Mason-NSF Local Government Cybersecurity Partnership Education Series

Personal Cybersecurity Advice from a Local Government CISO

Introduction

How to communicate cybersecurity best practices effectively to users has long been one of modern CISO's (Chief Information Security Officer's) top challenges. The situation is especially dire for CISOs of small local governments, who usually face an extremely tight budget, small staff, absence of established policies and regulations, a workforce that lacks security awareness exacerbated by rapidly changing technology and resists to change, and a management that's usually burdened with other business priorities. What's worse - cyber criminals have increasingly targeting local governments. The recent ransom attack of the City of Atlanta highlights the urgency of the situation.

User mistake or negligence continue to be one of the most common denominators behind an attack. "Non-tech personnels in particular are targeted by criminals and nation hackers. To prepare and educate these users would be an extremely powerful weapon and deterrent against common security attacks that utilize human intelligence factors", said Mr. Dave Jordan, former CISO of Arlington County, Virginia, who in his 20 year tenure as the security chief, has developed a communicative channel and style that are not only impactful, but also easy to follow. Dave's communications took in dynamic forms, from direct emails to web posts, from new employee orientation and annual trainings to various speaking engagements. Dave communicated new policies and best practices, introduced new technologies, raised security concerns and precautions, and delivered timely security advice. One of the legacies Dave would like to leave behind at his recent retirement is the wider adoption of effective communication methods among local CISOs.

This pamphlet reflects a small selection of the messages Dave drafted or cited during his tenure as Arlington's CISO, with the purpose of showcasing how a veteran CISO conducts his daily communications. For the cited

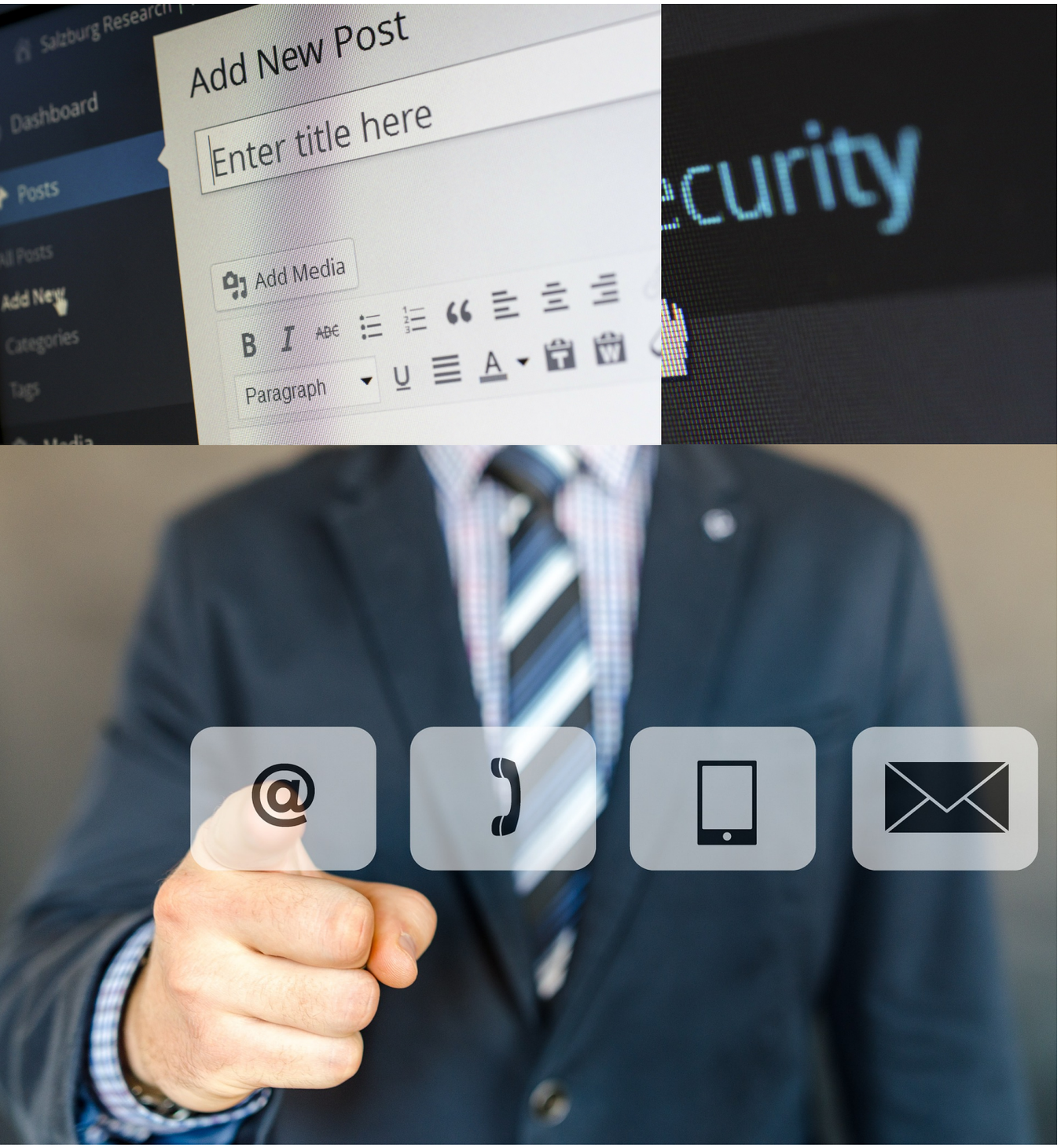
messages, Dave advised to “advertise the content in a timely manner, with a catchphrase and graphic on internal homepage with a link to the actual content. Sometimes compress the content to what is most relevant to the employees”. Of course, doing this requires the CISO to be well versed on latest incidents and trends. Dave wishes all CISOs master the art of effective communications and build the bridge critical in connecting user experience and security awareness.

This pamphlet was published as part of a NSF funded research project (Award #1623653), *City and County Cross Jurisdiction Cybersecurity Collaboration Capacity Building*. The purpose of the project is to develop training materials that focus on building stronger local cybersecurity capacity through partnerships.

This pamphlet is also a recognition of the tremendous contribution Dave has provided as an active advocate in enhancing local cybersecurity education and partnership and an adamant support of George Mason’s cybersecurity outreach efforts.

Please address any comments and questions to:
Dr. J.P. Auffret
jauffret@gmu.edu

Table of Contents:



Phishing Attacks - Suspicious Emails

By Dave Jordan

As you may have heard Phishing attacks are increasingly targeting local governments. The City of Atlanta, GA was the most recent victim. Phishing emails are nothing new, yet they remain one of the most alarming things to look out for online. These emails look very real, which can easily trick those not well aware. To lessen chances of falling victim to such schemes, it always pays to double check the sender of the email and the URLs that are being opened, as these usually point out if a message is indeed coming from genuine sources (friends, family, work contacts).

Please be vigilant:

· Do not open any unexpected or suspicious emails from unknown sources, exercise extreme caution with links and attachments!

· Browse very cautiously, do not visit unknown sites!

· Use the search window in the browser when typing in URLs and save your frequently used links to avoid mistyping LINKs as criminals are now setting up malware in frequently mistyped links

· Configure your Outlook toolbar (if available) with the new 'Suspect Email' button which will automatically delete suspect email from your inbox and forward it to IT Security Operations for analysis.

· Visit security articles frequently to stay well informed of recent cyber threats.

See suspect email say something:

If you receive a suspect email from an unknown sender or a sender you know that is asking you to open an attachment or click on a link regarding content that is unfamiliar to you or odd coming from your known sender then the chances are very high that this is a hoax email and most likely contains dangerous malware. DO NOT OPEN ATTACHMENTS OR CLICK on any links posted in the content of the message.

These types of email are a flavor of Social Engineering. When you are the target we call these emails a Phishing Attack; where the goal is to get you to click on an attachment or click on a link that will infect your PC with malware that can encrypt your data so the attacker can attempt to extort ransom from you or install malware that will capture your email, gain access to your data stores and or steal other sensitive information.

When you receive this type of suspect email you have options:

You can drag and drop the suspect email into a new email that you will send to IT help desk. In the new message content, please state that this email appears to be suspect and may contain malware.

You can simply delete the unwanted email (not preferred because security engineering uses your inputs to alert other recipients and block bad links contained in the suspect email).

We Will Never Do This

By Dave Jordan

Only Scammers will ask for your password!

There is an ongoing scam that all County employees should be aware of and protect themselves against.

The Help Desk / Service Desk Call Scam is a common scam where criminals from outside the U.S. use call centers to cold call victims. Most callers are able to hide their identities and locations by utilizing voice over Internet protocol (VOIP), or spoofing the phone numbers so that they appear to be coming from inside the US.

While there are variations to this scam, most follow a similar script where a caller will claim to work on behalf of a well-known software company (usually Microsoft or Windows and now the County's DTS Help Desk) and falsely inform the victim that their computer is either sending out error messages, attacking another computer, or exhibiting behaviors indicative of viruses, and that only they can repair the problem. When a victim is convinced that the situation is real, the scammers will gain remote access to the victim's computer; instruct them to download a software package (at work scenario that may enable them to breach the Enterprise network); or ask for the victim's financial information to charge for the services provided (in the case of a home user). This year some of these criminals after they acquire control of the user's PC will encrypt the data stored both in the PC's "C" drive and the Enterprise shared drives (U, M, L, W) and hold the data for ransom.

The latest scam asks victims to turn off their monitor, usually after gaining remote access to the computer. Be aware that this is a likely indicator of financial fraud, as the caller may be accessing bank accounts and transferring funds without the victim seeing. This could also allow the caller to access other sensitive information or make changes to the network while the victim is unaware. Possible results of the victim falling prey to the caller's instructions include: installation of malware, system compromise, and financial fraud. At this time DTS is monitoring these scams.

If you receive a suspicious call that follows the above patterns, please capture as much data as possible about exactly how the incident unfolded (Example: you were surfing the Internet and received a message that your PC was infected, the screen froze on the alert message or you received a call to your desk phone). Forward this information to the Center for Internet Security (CIS) at IIC@cisecurity.org. CIS does not need victim information, just a narrative, their area code and the next three numbers of the telephone number, city/state information, and the date of the incident. CIS hopes to aggregate this data nationwide and analyze such events to determine any geographical trends in order to better anticipate these scams and provide detailed situational awareness to potential victims.

Lastly, Service Desk personnel will never ask you for your user account or password information via email or by phone. Calls to you from the Service Desk should display a county four-digit number. A call from the Service Desk can always be returned by calling an extension.

Sun, Sand, and Cybersecurity Tips for Vacationers

Source: MS-ISAC

School's out and the beach and mountains are calling. It is that time of the year when so many of us pack our bags and hit the open road or head to the airport for a well-earned vacation. We may be ready to take a break from our normal lives, but we still need to be cyber secure while we are enjoying our time off! In this month's edition, we will explore some ways to be safe and smart with our devices, Internet usage, and social media while out traveling on vacation.

Stop-Think-Share

Always be careful about how much you post on social media about your vacations before and during your travels. Criminals can and do watch online posts to find people that are on vacation because that means you have left your home unattended.

Before "checking in" to a location on a social network, consider what else you are sharing – like the information that you aren't home. Consider skipping the "check in" and making your vacation posts after you have gotten back. This is another way people can see you aren't home. Perhaps this will have the double benefit of letting you take the time to choose only the best photos to post after your trip is over! At the very least, consider using privacy settings that only let friends see your posts.

Additionally, consider turning off GPS and auto-tagging/auto-check in features, if you have them enabled.

Disable WiFi auto-connect services

Some devices have an auto-connect feature that will search for and automatically connect to available and accessible WiFi networks without your interaction. This can allow your device to automatically connect to an unencrypted, public WiFi network, or even one that was set up by a malicious actor to eavesdrop on your browsing and connection activity.

If you want to connect to a store or hotel's network, check with an employee to see what the correct network is called, and see if they can provide a network password for a more secure, encrypted network. Always use a secure, encrypted network that requires login credentials if you have the option. In the event that isn't an option, and you can use your phone as a WiFi hotspot, use that instead to get a more secure connection for another device that can't make direct use of the cellular network's connection.

Additionally, make sure you do not choose to "remember this network" or "join this network automatically" once you have settled on a more trusted network for use during your vacation. If you have these settings switched on for a very generically named network, your device may connect you to a less secure one that happens to have the same name. Even if you have this turned off, there's another setting that will automatically connect you to a network you have joined before, which can be a problem since your device doesn't know the difference between your coffee shop's "Guest" network and a malicious "Guest" network. Turn these settings off so you don't automatically connect, and choose to connect only to more trusted, safer WiFi networks.

Keep your devices close, and keep them locked when not in use!

Whether it's your laptop, tablet, or smartphone, be sure to keep your device on you or with someone you trust. Never leave a device unattended in an airport, train station, restaurant, hotel lobby or anywhere else in public while traveling. There is a common scam that targets people who leave devices sitting next to them. In this scam, another traveler will approach you and ask for help and then lay a newspaper or map down over your device. While you're distracted answering their question, they are picking up and pocketing your device under the cover of the newspaper or map!

Set a strong password: Use at least 8 characters in upper and lower case, numbers, and symbols

Set a strong pattern lock: Use at least 7 points and double it back over itself with at least 2 turns

Additionally, keep your device locked using a password, pin, pattern, or fingerprint lock when you are not actively using it.

Cyber Tips for Online Shopping

Source: MS-ISAC

Online shopping can be a great solution, allowing you to find the perfect product or gift and saving time, but it can also end with identity theft, malware, and other cyber unpleasantness. Rather than letting it ruin your credit and steal your financial resources, you can take a few simple security precautions to help reduce the chances of being a cyber victim.

When purchasing online this holiday season - and all year long - keep these tips in mind to help minimize your risk:

1. **Do not use public computers or public wireless Internet access for your online shopping.** Public computers and wireless networks may contain viruses and other malware that steal your information, which can lead to identity theft and financial fraud.

2. **Secure your computer and mobile devices.** Be sure to keep the operating system, software, and/or apps updated/patched on all of your computers and mobile devices. Use up-to-date antivirus protection and make sure it is receiving updates.

3. **Use strong passwords.** The use of strong, unique passwords is one of the simples and most important steps to take in securing your devices, computers, and online accounts. If you need to create an account wit the merchant, be sure to use a strong, unique password, Always use more than ten characters

4. **Know your online shopping merchants.** Limit your online shopping to merchants you know and trust. If you have questions about merchant, check with the Better Business Bureau of the Federal Trade Commission. Confirm the online seller's physical address, where available, an phone number in case you have questions or problems. Do not create an online account with a merchant your trust.

5. **Pay online with one credit card.** A safer way to shop on the internet is to pay with a credit card rather than debit card. Debit cards do not have the same consumer protections as credit cards. Credit cards are protected by the Fair Credit Billing Act and may limit your liability if your information was stolen or used improperly. BY using one credit cared, with a lower balance, for all your online shopping you also limit the potential for financial fraud to affect all of your accounts. Always check your statements regularly and carefully, though.

6. **Look for "https" in the Internet address (URL) when making an online purchase.** The "s" in "https" stand for "secure" and indicates that communication with webpages is encrypted. This helps to ensure your information is transmitted safely to the merchant and no one can spy on it. Alternatively, look for the lock symbol (it's sometimes green) in the Internet address bar.

7. **Do not respond to pop-ups.** When a window pops up promising you cash or gift cards for answering a question or taking a survey, close it by pressing Control+F4 on a Windows computer and Command + W on a Mac. These could be social engineering attempts designed to convince you to open malware or click on a malicious link.

8. **Do not auto-save your personal information.** When purchasing online, you may be given the option to save your personal information online for future use. Consider if the convenience I really worth the risk. The convenience of not having to reenter the information is insignificant compared to the significant amount of time you'll spend trying to repair the loss of your stolen personal information.

9. **Use common sense to avoid scams.** Don't give out your personal or financial information via email or text. Information on many current scams can be founds on the website of the Internet Crime Complaint Center: https:www.ic3.gov/default.aspx and the Federal Trade Commission: https://www.consumer.ftc.gov/features/scam-alerts

10. **Review privacy policies.** Review the privacy policy for the website/merchant you are visiting. Know what information the merchant is collecting about you, how it will be used and if it will be shared with others.

What to do if you encounter problems with an online shopping site:

Contact the seller or the site operator directly to resolve any issues. You may also contact the following:

- Your state's Attorney General"s Office or Consumer Protection Agency

- The Better Business Bureau - www.bbb.org

- The Federal Trade Commission - https://www.ftccomplaintassistant.gov/#crnt&panel1-1

Reference provided by:

MS-ISAC Multi-State Information Sharing & Analysis Center™

STOP | THINK CONNECT™

Connected Home Security Checklist Tool Now Available

Source: Consumer Tech Association

The Consumer Technology Association (CTA)™ is now offering installers of smart home technology products a new security checklist for internet-connected devices. The Connected Home Security Checklist Tool, based on CTA's Device Security Best Practices white paper, details security protocols for installing and configuring products to better protect consumers and their smart home devices from unwanted malware or hackers. This tool is available free to CTA members.

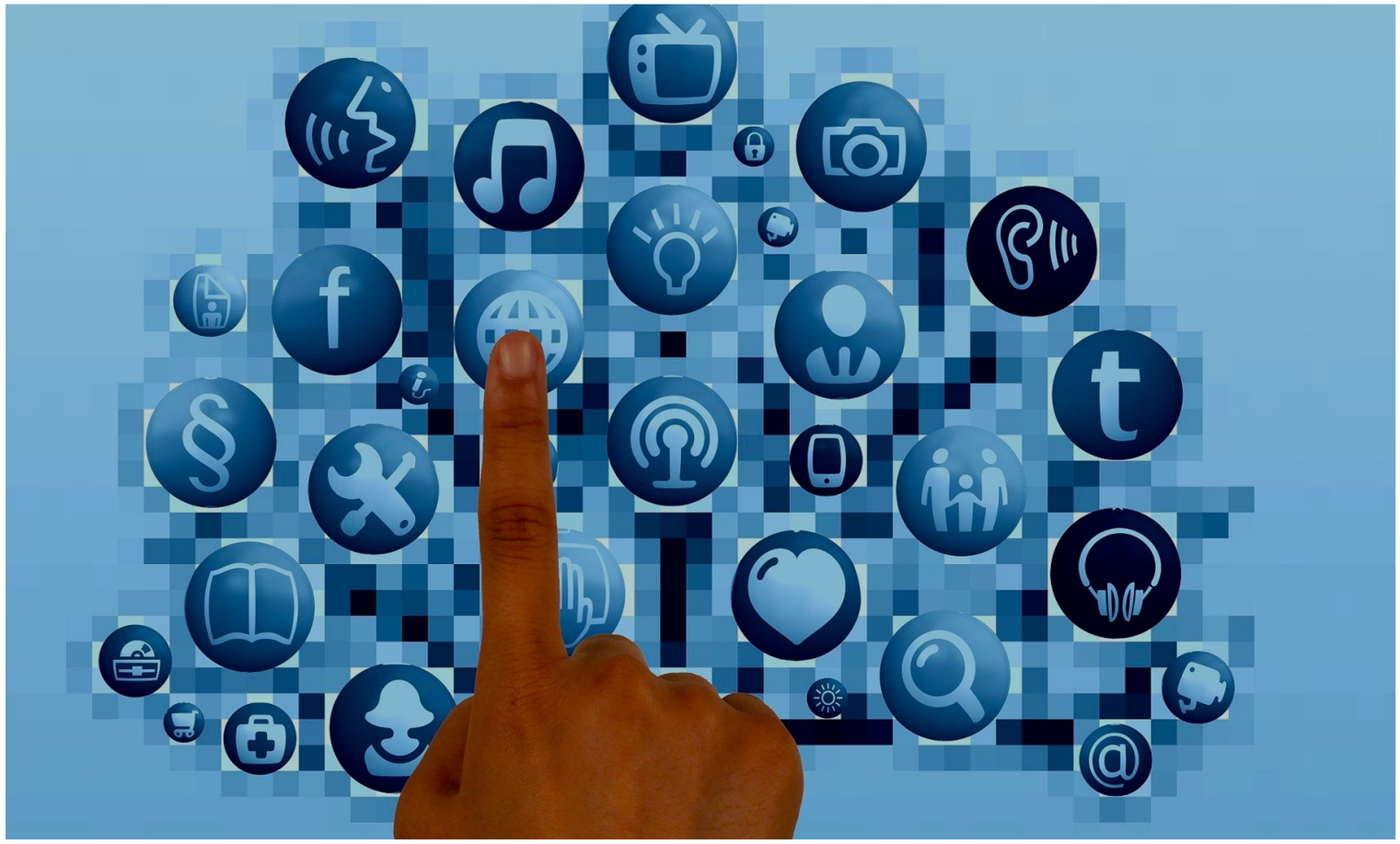
Cyber Spring Cleaning

Source: MS-ISAC

Spring cleaning is almost a rite of passage. With it we celebrate the renewal of life that occurs in nature each spring and eagerly await the exciting fun of summer. Traditionally, spring cleaning means cracking our windows and dusting, mopping, and vacuuming, but this year consider taking a few minutes to spring clean your digital life. Here are a few tips for home users for refreshing, renewing, and reinvigorating your cyber life.

Online Accounts

Just like your home, your online accounts can collect clutter and occasionally need a few minutes of care. Start by considering what accounts you have online for both work and home. Chances are your accounts include email, social networks, clubs and organizations, shopping websites, cloud storage accounts, and others. Do you need them all? Is there information in those accounts that isn't needed anymore, such as credit cards saved in your accounts with shops and old documents on cloud storage accounts? Are there accounts that you don't use anymore and can close, like that old email account you never check? Are you using the same password across any of these accounts that you could easily make unique and more secure?



Email Accounts

Speaking of email, is there information in your accounts that you can archive or delete? Many email providers have limits on mailbox sizes, and for security reasons it's always smart to limit what is available through your email account. On a side note, how many emails are in your inbox – are there any you can file into folders or delete? And when was the last time you cleared out your deleted items or trash folder? Can you set a rule that will automatically empty your deleted items or trash folder on a regular basis? Unsubscribe to recurring emails that no longer interest you.

Social Media

Just like everything else, it's a good idea to spring clean your social media accounts by taking a few minutes to review your security settings, friends and connections, and posts to make sure you're still comfortable with them. Is the information on your social networking and job websites, including Facebook, Twitter, Instagram, and LinkedIn, current? Do your security settings ensure that only the authorized individuals can view what you post? Do you still use or need all of the social media sites you are registered to?

Devices

Smartphones, tablets, laptops, and computers make our lives so much easier and here's your chance to ensure that doesn't change! Delete unused apps and clear out any downloads you aren't using any more. Make sure your device requires a password, pin, or fingerprint to log-in. Check for old files that can be archived or deleted. (Don't forget to empty the recycling/trash bin Then make sure your device's security software is working properly (you do have antivirus installed, right?) and all software is patched and set to auto-update

Web Browser Settings

Web browsers need a bit of care, just like other software. Many browsers can store your passwords or autofill settings, but over time the data stored by the browser can accumulate, and this isn't a secure place to store your passwords. So take a few minutes to check your browser settings, clear out old data, and ensure your browser's security settings are still keeping you safe. In particular, make sure that autofill doesn't contain sensitive information and that you don't store your passwords in your browser. Do you need all of the browsers on your system?

Home Networks

Take another moment to look at what is on your home network and how you're connecting to the Internet. Make sure your home router is secured with a complex and unique password and that it's broadcast name doesn't identify it as belonging to you. Additionally, setting up your wireless router to use a current encryption standard like WPA2 will greatly strengthen your home network security. This would also be a good chance to see if there are additional security features you can turn on or install, such as firewalls or antivirus software.

Back Things Up

Whether you save your files to CDs or DVDs, a cloud back-up service, or an external hard drive, spring cleaning is a good opportunity to make sure you have a complete backup of important files. No matter how you're saving those files, make sure you're saving the right files and that you can restore everything from your backup, since a backup that you can't restore from isn't useful at all!

Take Out the Trash

Last, but certainly not least, take out the trash. Literally. Are there old devices in your house or office that should be recycled? If so, many towns and stores support eCycling initiatives and will help you properly dispose of them. Just make sure to remove and shred/destroy hard drives and other components that may contain sensitive data!

By taking a few minutes to include these digital areas of focus in your spring cleaning plans, you can ensure that your data and devices are that much safer.

Content provided by cybersecurity leadership mentor and the First Arlington County CISO, Dave Jordan

Back to School in the Digital Age: Cyberbullying

Source: Homeland Security Digital Library

It's that time of year…the kids are back to school, and with that season comes a whole host of new experiences: new friends, new classes, new teachers, and for some, new harassment. One of the most common forms of harassment in the 21st century is cyberbullying. The Federal government website stopbullying.gov offers resources addressing "why cyberbullying is different from traditional bullying, what you can do to prevent it, and how you can report it when it happens," and provides the following definition:

Cyberbullying is bullying that takes place using electronic technology. Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Cyberbullying has been identified by the U.S. Department of Homeland Security as a threat to homeland security, and though cyberbullying is often thought of as a school-aged problem, it is far from limited to that demographic: public figures experience cyberbullying, as do those in the workplace and the wider community. However, given the time of year, the Homeland Security Digital Library wanted to highlight some helpful resources in its collection that address this major issue facing children and adults alike:

Indicators of School Crime and Safety: 2017
Bureau of Justice Statistics

Electronic Harassment: Concept Map and Definition
National Criminal Justice Reference Service

State Cyberbullying Laws A Brief Review of State Cyberbullying Laws and Policies
Cyberbullying Research Center

The Homeland Security Digital Library is constantly adding new resources, so keep checking back for the latest content on cyberbullying. For more documents like the ones mentioned here, check out the Homeland Security Digital Library's information on Cyberbullying, and its Featured Topics on School Violence and Cyber Policy.

Fraudsters Capitalize on Natural Disaster

Source: FBI

In the aftermath of Hurricanes Harvey and Irma, the FBI reminded the public there was the potential for fraud. The FBI's Internet Crime Complaint Center (IC3) received indications that fraudsters used e-mail and social-networking sites, including job search engines, to facilitate fraudulent activities.

Disasters such as Hurricanes Harvey and Irma prompt fraudsters to solicit contributions purportedly for a charitable organization or a good cause. Fraudsters may also attempt to capitalize on the misfortune of victims by advertising false temporary housing ads which victims send money to the subject in order to have property keys mailed to them. Victims may also receive information regarding false job opportunities in which victims will receive a fraudulent check they are expected to deposit and then distribute to various accounts. Therefore, before making a donation of any kind or supplying payment for any type of service related to victim relief, consumers should adhere to certain guidelines, to include the following:

- Do not respond to unsolicited (spam) e-mails.
- Be skeptical of individuals representing themselves over e-mail as officials soliciting for donations.
- Do not click on links within an unsolicited e-mail.
- Be cautious of e-mails claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders.
- To ensure contributions are received and used for the intended purposes, make contributions directly to known organizations rather than relying on others to make the donation on your behalf.
- Validate the legitimacy of the non-profit status of the organization by directly accessing the recognized charity or aid organization's website rather than following an alleged link to the site.
- Attempt to verify the legitimacy of the non-profit status of the organization by using various Internet-based resources, which may also assist in confirming the actual existence of the organization.
- Do not provide personal or financial information to anyone who solicits contributions; providing such information may compromise your identity and make you vulnerable to identity theft.
- Be cautious of e-mails claiming to offer employment for which you did not expressly apply.
- Thoroughly research housing ads prior to sending money to a potential landlord.

If you believe you have been a victim of disaster-related fraud, contact the National Center for Disaster Fraud by telephone at (866) 720-5721, by fax at (255) 334-4707, or by e-mail at disaster@leo.gov. You can also report suspicious e-mail solicitations or fraudulent websites to the Internet Crime Complaint Center at www.ic3.gov.

National Center for Disaster Fraud (NCDF) was originally established by the Department of Justice to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina. Its mission has expanded to include suspected fraud from any natural or man-made disaster. More than 20 federal agencies, including the FBI, participate in the NCDF, allowing it to act as a centralized clearinghouse of information related to relief of fraud.

Keep Our Elections Secure

Source: MS-ISAC

The MS-ISAC (Multi-State Information Sharing and Analysis Center) strongly encourages all members to take steps to secure their election-related systems against potential attack vectors, included in the attachment. Members should also review the MS-ISAC Security Primers regarding potential attack types and linked below.

- If you experience or become aware of any malicious or suspicious cyber activity, contact the MS-ISAC SOC at soc@msisac.org or call 1-877-787-4722. MS-ISAC performs a variety of free incident response services including log analysis, malware analysis, computer forensics, development of a mitigation and recovery strategy as well as network and application vulnerability scanning.
- Ensure that all systems are patched and up-to-date.
- Ensure all websites and databases are protected against SQLi attacks. Further information on SQLi attacks is available at: https://www.cisecurity.org/white-papers/technical-white-paper-sql-injection/ and https://www.cisecurity.org/white-papers/sqli/.
- Ensure you have a plan in place to identify and mitigate incoming DDoS attacks. The MS-ISAC Guide to DDoS attacks is available at: https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/.
- Ensure all websites are protected against XSS. Information on XSS attacks is available at: https://www.cisecurity.org/white-papers/cross-site-scripting-xss/.
- Consider implementing a web application firewall (WAF).
- Ensure the use of cybersecurity best practices to secure your networks, websites, and devices, including practices such as:
  - regularly scheduled vulnerability scans of all domains and all networks, systems, and devices, especially including those that are Internet-facing;
  - conducting penetration tests after system changes, and ensuring all changes are documented;
  - implement, monitor, and store logging for at least 90 days to identify unusual or unauthorized modifications and traffic, and to ensure that only authorized users are accessing resources; and
  - ensure backups are conducted daily and stored offsite and offline.

Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children

Source: FBI

The FBI encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments. Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.

Why Does This Matter to My Family?

The features and functions of different toys vary widely. In some cases, toys with microphones could record and collect conversations within earshot of the device. Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. The collection of a child's personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety. Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/IPs. The exposure of such information could create opportunities for child identity fraud. Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks.

Consumers should examine toy company user agreement disclosures and privacy practices, and should know where their family's personal data is sent and stored, including if it's sent to third-party services. Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use. Consumers should perform online research of these products for any known issues that have been identified by security researchers or in consumer reports.

What Makes Internet-Connected Toys Vulnerable?

Data collected from interactions or conversations between children and toys are typically sent and stored by the manufacturer or developer via server or cloud service. In some cases, it is also collected by third-party companies who manage the voice recognition software used in the toys. Voice recordings, toy Web application (parent app) passwords, home addresses, Wi-Fi information, or sensitive personal data could be exposed if the security of the data is not sufficiently protected with the proper use of digital certificates and encryption when it is being transmitted or stored.

Smart toys generally connect to the Internet either:

Directly, through Wi-Fi to an Internet-connected wireless access point; or

Indirectly, via Bluetooth to an Android or iOS device that is connected to the Internet.

The cyber security measures used in the toy, the toy's partner applications, and the Wi-Fi network on which the toy connects directly impacts the overall user security.

Communications connections where data is encrypted between the toy, Wi-Fi access points, and Internet servers that store data or interact with the toy are crucial to mitigate the risk of hackers exploiting the toy or possibly eavesdropping on conversations/audio messages. Bluetooth-connected toys that do not have authentication requirements (such as PINs or passwords) when pairing with the mobile devices could pose a risk for unauthorized access to the toy and allow communications with a child user. It could also be possible for unauthorized users to remotely gain access to the toy if the security measures used for these connections are insufficient or the device is compromised.

What Consumer Laws Exist to Protect My Children?

The Children's Online Privacy Protection Act (COPPA) imposes requirements on Web site and online service operators directed to children under the age of 13 and on operators of other sites and services who knowingly collect personal online information on children under 13 (for further details on COPPA and protecting children online, refer to https://www.consumer.ftc.gov/topics/protecting-kids-online). On 21 June 2017, the Federal Trade Commission (FTC) updated its guidance for companies required to comply with COPPA to ensure those companies implement key protections with respect to Internet-connected toys and associated services, to include the use of mobile apps, Internet-enabled location-based services, and voice-over IP services (https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business). In addition, a manufacturer's failure to implement reasonable security measures for data collected by its Internet-connected toys could subject that company to an FTC enforcement action under Section 5(a) of the FTC Act, which prohibits unfair or deceptive practices in the marketplace. The FBI is encouraging all consumers to research areas and circumstances concerning the toys and Web services where laws may or may not provide coverage.

What Should I Do?

- The FBI encourages consumers to consider the following recommendations, at a minimum, prior to using Internet-connected toys.
  - Research for any known reported security issues using online resources from sites that conduct cyber security research, consumer product reviews, and child and consumer advocacy
  - Only connect and use toys in environments with trusted and secured Wi-Fi Internet access
  - Research the toy's Internet and device connection security measures
  - Use authentication when pairing the device with Bluetooth (via PIN code or password)
  - Use encryption when transmitting data from the toy to the Wi-Fi access point and to the server or cloud
  - Research if your toys can receive firmware and/or software updates and security patches
  - If they can, ensure your toys are running on the most updated versions and any available patches are implemented
  - Research where user data is stored – with the company, third party services, or both – and whether any publicly available reporting exists on their reputation and posture for cyber security
  - Carefully read disclosures and privacy policies (from company and any third parties) and consider the following:
    - If the company is victimized by a cyber-attack and your data may have been exposed, will the company notify you?
    - If vulnerabilities to the toy are discovered, will the company notify you?
    - Where is your data being stored?

    - Who has access to your data?
    - If changes are made to the disclosure and privacy policies, will the company notify you?
    - Is the company contact information openly available in case you have questions or concerns?
- Closely monitor children's activity with the toys (such as conversations and voice recordings) through the toy's partner parent application, if such features are available
- Ensure the toy is turned off, particularly those with microphones and cameras, when not in use
- Use strong and unique login passwords when creating user accounts (e.g., lower and upper case letters, numbers, and special characters)
- Provide only what is minimally required when inputting information for user accounts (e.g., some services offer additional features if birthdays or information on a child's preferences are provided)

If you suspect your child's toy may have been compromised, file a complaint with the Internet Crime Complaint Center, at www.IC3.gov.