a Happy Online Holiday Shopping Tip Sheet that provides tips for online shopping. Have a very happy and safe holiday season!

Another Ransomware Attack

Another North Carolina government entity has been impacted by a ransomware attack – Onslow Water and Sewer Authority (ONWASA). Ransomware is a type of malicious software (malware) designed to deny access to a computer system or data until a ransom is paid. It typically spreads through phishing emails or by someone unknowingly visiting an infected website. ONWASA was still recovering from the effects of Hurricane Florence when they began experiencing a malware attack on October 4, believed to be the Emotet trojan. The utility believed the problem was under control until they continued to experience problems. In what could have been a timed event, the RYUK ransomware then attacked the utility on October 13. ONWASA staff took immediate action to protect their systems but the malware spread quickly and encrypted their databases and files.

ONWASA coordinated with the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the State of North Carolina, and several technology security companies to respond to the incident. The cybercriminals behind the ransomware attack reached out to ONWASA to demand a ransom, which the utility refused to pay. Many services will have to be completed manually until the systems are fully restored, which will likely take weeks, if not months. Other government entities that have been recently hit by ransomware include Mecklenburg County, Atlanta, Boston, and the Colorado Department of Transportation.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) has identified the five most common malware notifications escalated over the past three months (see chart). Emotet sits in the top spot this month. The initial infection typically occurs from malicious spam (malspam) phishing emails that are disguised as fake invoices which contain either malicious links or attachments.



The National Cybersecurity and Communications Integration Center (NCCIC) recommends the following to reduce the risk of a ransomware attack:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Backup data on a regular basis and keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet.

In addition, NCCIC also recommends that organizations employ the following best practices:

- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

Following these steps can help lower the risk of you becoming a victim to ransomware.

>>>Monthly Newsletter

Don't forget the other **monthly newsletters** that are available to you. The following are some other cybersecurity newsletters the ESRMO recommends to you. We hope you find them beneficial.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is on ***Staying Secure While Shopping Online.***

➢ https://www.cisecurity.org/resources/newsletter

SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Am I Hacked?***

➢ https://www.sans.org/security-awareness-training/ouch-newsletter

The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link:

https://www.sans.org/security-awareness-training/video-month

The SANS Institute free webcasts may be accessed via the following link:

https://www.sans.org/webcasts/upcoming.

Upcoming PCI Webinar

Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar titled ***Managing Service Providers*** for the State of NC's merchant community on **December 4, 2018, at 10 am**. The speaker will be Jon Bonham. More information is below.

With all the changes to the PCI Data Security Standard and the technologies that are evolving to address them, one of the biggest problems is vendor management. This final session of the year will focus on PCI-DSS requirements 12.8 and 12.9. It will cover the following items:

- How to set up and maintain a PCI compliant vendor management program

- What to look for when hiring third party vendors
- How to manage your vendors and prove their compliance
- How to set up a responsibilities matrix
- What are the responsibilities of the service providers

The session will conclude with time for questions. You may join the webinar from your computer or mobile by visiting https://fuze.me/93227287.

Standard Dial-In:

- Call United States: (855) 346-3893 (toll free)
- Enter the meeting ID: 93227287 followed by the # key

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses including:
    - Network +
    - Security +
    - Certified Information Systems Professional (CISSP)
    - Windows Operating System Security
    - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Individuals can take courses to build the required knowledge, skills, and abilities in the cybersecurity field
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

<u>Do you have something to share?</u> Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.

Tis the season... for scams

Many of us associate the end of the year as a time of thanks and giving. But it's also a time of taking, as scammers and criminals get into the holiday spirit (maliciously, of course). Regardless of what holiday you do or don't celebrate, stay alert this season, both online and in real life!

Shopping IRL (In Real Life)

"Only available in stores" is a marketing tactic used by retailers to lure shoppers away from their screens. While you might not "get hacked" when shopping in real life, there are still security risks! This is particularly true on Black Friday, when hundreds of thousands of people flock to stores to take advantage of deals.

Situational Awareness

Don't get lost in your phone or tablet, and be aware of who might be peering over your shoulder. Stay calm in crowded areas. Know where all the exits are and have a plan going in. If you are with a group, set up rendezvous points. A little situational awareness goes a long way!

Pickpockets & Thieves

You should keep a close eye on your belongings and never ask a stranger to watch your stuff for you. If you have personal items in your pockets, such as a wallet or cash, place them in your front pockets which are more difficult to pick.

Card Skimmers

If you must get cash from an ATM, inspect the machine thoroughly before inserting your card. Criminals rig ATMs with cards skimmers to steal your information. That's why it's best to get cash from inside a bank location whenever possible. Routinely check your accounts to ensure no unauthorized or additional charges have been processed.

Public WiFi

Never access sensitive information when on a public network, which means no purchasing items online when using public WiFi! Cybercriminals love to eavesdrop on unsecured connections and will happily steal your information. To prevent this, use a VPN (virtual private network) which encrypts your data. Even then, be sure you are on a secure, reputable site and keep the personal information you put into the forms to a minimum.

Online Shopping

No crowds. No lines. No traffic or busy parking lots. Just you, your computer, and a bunch of cybercriminals. The convenience of shopping on the internet obviously comes with risks. But savvy shoppers know how to identify threats and how to avoid them.

A SAVVY SHOPPER ALWAYS VERIFIES THE LEGITIMACY OF A WEBSITE. Scammers create bogus sites intended to steal information or sell knockoff, inferior products. You can avoid this by double-checking the URL and making sure you have a secure connection (https). Look for the green padlock!

A SAVVY SHOPPER KNOWS WHEN A DEAL IS TOO GOOD TO BE TRUE. An 80-inch TV shouldn't be priced like an eight-inch tablet. If you find a deal selling something for a price that doesn't make sense, chances are it's a scam. Be especially suspicious if the phishy deal ends up in your inbox (versus finding it while shopping). In other words, think before you click!

A SAVVY SHOPPER GOES INCOGNITO. Ever notice how a product you searched for ends up in the advertisements you see on various websites? It's called *targeted advertising*, which is made possible by cookies. You can eliminate it by shopping with your browser in privacy or incognito mode, or use an alternative web browser that doesn't store or track information.

A SAVVY SHOPPER USES STRONG PASSWORDS AND KNOWS THAT LESS IS MORE. When setting up online accounts to make purchases, it's vital that you use a strong, unique password, and never give out more information than needed. No online retailer needs your national ID number, for example. Only provide the minimum amount of data necessary to complete your transactions!

Gift Card Scams

Gift cards are a great way of saying "I don't know what to give you this year, so here's some money to get exactly what you'd like!" Just know there are a number of scams to be concerned with when purchasing gift cards. Avoid those reseller sites that offer cards for less than the original value. While it's a great way to save money, there is no guarantee that you'll get what you paid for. **Generally, to circumvent getting scammed or inadvertently giving a bogus gift, buy online gift cards from reputable sellers like Amazon, Walmart, Best Buy, etc.** And if you decide to buy a physical gift card, read the fine print. Some cards have a shelf life and usage fees, neither of which make for great gifts.