The Beacon

Florida Fusion Center #18-192 | Cyber and Critical Infrastructure Report | October 2018, Issue #17

Summary

Who Lives in a Pineapple Under Your Network?:

Find out how a sweet little device that was once used for penetration testing can trick you into giving up all of your information.

Wi-Fi Security Gets an Update:

WPA3 is finally here and it's a real cybersecurity treat. Learn what's new and how it works to keep sensitive information safe.

The Encrypt Keeper: End-to-End Encrypted Apps:

You may have seen some apps touting encryption for your SMS messages. What does this mean for your privacy and law enforcement?

HTTP vs. HTTPS: What's the Difference?:

What does the little green padlock next to the address bar in a web browser do? Here's what you need to know about HTTPS sites.

Passwords Managed: How to Keep Your Passwords Safe:

The first step towards good cybersecurity posture is a strong password.

Contents

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

Editor's Corner

Cyber Security Doesn't Have to be Scary

October is a month for scares and thrills, but staying safe online doesn't have to be frightful. The Department of Homeland Security has designated October as National Cyber Security Awareness month, and each week has its own theme and focus. Read on to learn more about each theme and for some ideas on how you can participate:

Week 1: October 1-5: Make Your Home a Haven for Online Safety

Incorporate teaching cybersecurity to children as a way to stay safe. Just like you teach on how to not talk to strangers and to lock your doors, teaching good cyber hygiene and awareness makes everyone safer. Now is a good time to check your privacy settings on social media and to make sure your newest internet-connected toy isn't giving out too much personal information over the web.

Week 2: October 8-12: Jobs in Cyber Security

It's estimated that in the near future there will be millions of unfilled cybersecurity positions, leaving many important systems vulnerable to scary cyber-monsters. It's never too early, or too late, to look into a rewarding career in cybersecurity. Many high schools, higher education institutions, and organizations offer training to get you started or expand your skills. This week seeks to motivate teachers, parents, and counselors on how they can guide students looking to make the leap into the cybersecurity field.

Week 3: October 15-19: Online Safety in the Workplace

Work cyber safety starts with you. Everyone shares the responsibility for keeping their organization's network safe, and as our personal lives become increasingly blurred with work life it has become more important than ever to be vigilant. This week focuses on ways we can increase security at work with awareness training, emphasizing risk management, resistance, and resilience.

Week 4: October 22-26: Safeguarding Critical Infrastructure

We don't often think of our water, electricity, public health, or communications as being entities that are affected by cyber threats, but they can be vulnerable. The nation has 16 critical infrastructure sectors, and a disruption to any of them can deeply impact our day-to-day lives. Week 4 emphasizes the importance of securing these systems as a matter of national security and transitions into November's Critical Infrastructure Security and Resilience Month.

This quarter's issue of the Beacon includes tips for keeping safe online. For more information on National Cyber Security Awareness Month, visit the Stay Safe Online site, powered by the National Cyber Security Alliance: https://staysafeonline.org/

BONUS!

Hidden somewhere in this issue of the Beacon is a Halloween Cyber Pumpkin! See if you can find it!

Cyber Threats

Who Lives in a Pineapple Under Your Network?

What is a Wi-Fi Pineapple?

A Wi-Fi Pineapple is a device that can spoof a Wi-Fi access point, impersonating a legitimate access point to intercept wireless traffic. Like most cyber-related gadgets, Wi-Fi Pineapples have two sides to their story. They can either be used to bolster your security or tear it apart. Hak5's product was originally created in 2008 as a means of conducting penetration testing.[1] Penetration testing is a form of ethical hacking that helps government agencies, companies, and private individuals keep their cyber-security on par with industry standards. The Wi-Fi Pineapple can "poke holes" into the security system of any cyber network in order to pinpoint weaknesses, allowing for issues to be rectified before they are exploited.[2] This kind of intrusion into a network is authorized by the agency or business entity, however, these tools can also be used for nefarious purposes. The Pineapple is easy for non-tech savvy individuals to use, as it is an all-in-one device and has its own app for Android that helps in device setup and updating.[3] Almost anyone with little to no experience in hacking that has an internet connection could control the device; this could be an issue as those without expertise could make mistakes or use it in an unfriendly manner.

How does it work?

Our phones have the ability to auto-connect to Wi-Fi networks that we have previously connected to. This feature is for convenience and labels the remembered networks as trusted. The Wi-Fi Pineapple can become a "hotspot honeypot," exploiting that auto-connect feature by using an SSID that is recognized by your phone, intercepting the connection, and performing a man-in-the-middle attack.[4] The hacker can then use other tools to manipulate traffic, or they can also initiate a "deauth attack" that disconnects the user's device from a legitimate network (such as at a coffee shop or office location) and reconnects it to the Pineapple.[5] The device is available for purchase to the public with no restrictions, and its easy-to-use interface and low cost make it

[1] https://www.makeuseof.com/tag/wifi-pineapple-protect/
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] http://www.eweek.com/security/wifi-pineapple-penetration-testing-tool-sparks-interest-at-def-con

an attractive starter option for many amateur hackers.[6] However, when used by a professional or someone with malicious intent, this device can cause significant damage.

What's the damage?

Without the knowledge of the individual being exploited, the Wi-Fi Pineapple essentially places itself in between a device and a safe network. It eavesdrops on data being transmitted, which can become an issue when online shopping or banking is involved, especially if the site is not using HTTPS encryption.[7] These man-in-the-middle attacks can take confidential information, such as passwords or emails.[8] While this device can improve security for everyone by helping to fix vulnerabilities, it also decreases the complexity of exploitation which causes every Wi-Fi Pineapple out in the world to become a threat towards unsuspecting individuals.[9] However hidden this kind of attack can be there are ways to increase your security and protect yourself from attack:

- Turn Wi-Fi off when you are not using it in order to avoid the issue of connecting to known networks.
- Always use a VPN when using a public Wi-Fi.
- Avoid sensitive websites such as online banking and shopping on public Wi-Fi.
- Check for HTTPS site encryption and do not ignore website certificate warnings.
- Stay alert when connecting to a network.[10]

Wi-Fi Pineapples can be both helpful and harmful, but with vigilance and the knowledge to protect yourself, the harm can be mitigated.

[6] https://www.pwnieexpress.com/blog/rogue-device-of-the-week-wifi-pineapple
[7] https://www.makeuseof.com/tag/wifi-pineapple-protect/
[8] Ibid.
[9] http://www.eweek.com/security/wifi-pineapple-penetration-testing-tool-sparks-interest-at-def-con
[10] https://www.makeuseof.com/tag/wifi-pineapple-protect/

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

Cyber Highlights

Wi-Fi Security Gets an Update

Wi-Fi protected access, or WPA is a series of security protocols used to protect users devices and information while connected to the server. Most Wi-Fi networks still run on a version of WPA from 2004 called WPA2, which has since become outdated and potentially leaves user's information vulnerable to hackers. However, the Wi-Fi Alliance, a worldwide network that handles any issues concerning Wi-Fi standards, announced this year that WPA3 is going to replace its outdated predecessor and usher in new innovations in Wi-Fi security.

One of the ways in which WPA3 will improve the security of Wi-Fi networks is by limiting a hackers' ability to guess your password through certain programs. With the current WPA2, a potential hacker can take information from your network while within range of the Wi-Fi network then go home and run the data through a dictionary-style program that guesses the password over and over until the password is guessed correctly. This is remedied with the new WPA3 software only allowing password attempts while within range and interacting with the network. The new security protocols associated with WPA3 are especially useful when using a password that is not very strong.

Another difference between WPA3 and WPA2 is the way WPA3 encrypts information. With WPA2, once a hacker has your Wi-Fi password, they would be able to view your old information with the compromised password. However, under the new WPA3 security protocols, old information will be protected by "forward secrecy." This means that as information is saved, it is encrypted for future storage, making it much more difficult for hackers to obtain old information once they figure out your password.

Smart devices are becoming much more prevalent every day, and WPA3 addresses this by adding in specific software to accommodate easier pairing with these gadgets. WPA3 manages to accomplish the quick pairing of devices by including a barcode on the device that the user only has to scan in order to connect it to the Wi-Fi network. This process is similar to capabilities provided under the previous WPA2 software but will patch several security concerns.

The final way WPA3 will improve overall security is by increasing the security of public Wi-Fi. Most people are guilty of compromising their information by connecting to public Wi-Fi which, until WPA3, has had very poor security features that were easily defeated by common hacking techniques. The data on public Wi-Fi is at risk because if a network does not require a password to join, most of your information will not be encrypted. This means that hackers could be sitting in the same public area as you and stealing your personal information. WPA3 will start encrypting these public Wi-Fi networks even if they are not password protected.

Wi-Fi security updates have been needed for several years now, but we also shouldn't expect to see WPA3 appear overnight. Manufacturers have started creating hardware that is WPA3 compatible but the Wi-Fi Alliance doesn't expect WPA3 to become widespread until late 2019. Even though all devices will eventually need to be upgraded in order to support WPA3, the Wi-Fi Alliance expects this to be a gradual change that will still support WPA2 in the meantime, meaning even the older devices will be able to connect to WPA3 routers and networks giving a grace period to upgrade all old devices.

https://www.theverge.com/circuitbreaker/2018/6/26/17501594/wpa3-wifi-security-certification
https://www.pcmag.com/article/362111/what-is-wpa3
https://www.wi-fi.org/discover-wi-fi/security

The Encrypt Keeper: End-to-End Encrypted Apps

In recent years cyber security has become the primary goal of many people all over the world, and for good reason. However, keeping personal information secure online has become a very hard task and many people are turning to end-to-end encrypted apps to keep personal conversations and information secure. So what exactly is end-to-end encryption? The term refers to software that makes sure only the sender and recipient of the message are able to read its contents on their devices. This encryption is done with specific apps that encrypt and decipher the message at both ends making the message undiscernible to anybody who does not possess the unique user key for that app.[1] Legitimate and legal uses for such apps include communications between employees of a business who need to protect intellectual property, members of government who require more discretion to their conversations, members of the media who need to receive information or protect sensitive sources, or even just citizens who value absolute privacy. In 2017, the U.S. Senate approved the use of an encrypted messaging app for staff use, meaning that despite the apps' mixed reputation there is still a need for absolute privacy.[2]

While the vast majority of people use these for lawful day-to-day communications, there have been many stories in recent years about how individuals have been able to use encryption services to aid them in the execution of unlawful activities. A notable example is the case of the individuals who attacked Paris in 2016. Officials in charge of investigating the terror attack say the attackers used popular encrypted apps such as WhatsApp and Telegram, both of which boast encryption for the sake of privacy.[3]

From a law enforcement perspective, apps and phones that use encryption may cause issues when investigating cases because of the level of difficulty in obtaining and deciphering the data, even if they have a warrant. When a smartphone is in a "locked"

[1] www.greenbot.com/article/3119449/android/the-best-messaging-apps-with-end-to-end-encryption.html.
[2] https://www.engadget.com/2017/05/17/us-senate-approves-signal-for-staff-use/
[3] https://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/index.html

state, all of the information on the phone is fully encrypted. Too many attempts at unlocking the device could result in the phone "wiping" the data, destroying it. While this type of software is built into modern devices to protect our data from thieves, it slows the process of investigating and can bring the case to a halt altogether.

Another useful purpose for encryption apps is that even server owners cannot access your information because it is encrypted. This is useful in preventing the service providers from accessing the information themselves for research or marketing purposes. While it is hard to calculate who is using these apps for what purposes (for obvious reasons), many are turning to it to protect their correspondences.

HTTP vs. HTTPS: What's the Difference?

With online commerce becoming more and more prevalent, issues of security and privacy online continue to grow in importance. When typing in a website's address, some users might not take the time to type "www", let alone check to see the website they are on is secured. The difference would look like this: "http://" vs. "https://". Although the difference of one letter can almost seem trivial, its impact and purpose is extremely important.

HTTP stands for hypertext transfer protocol and allows different systems to communicate with one another. Simply stated, it is a protocol that permits information to be passed back and forth between web servers and clients.[1] It is the most common protocol used for data transfers over the web. One important caveat to understand is that the data associated with HTTP is not encrypted. Encrypted data is information that is converted into a cipher, or code, with the intent for only users to have access to it. As a result, there is a higher risk of data getting intercepted as it travels between destinations.

Hypertext Transfer Protocol Secure (HTTPS) is the "protected" version of HTTP. The "S" stands for secure and ensures that all communication between an individual's browser and the website are encrypted. HTTPS uses one of two security protocols, either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). This allows for the connection to the website to be encrypted in order to prevent malicious actors from intercepting data. It should be noted that HTTPS information can still be intercepted, and even decrypted, but not as easily as HTTP traffic. This is usually done through Man-in-the-Middle attacks that spoofs the necessary certificates to decrypt the incoming information.[2]

HTTPS is used when there are highly confidential online transactions and was developed to allow for data to be transmitted securely. It is recommended that when making purchasing online to always be sure that the website is using HTTPS. This ensures that your information cannot be intercepted by hackers and also protects your personal identifying information (PII). Research conducted by GlobalSign found that more than 80% of respondents would not continue with

[1] https://www.instantssl.com/ssl-certificate-products/https.html
[2] https://www.quora.com/Can-HTTPS-traffic-be-intercepted

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

purchasing an item online if there was no HTTPS in use.[3]

In August of 2014, Google made an announcement that a page's HTTPS status will factor into its Google ranking and websites that fail to shift from HTTP to HTTPS will be ranked lower. As a result, more companies are heeding this announcement and making the switch to HTTPS in order to maintain their ranks with the search engine.

It's always good to make sure you aren't inadvertently giving away information while browsing the internet. Stay vigilant and watch out for the little padlock that keeps your information safe.

[3] https://www.brightlocal.com/2017/01/06/http-vs-https-website/
[4] https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https

Passwords Managed: Keeping Your Passwords Safe

Password strength is a necessity to ensuring your personal security. A strong password is one that is upwards of fifteen characters, does not contain personal information, and utilizes the entire keyboard. This includes incorporating numbers, symbols, special characters, and both upper and lower case letters. Passwords should also be different for each account or site you use. Using the same password and changing one digit or symbol each time you have to update it leaves you open to compromise. When creating or updating your password, avoid including your name, pet's name, or graduation year, as these are much easier to hack than a password consisting of random characters.

You may be asking at this point, "What can I do to ensure my password is unique?" The use of a password manager can assist in this area but keep in mind there are many pros and cons to their use. Password managers are software applications that are used to store

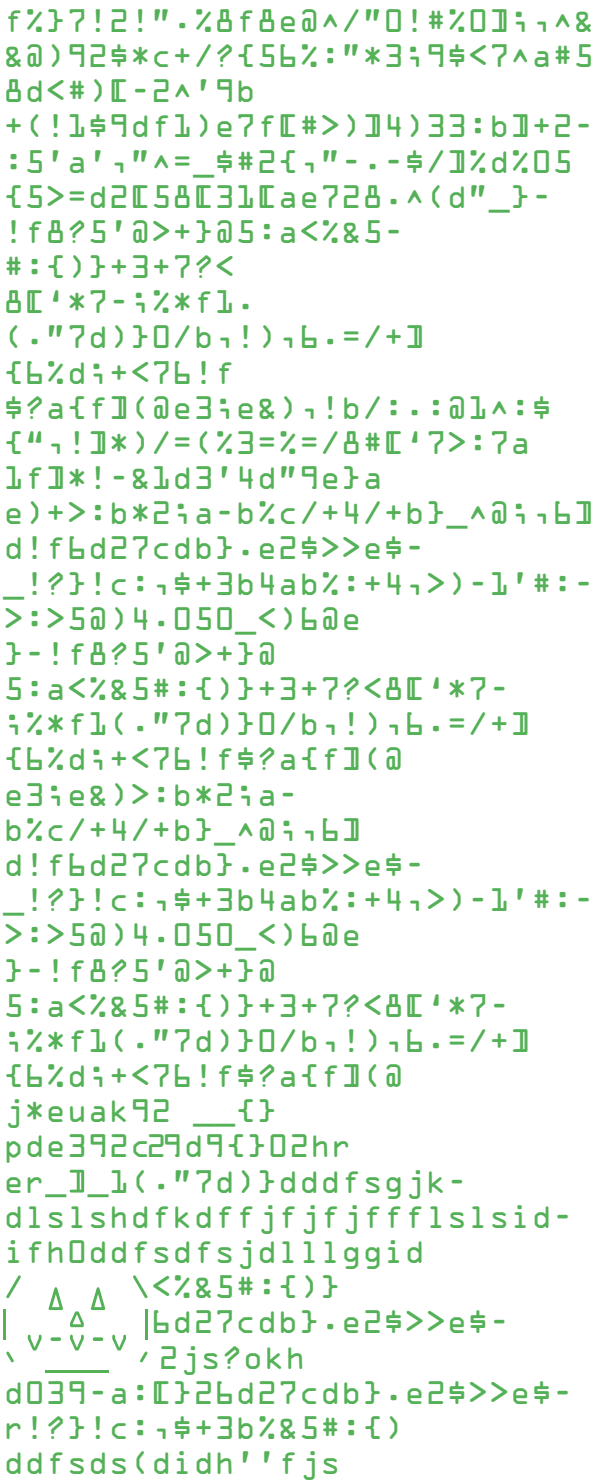
and manage a user's passwords. There are a variety of options available on the market to choose from ranging in price from free to a small fee per year.

Password managers store and encrypt multiple logins and passwords, meaning you only have to remember one login to access everything. For this reason, your log in to the application should be very secure. The password manager applications can also be used across multiple types of devices.

Keep in mind that a password manager service also puts all of your passwords in one place, which makes it a target for hackers. Several companies have had their databases successfully hacked in recent years, forcing many users to change all of their passwords. The choice is ultimately up to the user if the convenience is worth the risk.

Another best practice to fostering good password hygiene is to not let your applications or browsers remember and/or store passwords. This is one of the easiest ways for someone to get access to your logins. Always verify the web address you are accessing has https encryption in the URL. The https indicates a secure connection. If the URL does not have the "s" on the end of http (some websites might also display a little padlock next to the web address), you can request a secure webpage from the service provider that you can log into.

Managing password strength is a must to keeping you safe. Remember to avoid writing passwords down on paper and think outside of the box when generating a password to avoid the likelihood of someone compromising it.



https://www.comparitech.com/privacy-security-tools/password-strength-test/
www.marquette.edu/its/help/security/password.shtml
https://www.rit.edu/security/content/benefits-using-password-manager
https://its.ucsc.edu/policies/password.html
https://www.zdnet.com/article/onelogin-hit-by-data-breached-exposing-sensitive-customer-data/

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

Dispatch Highlights

This section highlights articles from past *FIPC Dispatches* that our analysts think are noteworthy based on trends we're seeing in Florida. *The FIPC Dispatch* is a list of open-source articles that is sent out twice weekly. If you are interested in receiving *The FIPC Dispatch*, **let us know.**

To sign up for the *FIPC Dispatch*, visit SecureFlorida.org and click the **Sign up for The FIPC Dispatch** link at the bottom of the homepage or send an email to **FIPC@fdle.state.fl.us**.

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

Polar fitness app revealed sensitive information about overseas soldiers

https://mashable.com/2018/07/08/polar-fitness-app-reveals-soldiers-homes/?utm_cid=hp-r-1#ZaCftPKbfkqR

- Fitness apps that track exercise use GPS to map routes taken while running or walking.
- A user can share their progress, including the route they took during a workout. Anyone who shares publicly can have their entire history accessed, revealing the layout of multiple locations.
- This feature has revealed the interior features of military bases overseas that can be accessed by anyone if the user published publicly.

Analyst note: Fitness apps have recently become popular and are a great way to track your health goals. It's not recommended to use the GPS feature, as that is a gold mine of data, but if you want to use it be sure to review your privacy settings so that you aren't sharing your jogging route with the whole world.sharing your jogging route with the whole world.

Is My Phone Recording Everything I Say?

https://gizmodo.com/these-academics-spent-the-last-year-testing-whether-you-1826961188

- A group of researchers spent a year running an experiment with more than 17,000 Android apps to see if any of them were secretly using the smartphone's mic to capture audio.
- There was no evidence that the apps were unexpectedly turning on the mic to record audio, but they did find that many of the apps were recording the phone's screen and sending that information to third parties.

Analyst note: Just because a phone might not be recording audio doesn't mean it's not tracking you in other ways. Be sure to turn off your location tracking, Bluetooth, and Wi-Fi when not in use and read permissions carefully before granting access to any app.

Facebook and Google accused of manipulating us with "dark patterns"

https://nakedsecurity.sophos.com/2018/06/29/facebook-and-google-accused-of-manipulating-us-with-dark-patterns/

- With the passing of the General Data Protection Regulation in the European Union, websites are required to be transparent about how they collect and utilize user data.
- Some large tech companies have been accused of using "dark patterns," (subliminal patterning) which make it harder for you to close accounts or trick you into clicking on advertisements.

Analyst note: This sort of subtle social engineering can be very hard to detect. Always be vigilant about what you're clicking on and read a site's security and privacy statements before signing up for anything; educate yourself as much as you can on the products you use.

$1 million heist on Russian bank started with hack of branch router

https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank/

- A group of hackers stole nearly $1M from a Russian bank after compromising a router used by a regional bank branch office.
- The group infiltrates a network and then lays low for a few weeks before using their "fileless" malware to steal money.

Analyst note: Routers are the entry point for an entire network, and if that entry point is breached, the whole network can be compromised. This is a good time to make sure your router is properly secured with a strong password and behind a firewall.

Facebook users are changing their social habits amid privacy concerns

https://www.engadget.com/2018/09/05/facebook-changing-social-habits-privacy-concerns/

- A survey says half of US users adjusted their privacy settings last year.
- Younger users (ages 18 to 29) were more likely to have either deleted the app or changed their privacy settings than older users (65 and older).

Analyst note: Privacy settings should always be your first stop after signing up for a new social media service and before you post anything. The recent breaches in user trust by some large platforms serve as a great reminder to check that you aren't sharing more than you think you are.

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):

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

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.

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

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

THE BEACON

Editing by: Ashley Grover
Designed by: Maria Olivella

October 2018

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

Information Resources

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. The FIPC is a team of cyber intelligence and critical infrastructure analysts who work to protect Florida's infrastructure.

SecureFlorida is an Internet safety and awareness outreach effort of the FIPC. Designed for the majority of computer users, Secure Florida covers all areas of computer, network, and communication security.

To sign up for alerts and other notices, **visit www.secureflorida.org/members/signup/**

The Beacon

The Beacon is published quarterly by Secure Florida to highlight cyber and critical infrastructure security information and awareness. **The Beacon** seeks to provide privacy and security information to all Internet users.

To read issues of **The Beacon**, visit **www.secureflorida.org/news/the_beacon/**

To sign up for **The Beacon**, visit **www.secureflorida.org/members/signup/**

The Dispatch

The FIPC Dispatch is compiled twice weekly by cyber intelligence analysts in the Florida Fusion Center. The content is intended as an informative compilation of current open-source cyber news for law enforcement, cyber intelligence, and information security communities.

To join **The Dispatch** mailing list, write to **FIPC@fdle.state.fl.us**

The **CSAFE** effort provides Internet safety presentations for organizations, clubs, schools, and businesses anywhere in Florida. For more information, visit **www.secureflorida.org/c_safe**

Class topics include:

- Best Practices for Internet Security
- Family Online Safety
- Combating Cyberbullying
- Online Safety for Seniors
- Identity Theft
- Mobile Communications
- Email Safety
- Internet Laws & Regulations