Summary

**Island Hopping: Far From Paradise** -
Learn about this term’s meaning in the information security field.

**Sneaky Phishing Tactics: Conversation Hijacking** -
We discuss this emerging tactic in action and its warning signs.

**Cyber Espionage Leaves Organizations Shaken, Not Stirred** -
A look at the challenges cyber espionage campaigns can pose.

**Managing Browser Password Managers** -
We discuss current security considerations associated with password managers and provide some hygiene tips for safer use.

**Handle with Scare: A Look at Scareware Tactics** -
Learn how to detect and avoid this malware type.

**Human Trafficking and the Use of Online Platforms** -
We provide guidance on security measures to consider to help avoid human trafficking in action on social media.

**Beware of Fleeceware** -
Certain apps we install may be tacking on extra expenses. We examine how to identify and get rid of these costly programs.

**Frankenstein Identities: The Rise of Synthetic Identity Theft** -
A description of synthetic identity theft and ways to protect yourself from it.

About The Beacon

*The Beacon* is the Florida Fusion Center’s cyber and critical infrastructure publication, produced by the Florida Infrastructure Protection Center (FIPC). Designed to highlight information of interest, *The Beacon* features events and trends that occur in Florida or specifically affect Florida.

The Florida Infrastructure Protection Center was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters.

Contact the FIPC
Phone: (850) 410-7645
Email: FIPC@fdle.state.fl.us
National Cyber Security Awareness Month 2020

October is National Cyber Security Awareness Month. This year’s theme is “Do Your Part. #BeCyberSmart” and focuses on the roles that each of us plays in keeping our personal and family networks, as well as our organizations’ and businesses’ networks, secure. Each week throughout October, there is a different theme identified by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance. In 2020, these themes will focus on the following topic areas:

**WEEK 1:**

**If You Connect It, Protect It**

Many of us use multiple internet-connected devices every day. These devices can contain important sensitive information that we want to keep protected. Securing each of these devices is an important step in protecting them from cyber actors seeking to exploit them.

**WEEK 2:**

**Securing Devices at Home and Work**

The COVID-19 pandemic spurred a major increase in the amount of people working from home. This unprecedented shift has introduced a number of challenges for both individuals and employers as we all adapt to new procedures, vulnerabilities, and threats.

**WEEK 3:**

**Securing Inter-Connected Devices in Healthcare**

The healthcare industry remains a vital component of our society. This industry increasingly relies on internet-connected devices to efficiently provide medical services. Securing these devices is essential to maintaining normal operations while also keeping patient health data protected.

**WEEK 4:**

**The Future of Connected Devices**

Connected devices help to link us to larger groups and communities via the internet. As connected devices continue to evolve, so do their threats. To prevent these threats from spreading and impacting others, each of us is responsible for doing our part by safeguarding our own connected devices.

If you missed this year’s topics, it’s not too late to learn more about cyber security! Secure Florida analysts continue to follow and provide information on cyber trends and safety tips. Visit [https://secureflorida.org](https://secureflorida.org) for more information on how you can protect your devices and networks. For more information on National Cyber Security Awareness Month, visit [https://www.cisa.gov/national-cyber-security-awareness-month](https://www.cisa.gov/national-cyber-security-awareness-month).
Cyber Threats

Island Hopping: Far from Paradise

The term “island hopping” originated during World War II as a tactic used by the U.S. to overtake smaller islands with fewer defenses in the Pacific as part of a broader attack strategy. The cybersecurity field has adopted the term to describe an indirect method used by hackers to infiltrate a target. Island hopping occurs when hackers attack smaller companies associated with their target and use them as footholds until they can reach the desired organization. While this method of attack isn’t new, island hopping has continued to grow in popularity and poses a serious threat to businesses’ and organizations’ network security.

Island hopping can be broken into three categories based on the attack vector: network-based, watering hole, and reverse business email compromise (BEC).

1. Network-based island hopping is the most frequently used and involves infiltrating one network to use as a bridge to get to the next.

2. The watering hole tactic is performed when attackers identify a website with vulnerabilities that is frequented by the target’s customers and employees. The attacker then infects that website with malware that spreads onto the victims’ machines and transmits information back to the attackers.

3. The reverse BEC attack vector is used to hack the email server of the business to send out phishing emails or malware attacks to the organization and its members.

In 2013, the international retail store, Target, experienced a cyberattack as a result of island hopping that resulted in the exposure of the personal information of 41 million customers. In this attack, the hackers did not penetrate Target’s networks head on. Instead they went through a third-party vendor that provided heating and refrigeration to some Target stores. This vendor was reportedly first victimized by the banking trojan, Citadel, deployed via a phishing email. This malware allowed the hackers to steal login credentials from the vendor that could then be used to access Target’s internal network. In total, this cyberattack which was orchestrated by island hopping from a trusted third-party company, cost Target $202 million.

One of the first steps in preventing these attacks can be having discussions with companies that you perform business with and future vendors. See what cybersecurity measures they have implemented into their business and how well it collaborates with your own organization’s security posture. Organizations can further bolster their cybersecurity posture by instituting multi or two-
factor authentication. Weak or recycled passwords are almost effortless for hackers to crack.\(^{10}\) Also consider asking about their password update policy since weak or recycled passwords are easier for hackers to crack. Furthermore, it's important to frequently back up data and ensure that backups are accessible. In the event of a breach, these backups can be extremely valuable in getting operations up and running again.\(^{11}\) Island hopping attacks aren't likely to decrease anytime soon, but organizations can decrease their chances of falling victim by maintaining the best cybersecurity posture possible.

---

**Sneaky Phishing Tactics: Conversation Hijacking**

Many businesses regularly make large purchases and handle large sums of money as part of their daily responsibilities. Cyber criminals are aware of this and are always looking for ways to con these organizations to intercept these funds, often by stealing sensitive information or personal data in an effort to enact their scheme.

One of the most common methods used by these actors is phishing, which is the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email and the goal is to steal sensitive data, like credit card and login credentials, or to install malware on the victim's machine.\(^{1}\) The use of a specific type of phishing attack known as “conversation hijacking” is on the rise. According to the research done by Barracuda Networks, an analysis of approximately 500,000 monthly email attacks shows a 400% increase in these types of attacks. There were approximately 500 incidents in July 2019, but by November 2019, the total number had reached about 2,000.\(^{2}\)

Conversation hijacking attacks are similar to email phishing attacks in that the target will receive an email sent with malicious intent. However, conversation hijacking is more complex. This attack is carried out by infiltrating email exchanges between employees who often know and trust one another. Usually, the infiltration is made possible by credential theft. Then, the attacker can read and send emails as one of the employees in the conversation. Messages are typically carefully tailored to make them seem relevant to the email conversation with the goal of convincing the recipient to act on the malicious email request rendering the attack successful.\(^{3}\)

Researchers point out that these types of phishing attempts can take months to execute as the hacker waits for the right moment.\(^{4}\) Attackers can but aren't likely to use the compromised account to carry out the attack because the account owner could easily spot the malicious email in their outbox or sent folder. Instead, they may try to impersonate the compromised email account by mimicking that

---

3. [https://www.itpro.co.uk/cyber-attacks/33200/what-is-island-hopping](https://www.itpro.co.uk/cyber-attacks/33200/what-is-island-hopping)
5. [https://www.itpro.co.uk/cyber-attacks/33200/what-is-island-hopping](https://www.itpro.co.uk/cyber-attacks/33200/what-is-island-hopping)
11. [https://vpnpro.com/web/what-is-island-hopping/](https://vpnpro.com/web/what-is-island-hopping/)
account’s email address with slight changes. For example, a hacker may impersonate janedoe@business.com by using the email address janedoe@businesss.com. By adding an extra “s” to the end of “business” the hacker is able to use a new email domain to route emails.5

Although conversation hijacking was a small percentage of overall attacks for 2019, due to its hyper-personalized nature, the attacks can be extremely effective and may grow in popularity as some organizations have increased telework and, therefore, decrease face-to-face interactions between employees.

There are ways to mitigate the risk of conversation hijacking compromising your business. Users should pay attention to the email addresses from which they receive messages and be suspicious if domains slightly differ compared to what they’re used to seeing. Users should also be wary of sudden demands for payments or transfers. If there’s doubt about the origin of the request, users should contact the person requesting it, either in person, by phone or by starting a new email to their known address. In addition, organizations can protect their employees from these attacks by implementing two-factor authentication. Adding this extra layer can prevent further attacks even if log-in credentials are stolen.6 These measures can help in preventing cyber criminals from gaining a foothold in your organizational emails, but continuous education for employees on the cyber threats that are out there along with constant vigilance when opening email attachments and links can provide a more robust overall cyber posture for your organization.

2 https://smartermsp.com/conversation-hijacking-emerges-as-a-cybersecurity-threat/
3 https://www.em360tech.com/continuity/tech-news/opinion-piece/conversation-hijacking/
4 https://smartermsp.com/conversation-hijacking-emerges-as-a-cybersecurity-threat/
5 https://www.zdnet.com/article/beware-of-this-sneaky-phishing-technique-now-being-used-in-more-attacks/
6 Ibid.

Cyber Espionage Leaves Organizations Shaken, Not Stirred

Most cyber criminals are mainly interested in using illegal cyber means to obtain money. A subset of these actors, however, remain interested in trying to steal information to gain a strategic benefit. This is called cyber espionage, and it is mainly pursued by groups working for or affiliated with nation states, although former employees, competitors, and criminal groups have also been involved at a much smaller percentage.1 According to Verizon reporting, state-affiliated or nation state hacking groups were responsible for 96% of all reported cyber espionage data breaches in 2018.2 Several governments, including those of China, Russia, North Korea, and Iran, are widely believed to employ sophisticated, well-funded cyber groups to illicitly uncover information from Western governments, corporations, and non-governmental organizations, although other nations also operate or are developing cyber espionage capabilities that may also target Western organizations.3

Cyber espionage attackers mostly target the public sector, likely due to their desire to obtain sensitive, classified, or personal identifying information than can help them obtain their strategic objectives. While all other sectors were hit mainly by financially-motivated data breaches, more than half of public sector data breaches were motivated by espionage in 2018. Public sector targets
constituted the vast majority of reported cyber-espionage breaches during this same time period, which is consistent with previous years.4

Successful cyber espionage attacks against the public sector can potentially have massive ramifications. Chinese hackers are believed to be behind a 2015 data breach at the Office of Personnel Management (OPM), which resulted in up to 21 million U.S. citizens having their information compromised.5 Meanwhile, Russian hackers were reportedly behind hundreds of cyber-intrusions against U.S. public and private sector targets in 2016, with the aim of influencing that year’s general election.6 The private sector is not immune to espionage attacks either, as cyber-spies may target certain industries involved in technology or research that is attractive to the attacker. Theft of proprietary information by state actors motivated almost half of all reported data breaches in the manufacturing industry in 2017, and in 2020, China-backed threat actors have allegedly targeted the U.S. healthcare industry to steal sensitive COVID-19 related research.78 Victims of cyber-espionage may take longer to identify an attack occurred compared to victims of financially-motivated data breaches, as external fraud reporting can identify potential financial breaches quicker. In some instances, years can pass before espionage-related data breaches are detected.9

Cyber espionage presents unique threats to organizations, but often relies on familiar methods of delivery. Most cyber espionage attacks utilize phishing to trick individuals with privileged access into inadvertently installing malware or revealing credentials that can be used to access important information: a tactic also used by financially-motivated cyber attackers.10 11 Because of this, educating your organization on how to recognize, report, and mitigate phishing, as well as incorporating enhanced security measures such as two-factor authentication, can help decrease vulnerability to cyber espionage attacks. Recognizing and preventing insider threats is also important, as some cyber espionage breaches are also facilitated by insiders who deliberately misuse their accesses or credentials to steal or compromise important information. More information on preventing phishing compromises and insider threats can be found on the Cybersecurity and Infrastructure Security Agency (CISA) website.13 14

13 https://www.us-cert.gov/ncas/tips/ST04-014
14 https://www.cisa.gov/insider-threat-mitigation
Password managers are applications that allow users to store multiple user names and passwords in a centralized storage system. Several types of password managers are available for those seeking assistance storing unique, complex passwords. A quality password manager will typically incorporate both the ability to generate strong passwords for the user’s accounts and filling in encrypted passwords for the user when prompted.1 Today, users seeking to use a password manager have the option of using a third-party password manager application or using a password manager built into internet browsers that offer this function. These built-browser applications are a convenient mechanism for many, but users should thoroughly weigh the advantages and disadvantages of browser password management systems before using them.

There are a number of advantages to using built-in browser password managers. For example, if you visit your social media profile, your online bank account, and your favorite streaming service all in one sitting, your browser is able to not only remember the username and password for each of these, but it can input this information securely into the login pages of each. This makes signing in quick and easy. Additionally, many of these applications are able to generate complex and random passwords for users. This feature can help prevent users from creating passwords that are too simple and can prevent users from reusing the same password across multiple accounts.2 Furthermore, browser password managers are largely free with no subscription fees that may sometimes be required is other third-party password management applications.3

However, there are also disadvantages to using built-in browser passwords. Using password managers may present some security concerns for those using shared computers or in the event that a device is stolen. Individuals that have access to the same computer accounts may be able to access other users’ personal online accounts. The autofill feature of the browser password manager allows access to secure online accounts, where changes to those accounts can be made. For example, an autofill feature for an online bank account may allow an unauthorized user to easily sign in and transfer funds from one account to another. Users can avoid this by signing out of their computer and online accounts or locking the computer or other device when not in use.4 Users can also disable autofill features for certain websites and can also prevent login information from appearing on website login screens to prevent disclosure.
Learning that your computer has a virus or is infected with malware can be scary! Getting a message of a possible infection, may lead some to jump into action in an attempt to fix the problem by cleaning out whatever malicious software, or malware, is on their device. Cybercriminals constantly play off of this fear. One tactic that some cybercriminals have turned to is the use of scareware: malware advertised via pop-up ads as antivirus software.

Scareware works by popping up when a user visits a website and advertises itself as antivirus protection. The pop-up window may allege that the user’s device has a virus or even that it has multiple viruses. The pop-up may even claim to “scan” the user’s computer and show fake alerts claiming that the computer is infected with viruses. The ad will then offer fake antivirus protection to the user. The software may even be advertised as free. However, this fake software is not antivirus software and is usually some form of malware intended to steal user information, gain access to unauthorized users. Additionally, users who frequently switch between browsers on different devices may not find built-in password managers useful. Many of these types of password managers won’t work across different browsers so the user would be forced to input their login credentials into each site or browser’s password manager.

Moreover, many experts have made the case for simply using a third-party password manager app due to their ability to store more than just login credentials for online accounts. Some third-party apps are capable of also saving files and important documents. These apps serve as a one-stop-shop for saving your most valuable information in one location. Many third-party password manager apps also allow for quick and easy logging in to chosen sites by simply scanning a fingerprint or using a PIN. However, it is imperative that users store the master password for these managers in a secure location.

All in all, the best password management option is based on the amount of security needed and each user’s wants and needs. However, having complex passwords unique to each account is a key way to safeguard against unauthorized access to accounts and potential criminal activity. As such, users should ensure that their choice in password management strike a good balance between convenience and security.

Handle with Scare: A Look at Scareware Tactics

Learning that your computer has a virus or is infected with malware can be scary! Getting a message of a possible infection, may lead some to jump into action in an attempt to fix the problem by cleaning out whatever malicious software, or malware, is on their device. Cybercriminals constantly play off of this fear. One tactic that some cybercriminals have turned to is the use of scareware: malware advertised via pop-up ads as antivirus software.

Scareware works by popping up when a user visits a website and advertises itself as antivirus protection. The pop-up window may allege that the user’s device has a virus or even that it has multiple viruses. The pop-up may even claim to “scan” the user’s computer and show fake alerts claiming that the computer is infected with viruses. The ad will then offer fake antivirus protection to the user. The software may even be advertised as free. However, this fake software is not antivirus software and is usually some form of malware intended to steal user information, gain access to unauthorized users. Additionally, users who frequently switch between browsers on different devices may not find built-in password managers useful. Many of these types of password managers won’t work across different browsers so the user would be forced to input their login credentials into each site or browser’s password manager.

Moreover, many experts have made the case for simply using a third-party password manager app due to their ability to store more than just login credentials for online accounts. Some third-party apps are capable of also saving files and important documents. These apps serve as a one-stop-shop for saving your most valuable information in one location. Many third-party password manager apps also allow for quick and easy logging in to chosen sites by simply scanning a fingerprint or using a PIN. However, it is imperative that users store the master password for these managers in a secure location.

All in all, the best password management option is based on the amount of security needed and each user’s wants and needs. However, having complex passwords unique to each account is a key way to safeguard against unauthorized access to accounts and potential criminal activity. As such, users should ensure that their choice in password management strike a good balance between convenience and security.

---

1 https://gizmodo.com/is-your-browser-a-good-enough-password-manager-1844685005
3 https://www.zdnet.com/article/is-it-ok-to-use-your-browsers-built-in-password-manager/
5 https://www.howtogeek.com/447345/why-you-shouldnt-use-your-web-browsers-password-manager/
6 https://www.cnet.com/how-to/best-password-manager-to-use-for-2020-1password-last-password-more-compared/
user accounts, or monitor user activity. If a user inputs credit card information to pay for the scareware, the criminal actors behind this scam will have that user’s credit card information, which can be used to make unauthorized purchases.2

Scareware uses social engineering tactics to scare users into reacting quickly to try and rid their device of non-existent malware. These ads often include some indicators that they’re fraudulent – similar to phishing emails. These indicators include spelling or grammar errors, strange phrasing, and demands to act immediately. Many scareware ads also include a countdown to further scare users into acting quickly.4

Users can avoid falling for this scheme by following a few good cybersecurity habits. Keeping trusted antivirus software up to date can help prevent these types of ads from popping up. Be wary, some of these cybercriminals may try to make their scareware look legitimate by using the logos of well-known and trusted tech companies. Remember that only the antivirus software you have installed on your device should notify you of security issues.

Using a pop-up blocker can also prevent scareware notifications and other problematic ads from appearing in your browser. If an ad does appear, carefully exit the ad by clicking the “X” to close the window. Cybercriminals may try to make it difficult to exit out of these pop-ups by hiding the option to close the ad. If this is the case, remember that you can also remove the pop-up by closing the browser window or forcing your computer to shut down the browser application using the task manager or the proper force quit procedure for your machine.5 With the proper precautions, scareware is nothing to be scared of.

1 https://www.forcepoint.com/cyber-edu/scareware#:~:text=Scareware%20is%20a%20malware%20tactic,installing%20fake%20anti%2Dvirus%20software
2 https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html
4 https://www.pcmag.com/how-to/how-to-avoid-scareware
Human Trafficking and the Use of Online Platforms

Today, almost 80% of the U.S. population maintains some form of online presence on social media.¹ These platforms are great for connecting with others, sharing information, and for entertainment. However, these platforms can also be exploited by criminal actors. In recent years, many cases of human trafficking have been traced back to an initial contact via online platforms.² The number of websites and platforms that can be used for illicit activities, to include human trafficking,³ are limitless.⁴ Criminal actors may advertise and recruit victims using social media platforms, gaming applications, dating applications, video sharing sites, photo sharing applications, classified websites, and talent websites.⁵ These platforms number in the thousands, are ever-changing, and are likely to continue to be used for human trafficking purposes due to the sheer number of people using online platforms to communicate.

Traffickers are likely to contact victims under many different guises, to include building a relationship, offering a better life, or promising resources such as housing or a job offer.⁶ In some instances, traffickers may target specific people based on things they post online to include fear, loneliness, or those facing destabilization either from substance abuse or homelessness.⁷ For example, a trafficker may see someone post online that they’re short on money for bills, need a place to live, or looking for a relationship. They could then use the victim’s circumstances to begin online communications with them. Unsuspecting victims may engage in conversation with these individuals...
unaware of their nefarious intentions. Some victims are lured into trafficking with the false promise of a relationship, deceptive job recruitment ads specifically for modeling/talent jobs, and/or dealing with low self-esteem or family challenges.8 Other means of targeting victims online can involve stalking them, impersonating others, or sending threatening/harassing messages.9

Because online environments can be used by traffickers to prey on unsuspecting victims, vigilance when interacting with others online is important.10 The guidelines below can help in preventing online criminal actors from exploiting your personal information for nefarious purposes.

Refrain from sharing personal information online. Information like your full name, school or place of work, and address or phone number can be used by criminal actors.

• Never share pictures of yourself online that you wouldn't want anyone else to see or have in their possession.

• Set online profiles to private so only authorized people can see your information. Be aware of who you are communicating with and remember that not everyone has good intentions.

• For parents, it is important to stay aware of what websites and applications children use, what information children post online, and who they are communicating with.

The Secure Florida website has a host of up-to-date information on how to practice online safety for children, families, and those in workplace settings. If you believe illicit activity, such as human trafficking, is occurring online, you may report it to any of the below entities:

• local law enforcement agency;

• National Human Trafficking Hotline at 1-888-373-7888 or via text at 233733; or the

• Federal Bureau of Investigation Internet Crime Complaint Center at www.IC3.gov.

Human traffickers are known to prey on vulnerable victims online, engaging with
Beware of Fleeceware

Fleeceware is a relatively new term in cybersecurity used to describe applications that overcharge users for a function that is widely available for free or at a low-cost. The term was first coined by British security software and hardware company, Sophos, after they discovered a group of Android apps on Google's Play Store and later the Apple Store that served no purpose other than to overcharge users for simple functions such as a flashlight app or a QR code reader.

Fleeceware app developers often take advantage of unsuspecting users via the “free trial” business model. In these instances, users generally download and use the app at no charge but are required to sign up with payment information for a short free trial period. Unless the user uninstalls the app and notifies the app developer that they no longer wish to continue using the app, the app developer will charge the user excessive fees, sometimes hundreds of dollars, when the trial period ends.

The problem with fleeceware is that it does not engage in what is traditionally considered malicious activity. It simply takes advantage of loopholes in the app store policies. On both Android and iOS devices, the app stores generally allow app developers to define their own terms for trial periods. Taking this loophole into consideration, fleeceware app developers often don't define uninstalling the app as a way to cancel the trial period. Instead, they set complex terms of cancellation such as physically writing to the app developer to cancel the trial. Since many users skip reading the terms and conditions for trials, they would not necessarily know that there are additional steps to cancel a trial.

Although Google and Apple have tightened their requirements for trial subscriptions, fleeceware apps are still available for download. The best way to avoid downloading fleeceware is by carefully researching the app, the app developer, and reading through the terms and conditions of purchasing or subscribing to the app. If the price seems too high for the type of functionality it provides, then it might be...
Many of us have heard of, or have fallen victim to, identity thieves. These criminals use stolen personal information for financial gain or to hide their true identity. As law enforcement agencies, financial institutions, and credit bureaus continue to crack down on this activity, identity thieves have expanded their tactics. Many identity thieves now practice synthetic identity theft to try and avoid sending up red flags to victims and credit monitoring services.

Synthetic identity theft is the criminal process of creating an all new identity from both real and fake information as opposed to stealing an existing identity. The resulting identity has been called “Frankenstein identities” by some due to the patchwork manner in which identities are created from both real and fake information.1 For example, a criminal actor may create and use a fictitious name while also using someone's stolen social security number to apply for a credit card. This crime is often not detected for extended periods of time because the identity in question is fake and can be difficult to trace. Individuals who fall victim to this crime may not realize that their information is being used illegally because negative credit reports will be tied to a victim’s social security number but not the victim's name. This means that victims may not receive credit alerts about the activity.2

Synthetic identity theft is one of the fastest growing and most common types of identity theft and can be used for a number of illegal acts including fraudulently applying for credit cards, filing fraudulent tax

---

2 Ibid.
3 Ibid.
4 https://www.zdnet.com/article/fleeceware-apps-discovered-on-the-ios-app-store/
5 Ibid.
6 https://www.wired.com/story/what-is-fleeceware-protect-yourself/
returns, or obtaining unlawful employment, amongst other crimes.\(^3\)\(^4\) Cyber thieves committing synthetic identity theft are likely to target the personal information of those who are less likely to regularly check their credit reports like young children or elderly individuals. Over the years, large scale data breaches have also made personal identifying information like social security numbers, names, and the dates of birth of millions of people available on the dark web. Cyber thieves scour dark web marketplaces for this stolen information and can use bits and pieces of this information to craft a synthetic identity.\(^5\) All this can make it challenging for law enforcement to locate the real identity of a criminal actor using a synthetic identity.\(^6\)

Synthetic identities have even been used to communicate with the credit card companies and set up lines of credit. Usually, companies and organizations bear the brunt of the losses from this crime when thieves deplete a credit line and leave the financial institution to deal with the debt.\(^7\) Synthetic identity theft accounts for 10-15% of lender losses annually.\(^8\) In all, credit card companies reported losses of approximately $820 million to synthetic identity fraud in 2018.\(^9\) However, negative credit reports may be tied to a victim if their social security number is used.

To ensure that your personal information isn’t being used to commit this crime, it’s important to regularly monitor your credit reports to ensure that no fraudulent activity is occurring. Also, keep your social security number secure by properly disposing of important documents and not giving this information out to unauthorized individuals, especially if it is request via phone, email, text, or social media. To help protect children and the elderly, consider freezing their credit when not in use, regularly checking or advising them to check their social security statements, and ensure that these individuals’ personal information is well-protected.\(^10\)

\(^3\) https://www.ftc.gov/sites/default/files/public-comments/credit-report-freeze-534030-00033.pdf
\(^5\) https://securityboulevard.com/2020/07/deep-dive-into-synthetic-identity-fraud/
\(^7\) https://www.lifelock.com/learn-identity-theft-resources-synthetic-identity-theft.html#:~:text=Since%202014%2C%20synthetic%20identity%20has%20caused%20institutions%20to%20hold%20the%20bag.
Healthcare giant UHS hit by ransomware attack, sources say


- One of the largest healthcare providers in the U.S. was hit by a ransomware attack that locked computer and phone systems at multiple healthcare facilities.

   Analyst Note: The importance of securing of healthcare networks has been highlighted during the COVID-19 pandemic as people increasingly rely on this industry to provide health services. Cyber attacks on the healthcare sector jeopardize not only those seeking services at healthcare facilities, but may also jeopardize patient and employee data.

Can Schools Pass Their Biggest Cybersecurity Test Yet?

https://www.darkreading.com/edge/thedeeper/can-schools-pass-their-biggest-cybersecurity-test-yet/b/d-id/1338975

- Many schools have implemented a mix of online and in-person learning to adhere to social distancing guidelines.

- K-12 school networks have historically faced challenges with securing their information technology infrastructure against cyber threats.

- The sudden shift to online learning has likely increased schools’ risk exposure to cyber criminals.

   Analyst Note: K-12 schools’ networks were already facing security challenges before the COVID-19 pandemic. The sudden expansion of remote learning has seen an increase in the targeting of educational facilities by cyber criminals. Ransomware attacks and distributed denial of service (DDoS) attacks continue to disrupt distance learning.
Business ID Theft Soars Amid COVID Closures


- Business identity theft occurs when criminals pose as the owner or an employee of a legitimate business to apply for lines of credit using the businesses name.
- Experts estimate a 258% increase in business identity theft in 2020 as business identity thieves take advantage of the increased rate of small business closures.

**Analyst Note:** Business owners can take steps to avoid falling victim to business identity theft by regularly monitoring their businesses credit files for unauthorized charges. Business can also check with their Secretary of State’s office or their state agency responsible for business registration.

Protecting data in the work-from-home age


- The COVID-19 pandemic has caused many people to begin working from home.
- This change has highlighted the risk of insider threats as employees access potentially sensitive data using home networks.

**Analyst Note:** The rapid increase in working from home has presented information security challenges for many organizations. As many organizations quickly adapted to allow for teleworking capabilities, cyber threat actors adapted their tactics as well to target teleworking infrastructure including remote desktop protocol tools.

The Attack That Broke Twitter Is Hitting Dozens of Companies


- A small group of hackers allegedly used phone spear phishing attacks to gain access to the Twitter accounts of 130 people including high-profile individuals.
- The hackers then sent out a series of tweets from these compromised accounts attempting to scam followers out of bitcoin.

**Analyst Note:** Phone spear phishing is another form of social engineering used to gain sensitive information. In this incident, hackers allegedly took advantage of the fact that employees were teleworking and posed as IT staff to trick employees into handing over their passwords.
What is TLP?

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

This Beacon is TLP: White and is intended for wide distribution. If you would like to read past issues of the The Beacon, visit the Secure Florida website.

www.SecureFlorida.org/The_Beacon

The following is from the United States Computer Emergency Readiness Team (US-CERT):

- **RED**
  
  Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

- **AMBER**
  
  Recipients may only share TLP: AMBER information of their own organization who need to know, and only as widely as necessary to act on that information.

- **GREEN**
  
  Recipients may share TLP: GREEN information with peers, partner organizations, and with their sector or community, but not via publicly accessible channels.

- **WHITE**
  
  TLP: WHITE information may be distributed without restriction, subject to copyright controls.