THE BEACON

Florida Fusion Center #23-049

April 2023 Issue #30

Table of Contents

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

Beware of Bad Investments: Investment Scams

Investment scams give false promises and advertise ways potential investors can make money quickly, easily, and with low risk. These scams sometimes start with a free seminar, possibly with a free meal and travel offers, during which the promoter will charge a hefty fee to get access to “the investment tricks.” Methods scammers may use to entice individuals include guarantees of high returns with low or no risk, invitations to join exclusive investment organizations, claims of new breakthrough technologies, and the ability to get on the ground floor of an investment. These scammers often try to get the victim to invest in financial schemes or real estate.[1] The scammers may use word of mouth, groups (religious or friendships), social media platforms, unsolicited calls, and emails to entice, scare, or otherwise pressure victims into investing.[2][3] There are many different investment scams. This article will discuss some of the most common scams.

Investment scams give false promises and advertise ways potential investors can make money quickly, easily, and with low risk.

Investment coaching scams offer a patented, tested, or proven strategy to make money through specific bonds, stocks, tax liens, or foreign currency. Scammers promote these methods as easy ways to be financially “set for life.”[4]

Real estate investment seminar scams teach potential investors how to invest in real estate and promote risk-free training or business coaching systems. These seminars can be in-person or online and promise financial freedom and big money.[5]

Affinity fraud targets specific groups, for example elderly populations or religious groups. These investors pretend to be part of the group to gain trust and build friendships through which they entice group members to buy into the program. Affinity fraud may involve a Ponzi or pyramid scheme in which new investments pay off old investors, giving the appearance of making money.[6]

Although no scam prevention is foolproof, there are ways to protect yourself against investment scams:

- Verify credentials. Legitimate investment professionals are registered with the Financial Industry Regulatory Authority (FINRA), the Securities and Exchange Commission (SEC), and your state securities and insurance regulator.

- Adopt a mindset that, “There is no such thing as easy money.”
- Don’t follow the crowd. If investors come to your church, social circle, or job, don’t take what others are saying at face value. Make your own informed decisions.
- Don’t rush to a decision. If given a limited window to make decisions, walk away.
- Don’t feel obligated or guilted to invest because a seminar includes a free meal or travel package.
- Ask for documentation. If there is no documentation, the securities may not be registered with the SEC which would prevent them from being sold to the public.[7]

No scam prevention is foolproof, but there are ways to protect yourself against investment scams.

[1] https://consumer.ftc.gov/articles/real-estate-investment-scams

[2] https://www.investor.gov/protect-your-investments/fraud/types-fraud/internet-and-social-media-fraud

[3] https://www.schwab.com/learn/story/how-to-spot-investment-scam

[4] https://consumer.ftc.gov/articles/real-estate-investment-scams

[5] Ibid.

[6] https://www.investor.gov/protect-your-investments/fraud/types-fraud/affinity-fraud

[7] https://www.schwab.com/learn/story/how-to-spot-investment-scam

Wolves in Sheep's Clothing: Fake Apps with Malicious Intent

Malicious mobile apps are applications downloaded onto an electronic device such as a computer, smart phone, or tablet which then infect the device with malware. Malware includes viruses, spyware, ransomware, and other unwanted software that can be secretly installed onto your device through malicious links and files, disguised as apps, or through other means.[1] Criminals use these malicious apps for many reasons, including financial gain, to obtain your personal identifiable information, to obtain login credentials from other apps on your device, to steal or encrypt sensitive files, to track your location, and more.[2]

Criminals use malicious apps for many reasons, including financial gain, to obtain your personal identifiable information, to obtain login credentials from other apps on your device, to steal or encrypt sensitive files, to track your location, and more.

These malicious apps can be added to a mobile device through an infected app in the device's app store, a link in a text message, a website, or an unofficial app store on the web. Malicious apps can be anything and look identical to well known or official apps, sometimes offering fraudulent services upon download. For example, some apps will direct users to websites through links in the app or a pop up which may offer fraudulent security tools that claim to help the user with phone, battery, or Wi-Fi issues. Once the user clicks on the links it may redirect to a phishing website that collects personal information, or it may have users click on links which then install files to the device. Additionally, some malicious apps can install website extensions which can open the web browser or generate pop ups that lead to phishing sites even with the device locked.[3]

A few steps you can take to protect your device from malicious apps are:

1. Never click on unknown or unsolicited links on websites, in text messages, or on pop ups.
2. Prior to downloading apps, look at the reviews to see if other users are reporting issues that may indicate this app is malicious. You can also research the app name on the web to see if it has been identified as a malicious app.
3. If the app is from a well-known publisher or brand, ensure you are downloading the company's official app and not a fraudulent malicious app made to look like the official one.
4. Look at the permissions the app is requesting access to on your device. This can give malicious apps permission to reach their target or allow access to files or other

applications they shouldn’t have access to.

5. Only download apps from trusted stores, websites, or providers.[4]
6. Always keep your app and device software up to date.

Being vigilant and doing the research before downloading an app can help protect your device and your personal information.

While it can be difficult at times to know if your device has been infected by a malicious app, there are some indicators to look out for including:

- Your device won’t power down when prompted or slows down, crashes, or drains your battery faster than usual.
- You are unable to remove specific apps or software.
- You receive a lot of pop-ups or your web browser displays inappropriate advertisements, or the advertisements on websites interfere with your ability to see or interact with the page content.[5]

While it may be difficult at times to spot malicious apps before or after installing them, being vigilant and doing the research before downloading an app can help protect your device and your personal information.

[1] https://www.yahoo.com/lifestyle/malicious-apps-signs-yahoo-subscriptions-170133021.html

[2] https://www.zdnet.com/article/cyber-criminals-are-repurposing-real-smartphone-apps-to-spread-malware-heres-how-to-stay-safe/

[3] https://www.bleepingcomputer.com/news/security/malicious-android-apps-with-1m-plus-installs-found-on-google-play/

[4] https://www.mcafee.com/blogs/mobile-security/before-you-download-steer-clear-of-malicious-mobile-apps/

[5] https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware#have

Modern-Day Street Smarts: Online Gaming Safety

There are more than a billion people around the world across all demographics who play online games.[1] Gaming is a huge and diverse industry ranging from small single-person mobile device games to Massively-Multiplayer Online games (MMOs) where a player can come into contact with several other players every time they log on. While online gaming is a great way to interact virtually, or just have fun, it also comes with a plethora of risks. In order to mitigate these risks,[2] gamers need to know what to watch out for.

While online gaming is a great way to interact virtually, or just have fun, it also comes with a plethora of risks. In order to mitigate these risks, gamers need to know what they are watching out for.

Phishing emails, in-game fraud, and malware downloads can aid criminals in acquiring virtual assets such as character, inventory, and account details as well as personal assets such as bank account information, credit card information, and personal identifiable information. It is important to know what to look for in order to avoid becoming a victim. Phishing emails sometimes include poor spelling and grammar and phrases like “urgent action required,” or “your account will be closed,” and ask for sensitive information or credentials.[3] Often, phishing emails include attachments or links that will download malware once clicked. Malware is also commonly bundled into pirated versions of games.[4] In-game fraud schemes commonly appear as other players offering to help you obtain free currency “deals” that seem too good to be true. This is because they are. The chance is if someone is asking for personal information, login credentials, or real currency in exchange for virtual goods or services, the trade is likely a scam and should be avoided.

There are several ways to limit your chances of becoming a victim of a cyber-crime. First, make sure every password is strong. A password should not include personal information or common words, it should use both upper- and lower-case letters with special characters when possible, and it should not be the same password you use for any connected account.[5] To strengthen your credentials even further, you can utilize a multifactor authentication app or key.[6] Additionally, make sure that your security and operating system on the device you are using is up to date.

Children also need education on how to avoid these crimes. Children who play games where they interact with other players should know not to share real-life personal information like their name and account information and to only trust information, requests, offers, and upgrades that come from a verified source such as the game itself and the official website. They should also be told how to avoid phishing scams once they have their own accounts to further protect them from becoming victims. Everyone needs to be aware of possible threats to protect themselves, their physical and virtual assets, and their peace of mind.

Everyone needs to be aware of the possible threats.

[1] https://www.statista.com/topics/1551/online-gaming/#topicOverview

[2] https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf

[3] https://knowledgeburrow.com/which-of-the-following-characteristics-might-indicate-an-email-is-a-phishing-attempt/#:~:text=The%20email%20makes%20unrealistic%20threats%20or%20-demands.%20Intimidation are%20common%2C%20unrealistic%20threats%20associated%20with%20phishing%20messages.

[4] https://www.cyberpeace.org/cybercriminals-using-online-gaming-to-target-kids/

[5] https://techspective.net/2017/10/18/5-steps-create-secure-passwords/

[6] https://www.techrepublic.com/article/how-cyberattacks-are-targeting-video-gamers-and-companies/#:~:text=Gaming%20companies%20and%20websites%20have%20also%20been%20targeted,industry.%20SEE%3A%20Identity%20theft%20protection%20policy%20%28TechRepublic%20Premium%29

Digital Espionage: Spyware

Have you ever thought about what may be lurking within the files of your computer or electronic device? If you haven't considered this, maybe it's time. Spyware is a malicious type of software that can be installed onto your device without your knowledge or consent and collects data from the device. This type of malicious software operates by first being installed onto a device through a malicious website, a file attachment, or a software download. After being installed, the software can track a user's online activity, login information, financial institution information, and/or their keystrokes. Once this information has been obtained, the spyware then sends the information to a third party, or directly to a criminal actor that could use the information for their own purposes. The stolen data can result in identity theft, damage to a device, or a disruption of a user's browsing experience.[1]

Spyware is a malicious type of software that can be installed onto your device without your knowledge or consent and collects data from the device.

Mobile devices can also be infected with spyware. Spyware installed on mobile devices may be able to track incoming/outgoing text messages and call logs, gain access to a device's microphone and camera, track a device's location, and track browsing activity.[2]

Although spyware is designed to work covertly on an infected computer, there are signs to look for that may indicate a computer has been compromised. Some signs of a possible spyware infection are:

- A hard drive running out of space;
- Experiencing frequent and ongoing pop-up ads;
- A browser redirecting a user to unwanted web pages;
- A user's homepage changing without permission;
- Programs being installed onto the device without the user's knowledge; and
- A user's browser installing new toolbars or plugins without the user's consent.[3]

If you suspect that your electronic device has been infected with spyware, the first course of action is to use your system's security software or third-party software to identify if spyware is present on the device. If spyware is detected, the use of a spyware removal program or application could be used to remove the infection. Some devices have anti-spyware software preinstalled. If not, a spyware removal program from a reputable source is recommended for removal. If programs or applications are unsuccessful in removing the spyware, a factory reset of the device may be appropriate. After removal, you may want to change your passwords and contact your financial institution to inform them that your information may have been stolen.[4]

Have you ever thought about what may be lurking within the files of your computer or electronic device?

In order to help protect yourself from a possible spyware infection, here are a few tips to help protect your electronic devices:[5]

1. Keep software and operating systems up to date with the latest security updates.
2. Stay away from unofficial software and application stores, and only download software from trusted sources.
3. Avoid clicking on links in text messages or email attachments when possible.
4. Be selective about granting permission for software to access your device.

Tips and reports of internet crimes can be submitted online to the FBI's Internet Crime Complaint Center.

[1] https://www.fortinet.com/resources/cyberglossary/spyware
[2] https://www.malwarebytes.com/spyware
[3] https://us.norton.com/blog/malware/spyware#
[4] Ibid.
[5] https://usa.kaspersky.com/resource-center/threats/spyware

Under Lock and Key: Data Encryption

An amazing advantage to the times in which we live is our ability to digitize data. Gone are the days when we are required to keep rooms full of files and folders (only sometimes even remotely organized!) as records of day to day business operations. Now, with a click of the mouse and perhaps a bit of mashing on a keyboard, we can easily bring up any record, including customer and employee data, communications and even financial reports. Even better: these records can be accessible through any computer connected to the business or agency network, making communication between different areas operate practically at light speed.

There is, however, a rather large downside to this ease of record keeping: security. Many of these records contain sensitive data, such as personal information of employees, bank account records, and other data that, in nefarious hands, could cause an agency or business real issues. Obviously, operations and privacy are massive concerns. In the age of the files and folders in a locked room, the only access is physical (and an ability to actually find what you want in a nonsensical filing system). Nowadays, someone with a little bit of know-how can breach networks and capture that data from elsewhere in the country, or even the world.

In the age of the files and folders in a locked room, the only access is physical (and an ability to actually find what you want in a nonsensical filing system). Nowadays, someone with a little bit of know-how can breach networks and capture that data from elsewhere in the country, or even the world.

Now, many who know a smidgen of how the tech world works would comment that our data is behind a lot of security – firewalls, password protection, closed networks, etc. However, the reality is that the world of cybersecurity is akin to an arms race. Tech companies that handle a lot of our operations release patches to known security holes, which hackers will find ways past, and which are then patched again. The cycle keeps continuing with no end in sight. The only certainty in cybersecurity is that nothing is ever truly secure. So, what can we do to further protect our data? The answer to that lies in encryption.

Simply put, encrypted data can only be read when the user has the correct "key" to decrypt it.[1] Compare it to cryptography in World War II. The enemy can see all the communication they want, but to read it they need to have the key to decrypt the seemingly nonsensical words. Otherwise put, the idea is that even if your data falls in the wrong hands, it cannot be read or understood.

The National Institute for Standards and Technology (NIST) is a government agency that provides standards of security.[2]

They published an encryption standard called the Advanced Encryption Standard (AES), which is used by all mainstream operating systems.[3] An encryption software using AES is highly recommended to protect data. The good news is that many programs and systems automatically use AES – such as VPNs, Wi-Fi, and components of operating systems.[4]

The only certainty in cybersecurity is that nothing is ever truly secure.

For more control over the encryption process, there are many trusted programs that can encrypt both data at rest (data on a hard drive or server) or data in transit (emails and the such). As a matter of fact, Windows comes with a built-in encryption tool, BitLocker. Mac OS uses Firevault and the Android operating system has its own encryption software built-in.[5]

These and other tools provide an extra layer of security in the event of a data breach. With encryption, we can feel better about scanning all those physical documents – once we can find them in that haphazard filing system.

[1] R. Johnson and C. Esttom, Security Policies and Implementation Issues.
[2] https://www.nist.gov/
[3] M. Goodrich and R. Tamassia, Introduction to Computer Security.
[4] https://cybernews.com/resources/what-is-aes-encryption/
[5] https://preyproject.com/blog/data-encryption-101

Revisiting an Old Foe: Ransomware

In the past decade, headlines abounded with stories of corporations and government entities being targeted by cyber criminals. Many of those stories involved criminal actors using ransomware to target their victims and elicit payment(s). Ransomware is malicious software that, after installation, gains access to files and systems and restricts the authorized users access to those files and systems.[1] Ransomware is not a new phenomenon and has a history dating back to the 1980s with the first well documented attack being the AIDS trojan.[2] [3]

The AIDS trojan was distributed on floppy disks in 1989 by Dr. Joseph L. Popp, an evolutionary biologist, to approximately 20,000 individuals and medical institutions. Dr. Popp gained access to these individuals and entities through the use of hijacked mail subscriber lists of the World Health Organization (WHO) AIDS conference and PC Business World magazine. The virus didn't encrypt the system instantly but instead used the Autoexec.bat file, which was used by Windows at the time to boot the system. The virus monitored the file for how many times the system was booted and after a certain number of boots, typically around 90, it would then encrypt file names including the operating system's files. This rendered the computer unusable. It would then display a ransom message demanding payment of at least $189 be sent to a P.O. Box in Panama.[4] [5]

In the past decade, headlines abounded with stories of corporations and government entities being targeted by cyber criminals. Many of those stories involved criminal actors using ransomware to target their victims and elicit payment(s).

Ransomware attacks took a backseat for about fifteen years until the mid-2000s when the internet became more prevalent and resilient. This was also the era when free email accounts were gaining popularity and phishing[a] became a major mode of attack. Around the advent of the cryptocurrency Bitcoin in 2010, ransomware attacks came roaring back to life and to the headlines of the news cycle. Bitcoin and other cryptocurrencies[b] have become so central to ransomware payments that major criminal actors sometimes go so far as to set up "customer service lines" to help their victims navigate how to purchase and send Bitcoin payments.[6] [7]

The late 2010s saw many of the major cyber-criminal actors switching methods from traditional ransomware to altered versions, one of those being data extortion. This method of attack exfiltrates the data from the victim's servers instead of locking them out from it. The criminal actors then threaten to sell or release the data if a ransom payment isn't made. This new attack method can also increase the potential number of victims. The criminal actors not only target the organization from which they stole the data but other organizations or individuals to whom the stolen data belongs.[8] [9]

November 2018 saw one of the most famous and damaging examples of this type of attack with the hack of the Finnish psychotherapy company Vastaamo. Thousands of patient files were stolen from Vastaamo's servers and the individual patients began receiving ransom emails demanding payment of 200 euros worth of Bitcoin, accompanied by a threat of releasing their records if they refused payment. The stolen database was discovered published on the dark web,[c] the company owners had their assets seized during the government investigation, forcing the company into bankruptcy in 2021.[10] [11]

Ransomware attacks continue to rise with no signs of slowing down.

Ransomware attacks continue to rise with no signs of slowing down. In 2022, the total number of attacks rose 80% and the number of data extortion ransomware attacks increased 500%. Since 2021, there has been a 78% increase in the amount criminal actors demanded for ransom.[12] [13] [14] Here are some steps to help mitigate against the threat of a ransomware attack.

1. Always update the software and security patches for computers accessing data and the servers which store it.
2. Create backups of the files and systems and store them separately from the primary systems.
3. Implement security controls to restrict access to sensitive systems to only those who need to use them, and use two-factor authentication.
4. Train staff to recognize threats such as suspicious emails and weblinks that have spelling errors or incorrect domains and to be careful with email attachments.

Additional resources can be found on the Stop Ransomware site provided by the Cybersecurity and Infrastructure Security Agency (CISA), a component of the Department of Homeland Security (DHS). They offer tips, guidance, guides, and other resources to assist with protecting against ransomware attacks. They also allow affected entities to report instances of ransomware and cyber-attacks. Attacks can also be reported to your local FBI Field Office and their Internet Crime Complaint Center (IC3).

[a] According to the Federal Trade Commission (FTC), "Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company."

[b] According to the FTC, "Cryptocurrency is a type of digital currency that generally exists only electronically. You usually use your phone, computer, or a cryptocurrency ATM to buy

cryptocurrency."

[c] As defined by Tulane University, the dark web is "an area of the internet that is only accessible by users who have a Tor browser installed."

[1] https://www.digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[2] www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

[3] www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware

[4] www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-aids-trojan-ransomware/

[5] www.makeuseof.com/aids-trojan-the-first-ransomware-attack-in-history/

[6] www.businessinsider.com/hackers-now-offer-customer-support-service-guarantees-and-perks-2016-1

[7] https://safr.me/blog/2016/05/28/ransomware-hackers-provide-customer-service-dept-to-victims/

[8] www.corvusinsurance.com/blog/a-chilling-campfire-tale-of-data-extortion-how-data-theft-happens-in-detail

[9] www.blackfog.com/shift-from-ransomware-to-data-theft-extortion/

[10] https://www.computerweekly.com/news/252496227/Hacked-Finnish-therapy-business-collapses

[11] https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

[12] www.itpro.com/security/ransomware/367624/the-rise-of-double-extortion-ransomware

[13] https://techcrunch.com/2022/11/18/combatting-ransomware/

[14] www.cfodive.com/news/cyber-extortion-surges-78-spread-ransomware-as-a-service/621133/

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**.

5 TOP THREATS FROM 2022 MOST LIKELY TO STRIKE IN 2023

https://www.csoonline.com/article/3688988/5-top-threats-from-2022-most-likely-to-strike-in2023.html

» In the newly released annual State of Malware report, cybersecurity firm Malwarebytes selected five threats that they consider to be archetypes for some of the most common malware families observed in 2022.

» The report contains potential threats and ways to protect your network, assets, and employees.

Analyst Note: It is important to remember, for better or worse, that cyber threat actors tend to rely on trendy sets of tried-and-true tools and tactics.

DON'T OVERLOOK SUPPLY CHAIN SECURITY IN YOUR 2023 SECURITY PLAN

https://www.techrepublic.com/article/supply-chain-security-plan/

» With cybercrime on the rise, many companies fall victim to viruses and malware that are inadvertantly passed to them by vendors and business partners.

» However, there are new third party risk assessment strategies, services and tools that can help identify security "weak points" in your company's supply chain.

Analyst Note: Considering the variety of reasons why a cyber threat actor may target a company's supply chain, it is important for companies to take the time to learn about and secure their "links" in the chain to the best of their abilities.

CYBERATTACKS AGAINST GOVERNMENTS JUMPED 95% IN LAST HALF OF 2022, CLOUDSEK SAYS

https://www.csoonline.com/article/3684668/cyberattacks-against-governments-jumped-95-inlast-half-of-2022-cloudsek-says.html

» The number of attacks targeting the government sector increased by 95% worldwide in the second half of 2022 compared to the same period in 2021.

- The increase in attacks can reportedly be attributed to rapid digitization and the shift to remote work during the pandemic.

  Analyst Note: The US, along with India and China, were reportedly the most targeted countries over the last two years.

MASSIVE AD FRAUD SCHEME TARGETED OVER 11 MILLION DEVICES WITH 1,700 SPOOFED APP

https://thehackernews.com/2023/01/massive-ad-fraud-scheme-targeted-over.html

- According to the fraud prevention firm HUMAN, the attack injected malicious JavaScript code into digital as creatives, which allowed the fraudsters to stack numerous invisible video ad players behind one another and register as views.

  Analyst Note: Botnets used in the pursuit of ad fraud have been a significant threat to the online advertising market in recent years.

MORE VULNERABILITIES IN INDUSTRIAL SYSTEMS RAISE FRESH CONCERNS ABOUT CRITICAL INFRASTRUCTURE HACKS

https://cyberscoop.com/vulnerabilities-industrial-conference-s4x23/

- Researchers have revealed details about flaws in industrial systems that could give hackers access to the most sensitive networks.

  Analyst Note: Since most critical infrastructure control systems were not built with internet connectivity in mind, integrating them into modern operational networks often leaves a variety of vulnerabilities open for exploitation.

MASSIVE ESXIARGS RANSOMWARE ATTACK TARGETS VMWARE ESXI SERVERS WORLDWIDE

https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

- Attackers actively targeted VMware ESXi servers unpatched against a two-year-old remote code execution vulnerability to deploy a new ESXiArgs ransomware.
- Tracked as CVE-2021-21974, the security flaw is caused by a heap overflow issue in the OpenSLP service that can be exploited by unauthenticated threat actors in low-complexity attacks.

  Analyst Note: Commonly used by many organizations, virtualization software makes an appealing target for cyber threat actors and should be kept patched and up-to-date.

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

TLP:RED	For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization *only*, they must specify TLP:AMBER+STRICT.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP:CLEAR	Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

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-1; FDLE SINs 1.1.1, 1.1.4, 1.1.6, and 1.2.2; and FFCSINs 11.1, 1.2, 1.3, 1.5, and 4.3