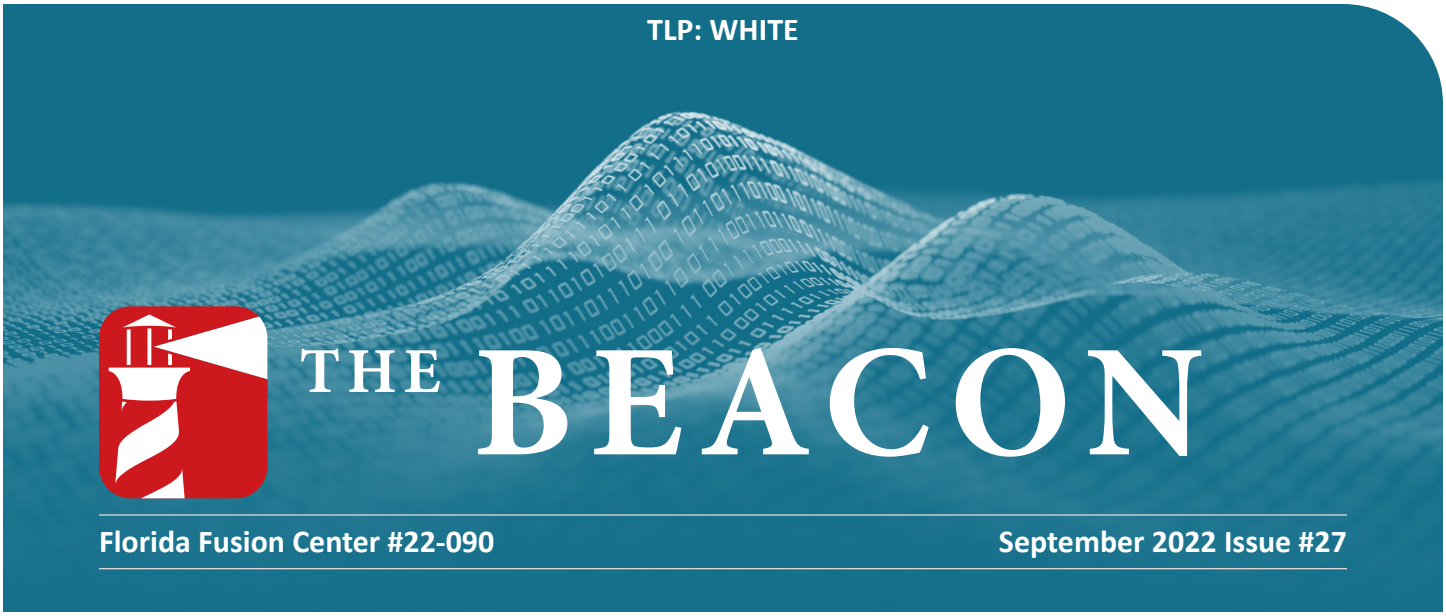

THE BEACON

Florida Fusion Center #22-090 September 2022 Issue #27

Table of Contents

CONTACT THE FIPC:
Phone: (850) 410-7645
Email: FIPC@fdle.state.fl.us

EDITOR'S CORNER

Is This What I Signed Up For? Tracking Online Accounts

Do you know how many online accounts you have? We live in a world where many people prefer to do everything online whether they are shopping, banking or interacting with people through different applications. Many of us have probably forgotten about more online accounts than we realize. It's important for users to know what accounts they have and make sure those accounts are secure.

We live in a world where many people prefer to do everything online whether they are shopping, banking or interacting with people through different applications.

According to research, the average person has at least 100 online accounts with passwords used to access them.[1] A major step you can take to protect yourself online is to make sure you keep track of all of your online accounts and passwords. Cybercriminals are always looking to steal or buy online account credentials and take over accounts. This stolen information can be used to conduct phishing schemes and lure individuals into giving them sensitive data or money.[2] The credentials can also be used to hack into other organizations' networks especially if you reuse passwords or use a weak or common password.[3]

When it comes to tracking your online accounts, there are some things to take into consideration:

1. Do you need all of your online accounts? If not, consider deleting the ones you don't need.
2. For the accounts you want to keep, are your passwords strong enough? Visit Secure Florida's Passwords page for information on how to build a strong password.
3. Have any of your online accounts been compromised? Visit https://haveibeenpwned.com/ to find out if your account information has been compromised. This may also prompt you to update your password.

If you find it difficult to manage your online accounts using these tips, you should consider using a password manager[a] to help you. They are generally safe and can offer multiple features depending on which one you use.[4] There are different options available at different price points, but it is best to research which password

Find what works for you!

manager works best for you.

Keeping inventory of your online accounts is a vital part of staying safe online. Don't let it overwhelm you. Consider the tips above as the internet, and how you use it, continues to evolve!

[a] A password manager is a software application designed to store and manage online credentials.

[1] https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html
[2] https://www.f-secure.com/us-en/home/articles/why-do-hackers-want-your-personal-information#:~:text=Login%20details%20are%20needed%20for,lose%20access%20to%20your%20account
[3] https://www.zdnet.com/article/dont-use-these-passwords-these-are-the-most-popular-log-in-details-found-for-sale-online/
[4] https://www.experian.com/blogs/ask-experian/should-you-use-a-password-manager/

CYBER THREATS

Who Cut the Cheese... Production? Cyberattacks and the Supply Chain

While a shortage of cream cheese may not be an issue for the everyday shopper, a shortage around the holidays can have major implications for businesses and consumers that rely on this ingredient to create various dishes for shoppers and family gatherings. In October 2021, a Wisconsin-based food production company, and one of the biggest dairy product manufacturers in the U.S., was forced to temporarily stop operations due to a cyberattack. While the facility was eventually able to resume operations, the impact to the supply chain rippled outward and impacted other food manufacturing companies, bakeries, delis, grocery stores and others. The disruption also added additional strain on other dairy producers, who already faced higher than average demand.[1 2 3]

Cybercriminals have targeted nearly all sectors of the consumer supply chain and continue to target manufacturers and producers in all sectors.

Cybercriminals have targeted nearly all sectors of the consumer supply chain and continue to target manufacturers and producers in all sectors. Some of the more common attack methods include distributed denial-of-service (DDoS), phishing, malware and ransomware. In recent years, cybercriminals have increased the use of ransomware attacks to try to profit from victims. Cybercriminals carry out these attacks by exploiting software vulnerabilities, using stolen credentials obtained through other cyberattacks, brute force attacks or using ransomware-as-a service.[a 4 5]

In September 2021, a ransomware group known as BlackMatter hit a farmer co-op in Iowa. The organization was forced to take its computer systems offline, which resulted in the loss of its master-control system for software that optimizes irrigation and fertilization as well as other operating systems used for supply tracking and invoicing. While only a small part of the agriculture sector in Iowa was affected, similar attacks resulting in the loss of access to systems, information, data and downtime could challenge other agricultural organizations' ability to meet consumer and food supply chain needs.[6]

Being vigilant and up-to-date on cyber threat trends and mitigation techniques can help organizations protect themselves from cybercriminals looking to exploit and profit from organizations that are vital to U.S. supply chains.

In May 2021, cybercriminals associated with a group known as DarkSide, deployed ransomware on a major pipeline company that supplies approximately half of the fuel for the East Coast and some Southern states. In an effort to contain the threat, the company shut down its pipeline operations. The attack resulted in the company's oil pipeline, which stretches from Texas to New York and is around 5,500 miles long, to be shut down for approximately five days. The shutdown resulted in some regional gas shortages.[7] [8] [9] [10]

There are multiple actions businesses can take to secure their networks against cyberattacks. Ensuring all systems are secure and all software is patched and updated is a must. A few additional security steps include:

- Ensuring all employees are regularly trained on cybersecurity best practices.
- Requiring multifactor authentication and strong unique passwords for logins.
- Limiting remote access, where possible.
- Ensuring all backups are encrypted, and where possible, using multiple secure backup types.[11]

Being vigilant and up-to-date on cyber threat trends and mitigation techniques can help organizations protect themselves from cybercriminals looking to exploit and profit from organizations that are vital to U.S. supply chains. For more information on cybersecurity best practices or to schedule a FREE cybersecurity training for your organization, visit SecureFlorida.org.

[a] Ransomware-as-a-service is a business model used by cybercriminals where criminals will pay other criminals to launch ransomware attacks developed by other cybercriminals. In this situation, both the ransomware developer and user agree to a share of the ransom collected from the victim.

[1] https://www.usatoday.com/story/money/food/2021/12/11/cream-cheese-shortage-impacts-companies/6460876001/
[2] https://www.cnet.com/news/privacy/cream-cheese-shortage-stemmed-partially-from-cyberattack/
[3] https://www.bloomberg.com/news/articles/2021-12-09/that-cream-cheese-shortage-you-heard-about-cyberattacks-played-a-part
[4] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[5] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[6] https://www.washingtonpost.com/business/2021/09/21/new-cooperative-hack-ransomware/
[7] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
[8] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
[9] https://www.cnet.com/news/privacy/fbi-says-darkside-hacking-group-responsible-for-pipeline-cyberattack/
[10] https://www.cnbc.com/2021/05/12/colonial-pipeline-restarts-after-hack-but-supply-chain-wont-return-to-normal-for-a-few-days.html
[11] https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

Fake It 'Till You Make It: Fake Ransomware Attacks

Ransomware is a type of malware that is designed to encrypt files on a device, making the files and their systems unusable unless the victim obtains an encryption key by paying a ransom. In recent years, the threat of ransomware has led to cybercriminals initiating fake ransomware attacks to extort money from individuals and organizations. Fraudsters will reach out claiming that your device has been subject to ransomware, or hack in and display a message and demand money in exchange for decryption, when there is no actual malware on your device.[1] Cybercriminals are counting on victims to not confirm they have been hit with ransomware first and will just pay the ransom immediately. Unfortunately, this attack type leverages fear and has caused significant financial losses for victims.

Fake ransomware attacks have traditionally been used for extortion, but some cybercriminals are now using these attacks with different motivations.

In November 2021, an open-source content management company's software, which is widely used for building websites, was targeted with fake ransomware attacks. Nearly 300 websites were affected. It is likely that cybercriminals compromised administrative accounts through brute force attacks[a] or stolen credentials from the dark web to launch their attacks and create the illusion of a ransomware infection. Approximately $6,000 was demanded in the ransom notes sent to the victims. Cybersecurity researchers analyzed the attacks and determined there was no malware deployed in this specific campaign, however, they did find a software vulnerability that could have potentially allowed for actual ransomware deployment if discovered.[2 3]

Fake ransomware attacks have traditionally been used for extortion, but some cybercriminals are now using these attacks with different motivations. Recently, this tactic has been used to cause chaos in Ukraine, where organizations were hit with wiper malware[b] known as WhisperGate, which was used to destroy data versus extorting a payment. WhisperGate attacks undergo three stages:

- Stage 1: The master boot record (MBR)[c] is overwritten with a fake ransom note.
- Stage 2: A JPG attachment is downloaded and it consists of data-destroying malware.
- Stage 3: Files of nearly any type on the device are corrupted by the malware.[4 5]

In this case, even if a ransom is paid, you likely won't get your data back. It is important for people and businesses to be aware of

this tactic because there is the potential for this type of malware to be used to target critical networks in the U.S. in the future. Additionally, attacks conducted on organizations in Ukraine could have global impacts for organizations that have a presence in Ukraine or rely on supply chains from the country.

Cybercriminals will likely continue to find ways to leverage fake ransomware in multiple ways. Whether the motivation is money, data destruction or another motive, these attacks are serious! Rather than waiting until you're notified of a ransomware attack to figure out if the attack is fake, here are some prevention and mitigation strategies that can be used to protect yourself and/or organization regardless of the attack type:

Cybercriminals will likely continue to find ways to leverage fake ransomware in multiple ways.

- Keep your software patched and updated.
- Implement network segmentation.[d]
- Consider using an intrusion detection system, intrusion prevention system or another mechanism to monitor your network(s).
- Maintain offline data backups and monitor them.
- Require multi-factor authentication for any remote access services you use.[6] [7]

Being aware of global cyber threats can help individuals prepare for them in the event that they are impacted. It is important to also keep in mind that paying a ransom will not necessarily get your files back. For more information on protecting yourself from ransomware visit StopRansomware.gov and for more information on destructive malware affecting organizations in Ukraine, visit the Cybersecurity and Infrastructure Security Agency's website.

[a] A brute force attack is a trial-and-error method used to gain unauthorized access to a system or account by repeatedly entering account credentials either manually or using automated software.
[b] Wiper malware is designed to erase the hard disk of a targeted machine or destroy data on a machine.
[c] MBR refers to a location on a computer's hard drive that contains hard drive disk partition information and allows for it to load its operating system.
[d] Network segmentation divides a network into smaller parts, isolating some devices from others, to protect those that are critical to operations.

[1] https://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/?sh=5a12e7e4baab
[2] https://threatpost.com/fake-ransomware-infection-wordpress/176410/
[3] https://www.bleepingcomputer.com/news/security/wordpress-sites-are-being-hacked-in-fake-ransomware-attacks/
[4] https://www.bleepingcomputer.com/news/security/microsoft-fake-ransomware-targets-ukraine-in-data-wiping-attacks/
[5] https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine
[6] Ibid.
[7] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

Safe Social Networking: How to Avoid Social Media Phishing Attacks

Social media platforms like Facebook, Twitter and Instagram have provided a way for people to communicate, share and connect with others globally. Approximately 4.2 billion people worldwide use social media.[1] Some businesses even use social media to notify their customers about their latest products, marketing events or attract new business. This makes social media an attractive target for schemes that often involve social engineering.[a] These platforms, in particular, can be a target of social media phishing,[b] where some criminal actors use social platforms to steal personal information or access to their accounts.[2] It's important for users to understand social media phishing and how to protect themselves from it.

Social media users may publicize where they live, work, their interests, birthdays or other personal details, which can provide criminal actors with a wealth of information when conducting an attack.

Social media users may publicize where they live, work, their interests, birthdays or other personal details, which can provide criminal actors with a wealth of information when conducting an attack. Regardless of the platform, the attack usually involves sending a direct message or a post with a malicious link that leads to a fake website that looks like a legitimate social media login page. The messages typically come from fake accounts, usually impersonating someone the user may know or a well-known company. The types of messages used may vary based on the platform or the perceived interest of the target. For example, LinkedIn has been used by criminal actors to exploit job hunters and messages may include a request to download an application for the job of a lifetime. On another social media platform, criminal actors might post about how they made a large amount of money in a short period of time and include a link to find out more information.[3] [4] [5] [6]

Recently, another way criminal actors have leveraged social media is through posting quizzes or questionnaires.[7] Users may see a post that says something like: "Your superhero name is your high school mascot along with the model of your first car." The post may seem harmless and will ask someone to share their result in the comments section. The comments may seem entertaining, but it's possible several users have provided potential passwords or answers to common security questions for their personal accounts. Sharing this information could lead to accounts being hacked and used for impersonation schemes targeting a user's friends or family members.[8]

Phishing on social media can happen a number of different ways, but there are several things users can do to protect themselves from this threat.

Phishing on social media can happen a number of different ways, but there are several things users can do to protect themselves from this threat. Implementing the following tips may help reduce the risk of being a victim:

- Use unique login credentials for each account. This will help protect users' various social media accounts in the event one account's login credentials become compromised.[9]
- Don't provide sensitive information on social media.
- Look for inconsistencies in messages and posts. For example, hover over links without clicking on them to see if linked websites match up to the content.[10]
- Regularly check privacy settings on social media accounts to make sure users know what people, especially people they don't know, can see on their profile.[11]
- Don't accept friend requests from accounts or people that are unknown. Make sure requests come from a trusted source before approving them.[12]
- Visit Secure Florida's website for more information on how to recognize social engineering.

If you or someone you know becomes a victim of an online scam, you can report the scam to your local law enforcement agency or to the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) at https://www.ic3.gov.

[a] Social engineering is the use of deception to trick individuals into sharing confidential or personal information for fraudulent purposes.
[b] Phishing happens when malicious actors send messages pretending to be a trusted person or entity. Phishing can trick a user, causing them to install malware, click on a malicious link or share sensitive information.

[1] https://www.vadesecure.com/en/blog/the-art-of-deception-in-social-media-phishing
[2] https://www.trendmicro.com/en_us/what-is/phishing/social-media-phishing.html
[3] https://cofense.com/knowledge-center/social-media-phishing-what-you-need-to-know/
[4] https://us.norton.com/internetsecurity-online-scams-social-media-scams.html
[5] https://inspiredelearning.com/blog/social-phishing/
[6] https://www.vadesecure.com/en/blog/the-art-of-deception-in-social-media-phishing
[7] https://www.cnet.com/tech/services-and-software/these-phishing-tactics-disguised-as-fun-on-social-media-heres-what-to-look-for/
[8] https://www.bbb.org/article/scams/16992-bbb-scam-alert-bored-think-before-taking-that-facebook-quiz
[9] https://www.metacompliance.com/blog/how-to-protect-yourself-from-social-media-phishing/
[10] https://www.cnet.com/tech/services-and-software/these-phishing-tactics-disguised-as-fun-on-social-media-heres-what-to-look-for/
[11] https://www.metacompliance.com/blog/how-to-protect-yourself-from-social-media-phishing/
[12] https://cofense.com/knowledge-center/social-media-phishing-what-you-need-to-know/#_ftnref1

Scams Targeting Seniors and How to Avoid Them

Seniors are often targeted with scams to steal sensitive data like their personal identifiable information (PII), bank account information or money.[1] In 2021, the Internet Crime Complaint Center (IC3) received reports from 9,645 victims over 60 in Florida representing more than $224 million in losses. Scammers look to victimize seniors for multiple reasons because they feel they may be wealthy or less likely to report a crime if they are targeted.[2] Criminal actors will usually look to exploit fear or find a way to gain their trust to carry out their scams. Below are three common scams that target seniors.

Seniors are often targeted with scams to steal sensitive data. Criminal actors will usually look to exploit fear or find a way to gain their trust to carry out their scams.

A romance or confidence scam is when a person adopts an online identity to gain a victim's affection or friendship and uses the illusion to manipulate and steal money.[3]

+ A Jacksonville, Florida, resident met a woman online, and she convinced him to send money to pay an attorney for a marriage license and fees she claimed would allow her to receive a $40 million inheritance. He received checks from his supposed wife for repayment, but the checks returned insufficient funds. The resident eventually discovered he was not married and reported the scam.[4]

The lottery or sweepstakes scam can start with a call, text, email or letter stating that the intended victim won a lottery, contest or sweepstakes that they did not enter. In order to receive the prize money, a fee or taxes must be paid upfront.[5]

+ Port St. Lucie Police Department conducted an investigation after an elderly man sent over $100,000 to criminal actors claiming he won the lottery and needed to pay the taxes and fees to receive the prize. He sent the required money to New York and Florida. The police were able to recover $40,000.[6]

Some criminal actors will target a senior, pretend to be their grandchild and create an "emergency" to illicit money from them with fear, urgency or intimidation. To make these scams more believable, criminal actors sometimes scour social media to gather data about potential victims or purchase stolen PII from cybercriminals. These criminal actors may use additional actors or couriers to pick up money from a grandparent's home.[7] This scam is usually conducted by phone; however, it can also be initiated via email using urgent subject lines (e.g. Help Grandma, I'm in Jail!).

+ In May 2022, a Hollywood, Florida, resident pled guilty

to being a part of a grandparent scheme that involved a sophisticated criminal network that would leverage victims' fears by stating their relatives were in legal trouble and needed bail money or money for medical expenses after a car accident. The network extorted tens of thousands of dollars that affected several seniors across the United States.[8]

Here are some tips for online safety for seniors:

Think before you act, especially when it comes to urgent correspondence or requests.

- Think before you act, especially when it comes to urgent correspondence or requests.
- Share with care, especially on social media.
- When in doubt, throw it out. Do not click on links in emails or text messages.
- Do not send money to strangers, especially if the email/text appears suspicious.
- Monitor your online financial accounts for unusual activity.
- Never provide sensitive information to unvetted individuals or organizations.
- Report scams to the authorities, including local police.[9] [10] [11]

Using these tips about common threats can help protect seniors from common online scams.

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
[2] https://www.experian.com/blogs/ask-experian/top-scams-targeting-seniors/
[3] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
[4] https://www.news4jax.com/news/local/2021/12/03/jacksonville-veteran-says-hes-victim-of-a-social-media-romance-scam/
[5] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf
[6] https://www.orlandosentinel.com/news/florida/os-ne-elderly-florida-man-sends-100k-to-lottery-scammers-police-recover-40k-20220106-hk3eh6inyvelhd3mse3rhfu42u-story.html
[7] https://www.fcc.gov/watch-out-grandparent-scams
[8] https://www.justice.gov/opa/pr/fourth-defendant-grandparent-scam-network-pleads-guilty-rico-conspiracy
[9] https://www.connectsafely.org/seniors-guide-to-online-safety/
[10] https://cyberinsureone.com/online-safety-seniors/
[11] https://www.justice.gov/usao-ndal/pr/us-attorney-s-office-and-fbi-raise-awareness-elder-abuse

CYBER HIGHLIGHTS

Call for Backup! (and Prepare for Cyberattacks)

With the increasing amount of digital data comes the ever-present threat of cyberattacks, and organizations, including government agencies, are often targeted.

"Call for backup!" is an iconic line, frequently referenced in our favorite television shows. Calling for backup can improve the odds of a positive outcome, offer solidarity and increase protection. A similar desire for backup can be exercised daily in our lives, especially when it comes to the cyber realm. It is essential for organizations and individuals to establish effective data backup plans to preserve information. With the increasing amount of digital data comes the ever-present threat of cyberattacks, and organizations, including government agencies, are often targeted.[1]

Data backup refers to duplicating and copying data or files so that they can be retrieved in the instance they are lost or damaged somehow.[2] This endeavor can be considered a disaster contingency plan and a way to prepare in case of a cyberattack.[3] Try as you might to eliminate these threats, it can be difficult to protect against all threat types simultaneously.[4] Some common cyberattacks include ransomware or the installation of other forms of malware, which may encrypt, destroy or restrict access to files.[5]

Cyberattacks can come with devastating consequences, such as data loss, the leaking of confidential information and blocked access to essential functions. For example, law enforcement agencies that have been hit with attacks in the past lost digital files and critical documentation, including video evidence.[6] Many cybercriminals steal data to make a profit by selling user information on the dark web. Buyers often use stolen data to make fraudulent transactions to commit extortion, or to resell to marketing firms for spam campaigns.[7] Bearing this in mind, it is important to prevent losing access to data files and suffering the consequences of stolen information, which notoriously place victims in monetary and operational jeopardy.[8]

There are several strategies people and organizations can take to preserve information through data backups. A notable example is the 3-2-1 rule: this guideline encourages having three copies of data, stored across two different mediums and one storage cloud provider.[9] [10] If a cybercriminal successfully attacks one's

network, they often have the capability to target any local backup present on the same network, so it can be helpful to implement a backup plan that involves being physically disconnected from the internet network. Regardless of the method you choose, it is recommended to have different locations for data storage, such as offline or offsite, to receive the best protection.

Data backup is considered an essential practice in this day and age. To ensure the preservation of information vital to the public, one must call for backup.

There are also other types of data backup plans, with the full-backup[a] plan being chief among them. This refers to a complete copy of all data and it is recommended to implement this type at least once for sufficient data preservation.[12] A full backup ensures that the bulk of an organization's information can be retrieved and restored. Once a full backup is established, other backup plans can be incorporated, such as differential[b] and incremental[c] data backup. These can be used to recover changes and additions made since the previous full data backup.[13]

Data backups should be a key part of every organization's plan for recovery and business continuity in the event of a cyberattack.[14] It is also important to regularly test backups to ensure they work. This can be through the use of third-party audits, disaster recovery drills or other testing methods.[15] Agencies related to law enforcement, health care, policymaking and other essential sectors should invest in the necessary precautions to safeguard against cyberattacks.

[a] A full backup involves making at least one additional copy of all data files an organization wishes to protect.
[b] A differential backup copies all of the files that have changed since the last full backup.
[c] An incremental backup only copies data that has been changed or created since the previous backup.

[1] https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/?ref=33debf3f4b70ddaed1a98bb9344c4522
[2] https://www.techopedia.com/definition/1056/backup
[3] https://www.whymeridian.comblog3-data-backup-types-for-business-continuity-full-data-backup-differential-data-backup-and-incremental-data-backup
[4] https://www.techtarget.com/searchdatabackup/news/252515389/White-House-Data-backups-critical-part-of-cyber-strategy
[5] https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks
[6] https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/
[7] https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it
[8] https://www.egnyte.com/guides/governance/data-breach-cost
[9] https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html
[10] https://infosecurity-magazine.com/opinions/keeping-backups-ransomware/
[11] Ibid.
[12] https://www.whymeridian.comblog3-data-backup-types-for-business-continuity-full-data-backup-differential-data-backup-and-incremental-data-backup
[13] Ibid.
[14] Ibid.
[15] https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/?ref=33debf3f4b70ddaed1a98bb9344c4522

Devise a Device Plan! Protect Yourself From Mobile Malware

Can't put that phone down for some reason? A 2021 study revealed consumers spent an average of about five hours per day on their mobile devices.[1] Many people use their devices for multiple purposes including work, school, social media, shopping, banking and gaming. The increase in use of mobile devices during the pandemic allowed many to continue their jobs or education at home. Our mobile devices are an essential part of our lives, so it's essential to protect them from cyber threats.

Many of us use mobile devices for personal reasons, but many organizations may also use mobile devices for point of sale transactions, record-keeping, data logging and custom form submissions. Some organizations may even find ways for mobile devices to be used as full workstations with proper configurations in place.[2] Continued reliance on mobile devices also increases the potential for these devices to be targeted by cybercriminals.[3] According to mobile security researchers, 30% of the known, zero-day vulnerabilities[a] discovered in 2021 specifically targeted mobile devices. Additionally, there were over two million new mobile malware samples detected globally in 2021.[4]

Many of us use mobile devices for personal reasons, but many organizations may also use mobile devices for point of sale transactions, record-keeping, data logging and custom form submissions.

There are several types of mobile malware that cybercriminals commonly deploy to infect mobile devices including:

- Remote Access Tools (RATs)[b]
- Bank trojans[c]
- Advertising Click Fraud[d] [5]

Cybercriminals will often use phishing, or in this case smishing, to initiate their mobile malware attacks. Smishing involves sending SMS or text messages with malicious links that can lead to stealing personal information or downloading malware to your device. One well known form of mobile malware is FluBot, which is designed to steal usernames and passwords from banks on other sites users visit. Another is TangleBot, which is usually delivered through fake package-delivery notifications. Not only can TangleBot steal sensitive information, but it can also take over devices and intercept camera footage and audio recordings.[6]

The rise of mobile malware attacks brings forth the need to be extra cautious in the ways you use your mobile devices. Having a mobile device comes with risks, but there are steps that can be taken to protect your work or personal devices. A few tips that

will improve security include:

- Keep your software up-to-date to avoid being exposed to security vulnerabilities.
- Never open files or links sent from an unknown, suspicious or untrustworthy source. This applies to emails, direct messages on mobile applications (apps) and text messages.
- Use encryption features on mobile devices to keep data more secure. Many devices come with these features.
- Be careful when downloading an app to ensure it is a vetted app from a trusted source. Many have malicious software that can lead to compromising your device.
- Avoid using public Wi-Fi for sensitive transactions. Public networks can easily be breached by hackers and lead to accessing your data and device.
- Use biometric authentication such as facial recognition or fingerprints, when possible. This could prevent cybercriminals from accessing certain online accounts you have.

If you are using your own device for work purposes, remember to follow your organization's policies for utilizing your own device.

If you are using your own device for work purposes, remember to follow your organization's policies for utilizing your own device. Following these tips and your organization's policies and procedures can help you avoid becoming a victim of a mobile device breach.[7] [8]

[a] A zero-day vulnerability is an unknown software flaw or weakness that can be exploited and has not yet been patched.
[b] RATs give nearly full access to a device's data and can also allow cybercriminals to control it.
[c] Bank trojans are often disguised as legitimate applications and aim to steal financial login and password details.
[d] Advertising click fraud is a type of malware that allows an attacker to hijack a device to generate income through fake ad clicks.

[1] https://www.cnet.com/tech/services-and-software/americans-spent-a-third-of-waking-hours-on-mobile-devices-in-2021-report-finds/
[2] https://www.techtarget.com/searchmobilecomputing/The-ultimate-guide-to-mobile-device-security-in-the-workplace
[3] https://trivestgroup.com/5-major-types-of-security-breach-to-watch-out-for-in-your-organisation/?msclkid=0bb73b6abb3311ecbb68dcd9a7a1857c
[4] https://blog.zimperium.com/global-mobile-threat-report-key-insights/
[5] https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/
[6] https://www.zdnet.com/article/smartphone-malware-is-on-the-rise-heres-what-to-watch-out-for/#:~:text=Cybersecurity%20researchers%20at%20Proofpoint%20say,beginning%20and%20end%20of%20February
[7] https://www.vmware.com/topics/glossary/content/mobile-device-security.html
[8] https://mobiletrans.wondershare.com/android-transfer/mobile-device-security.html

DISPATCH HIGHLIGHTS

This section highlights articles from past issues of FIPC's *The Dispatch* that our analysts think are noteworthy based on trends we're seeing in Florida. *The Dispatch* is a list of open-source articles compiled for the law enforcement, cyber intelligence and information security communities that is sent out twice weekly. To sign up for the *The Dispatch*, visit SecureFlorida.org and click "**Get Connected**" at the top of the homepage or send an email to **FIPC@fdle.state.fl.us**.

FBI WARNING: THIS RANSOMWARE USES DDOS TO THREATEN VICTIMS. HERE'S WHAT TO WATCH OUT FOR

https://www.zdnet.com/article/fbi-warns-on-ransomware-that-uses-ddos-to-threaten-victims-heres-what-to-watch-out-for/

- A ransomware group known as AvosLocker has targeted the financial services, critical manufacturing and government facilities sectors in the U.S. since July 2021.
- In some cases, AvosLocker has threatened to conduct DDoS attacks, which can lead to triple extortion, which involves the threat of releasing data, disrupting services and embarrassing the organization by revealing the attack.

Analyst Note: Ransomware groups are increasingly using triple extortion. For mitigation, organizations should consider implementing a recovery plan that involves maintaining multiple copies of critical data and servers in a secure location that is physically separated from the network.

FTC TO CRACK DOWN ON COMPANIES THAT ILLEGALLY SURVEIL CHILDREN LEARNING ONLINE

https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online

- Under the Children's Online Privacy Protection Act, companies are not permitted to deny children under age 13 access to educational technologies if their parents or schools refuse to opt into commercial surveillance.
- Companies looking to harvest personal information on virtual learning platforms could potentially face civil penalties for any misuse of children's personal information.

Analyst Note: Before downloading educational apps, parents can check reviews and find information on the data that would be accessed while using them. This can help parents determine if an app is safe for their children to use.

CHINESE SPIES HACKED A LIVESTOCK APP TO BREACH US STATE NETWORKS

https://www.wired.com/story/china-apt41-hacking-usaherds-log4j/

» A Chinese cyberespionage group known as APT41 compromised an app used by U.S. state governments to track and trace animal diseases through livestock.

» APT41 has also hacked into other apps to gain initial access to state government networks.

Analyst Note: Nation-state actors continue to use multiple attack vectors to gain footholds in U.S. networks. Organizations should patch their software as soon as reasonably possible once security updates become available.

MASSIVE ONLINE MARKET FOR STOLEN DATA TAKEN DOWN BY GLOBAL OPERATION

https://www.cnet.com/tech/services-and-software/massive-online-market-for-stolen-data-taken-down-by-global-operation/

» U.S. and European law enforcement agencies collaborated to take down a large illegal online market that sold millions of stolen credit card numbers and other sensitive information.

Analyst Note: Cybercriminals will often use illegal forums to purchase sensitive data to commit nefarious activity such as identity theft or scams. Users should monitor their financial accounts carefully to identify any fraudulent transactions.

RUSSIAN STATE-SPONSORED AND CRIMINAL CYBER THREATS TO CRITICAL INFRASTRUCTURE

https://www.cisa.gov/uscert/ncas/current-activity/2022/04/20/russian-state-sponsored-and-criminal-cyber-threats-critical

» Russian state-sponsored cyber threat actors possess capabilities to compromise IT networks, maintain long-term network access and disrupt industrial control systems.

Analyst Note: While there may be no known credible threats to Florida, Russian cyberattacks on Ukraine have the potential to spread. Organizations should visit CISA's Shields Up page for more information on prevention strategies.

TWO ALLEGED LAPSUS$ TEENS APPEAR IN LONDON COURT

https://www.cyberscoop.com/lapsus-defendants-in-court-more-hacks/

» An extortion group known as Lapsus$ is responsible for stealing data from multiple major companies around the world.

» Impacted companies include a widely-used computer operating systems software company, a computer chip manufacturing company and others.

Analyst Note: Lapsus$ breached networks using SIM swapping, stolen account credentials or by recruiting employees at targeted companies. Organizations should consider implementing an insider threat program to detect potential risks.

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.

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 with members 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	Recipients may share **TLP: WHITE** information without restriction, subject to copyright controls.

THE BEACON

ABOUT THE FIPC AND *THE BEACON*

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

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

This addresses DHS HSEC-SIN-1; FDLE SINs 1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.6.1, 1.2.1, 1.2.2, 1.5.2, 1.8.2, 1.10; and 1.13; and FFC-SINs 1.1, 1.3, 1.4, 1.5, and 1.7