The Beacon

Florida Fusion Center | Monthly Cyber and Critical Infrastructure Report | July 2014 Issue #3

Summary

The Story Behind The Beacon — We started this publication with the desire to protect the citizens and economy of Florida by safeguarding our information systems and reducing our vulnerability to cyber attacks.

Hashing — We have started *hashing* this publication in order to add a layer of security for our readers.

Citizen Issues — Scammers are pretending to be law enforcement officers in order to coax victims into paying fake fines using prepaid payment cards.

Why Hash? — Hashing files is a way to verify their integrity. We started hashing this publication in order to add a layer of protection for our readers. This article explains why hashing is important and how you go about checking a hash.

Mobile Devices: Living on the Edge — The onslaught of mobile/smart devices has complicated security efforts by increasing opportunities for hackers to get your information.

Do You Really Have to Give Up on Windows XP? — Yes.

The Physical Side of Cyber Security — New technology increasingly ties the physical security world to the information technology world. This new convenience creates security concerns for both information security and physical security professionals.

Viewing Schools as Critical Infrastructure — When people think about critical infrastructure schools do not come to mind. However, school closures have a major impact on lives and day-to-day community activities.

Contents

About *The Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness.

Secure Florida is an Internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC). The FIPC 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 protection analysts. FIPC analysts work to protect Florida's infrastructure through FDLE's Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

If you see a topic where you would like more detailed reporting, or have seen something you think we need to know about, **Let Us Know.**

The Secure Florida Beacon welcomes your feedback.

https://www.surveymonkey.com/s/SFBeacon3

Contact SecureFlorida.org at:
(850) 410-7400
Admin@SecureFlorida.org

Editor's Corner

The Story Behind The Secure Florida Beacon

Here in the Florida Fusion Center, our cyber analysts have a two-fold job. We work to interpret and disseminate cyber intelligence to law enforcement, and we raise awareness of information security and Internet safety to everyday computer users.

We established and maintain the Secure Florida initiative and the Florida Infrastructure Protection Center in an effort to protect the citizens and economy of Florida. Our week may find us working with the Department of Homeland Security on a nationwide cyber initiative one day and then speaking to a group of middle school students about cyberbullying the next.

To accomplish our mission we strive to be a liaison between the average computer user and the larger realm of the proverbial good, bad, and ugly of cyber actors. We have at our disposal numerous information channels that we work and interpret to provide average computer users with the knowledge they need to stay safe.

Almost everyone uses some sort of computer. Most people do not have drug problems, terrorist plans, or ties to organized crime. However, the same Internet that a nation state cyber spy uses to steal state secrets connects your grandmother to Facebook. Anyone who has an Internet-connected computer is a target.

We work to equip any and all in our effort to protect the citizens and economy of Florida by safeguarding our information systems and reducing our vulnerability to cyber attacks.

We Started Hashing the PDF…

In an effort to add a layer of security to *The Secure Florida Beacon*, we have started to "hash" the PDF before distribution. To see the official file hash for the document go to www.secureflorida.org/hash. If you are wondering what a hash is and how it is a security feature, see the "Why Hash?" article in this issue to learn more.

See this picture of a cat walking like a boss. The picture on the left is the original. In the picture on the right we changed one pixel from its original color to white. Look closely just below the cat's right forepaw. Changing a single pixel produced two completely different hashes in both of the hashing algorithms we used.

MD5: bc8479a4143d3485df753bee6614bf17
SHA1: 81f73ac1dce53763c51ee9637c3153bcc68c2516

MD5: d5ade2d6069261621b63958f9ebed575
SHA1: 17ec632d491ace238d556882eff10ac5006fe6f3

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7400
Admin@SecureFlorida.org

Citizen Issues

Florida Fusion Center cyber analysts regularly receive citizen concerns and complaints. These calls vary greatly, but here we present developing trends.

Scammers Pretend to be Law Enforcement Officers

Recently, numerous calls came to Florida Fusion Center cyber analysts from citizens complaining of phone calls, email, and malware reportedly from law enforcement personnel. Potential victims were told that they have unpaid fines, failed to report for jury duty, or owe taxes. Another variant involves victim's inadvertently loading malware on their computer that claims they have done something illegal with the computer. In each version of this activity, scammers request that the victim wire money or purchase some form of prepaid payment card such as a Green Dot card. The scammer then asks the victim to send them the number on the card so they can withdraw the money.

In this scenario scammers impersonate law enforcement to pressure victims to pay fines by threat of arrest. While this method seems farfetched, many victims do not realize that law enforcement does not collect fines in this manner.

There are variations of the scam. In one instance, an elderly victim received a telephone call from someone claiming to be an officer from a Florida law enforcement agency. The scammer provided a false name and badge number, directing the victim to purchase a Green Dot Card in order to "assist law enforcement with a sting operation." The victim followed the instructions of the scammer out of a sense of civic duty and because he believed he was dealing with a real law enforcement officer.

If you receive this type of call or email, you should not provide any personal information. Ideally, you should get as much information as possible from the caller, such as a call back number, and then contact your local law enforcement agency to report the incident.

Contents

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

Cyber Highlights

Cyber Highlights represent issues cyber analysts have seen active in Florida. The following articles are intended to serve as overviews of issues we feel the citizens of Florida would benefit from knowing.

Contents

Why Hash?

To add a layer of protection for our readers we have started "hashing" this publication before distribution.

Hacking your computer does not require the classic energy-drink-addled hacker. Truth, to the contrary, is less dramatic. Breaking into your computer may simply require getting you to open or click on a "weaponized" email attachment.

Weaponized File Attachment

- Malware that is hidden in file attachments and programmed to run silently when the attachment is opened.

Security awareness teaches that you should never open an attachment from someone you don't know. But, is it possible that you can still get a weaponized email attachment from a trusted source? The short answer—yes. Curious? Keep reading.

Consider this: an email arrives from a colleague containing a PDF of an important report. Some time later, you get the same PDF forwarded from another co-worker. Now, with two copies of the same report in your inbox which one is the original? How many stops did that second copy make before it got to you? Is it possible that someone somehow got a copy of that report, somehow weaponized it only to re-inject it into the office mail flow?

How would you know if the second attachment were the original unadulterated PDF? The documents look the same; nothing, but the file size, has changed. But, would you even look that closely? Turns out malicious email attachments prove very effective. If I did my job well as a hacker, I just slipped a piece of brand new malware on to your computer that your anti-malware program may not recognize.

For context, are you reading this document on a piece of paper that you got from FDLE? Chances are, no; we actually print very few of these. You likely opened this as an email attachment or clicked a link to download it. How can you tell if this is the original version of this publication?

One way to verify the integrity of an attachment is by using a hash to verify that no one has altered the file. **Hashing uses an algorithm to generate a unique string of letters and numbers to create an abbreviated representation of each bit of a file.** The algorithms used are so precise that changing one bit in the file will create an entirely different hash.

If you are not familiar with the hash verification process here is a step-by-step process you can use to verify the authenticity of this document.

1. If you do not have a hash verification tool go to Google. Search: "hash verification tool" and find one from a trusted source.
2. Using your hash verification tool hash the PDF file you wish to verify.
3. Match the alphanumeric hash your tool created to the MD5, SHA1, or SHA256 hash we have published at www.secureflorida.org/hash

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

Mobile Devices: Living on the Edge

On April 3, 1973, Motorola employee Martin Cooper made the first cell phone call from a street in midtown Manhattan. Since that day in 1973, mobile phones have dramatically decreased in size while becoming increasingly sophisticated handheld computers. As of February 2014, there are an estimated 4.5 billion mobile phone users. At this point, the mobile phone industry has grown such that half the world has one and the majority of time it seems like their owners use them for everything but phone calls.

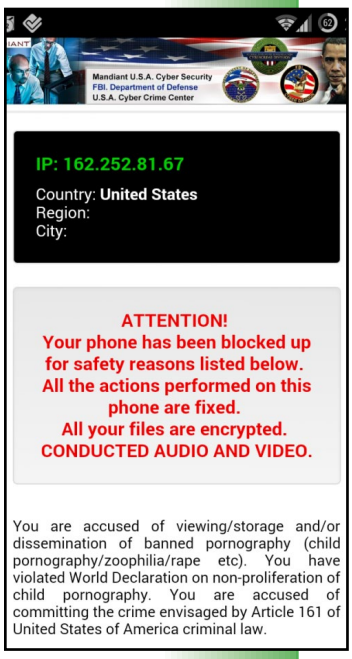
While mobile phones offer great convenience, what about their security? As mobile phone popularity grows and phones become smart, so do the number of malicious programs targeting the devices. Smart phone malware sophistication grew from annoying early worms like the SMS "Timofonica" to exceptionally troublesome ransomware Trojans identified in 2014. In January 2014, SecureList reported the detection of 143,211 new modifications of malicious programs targeting mobile devices in 2013.[1] The popularity of mobile devices has created a fertile environment in which criminals target a large number of systems where security is far from the mind of the user.

In early 2013, Kaspersky Lab maintained that 99% of newly-discovered mobile malware targets Android devices. The bulletin reported that there are three main types of Android malware: SMS Trojans, advertising modules, and root access exploits. The SMS Trojans are the most widespread; however, the root access exploits tend to be more damaging.

Symantec discovered a bogus Android antivirus Trojan called "Fakedefender" in June of 2013.[2] The malware worked by displaying a message designed to convince the user to purchase an antivirus app that could remove the bogus malware found on the phone.

Apple iOS is not immune from target by malware writers. In July 2012, Kaspersky's Lab found a Russian app called "Find and Call," designed to upload contacts from victim phones to a remote server.[3] The server then sent out SMS spam to the collected contacts, marking the first time a malicious app successfully completed Apple's App Store approval process.

In early 2014, a ransomware called Android.Trojan.Koler.A effectively locked an infected device by repeatedly displaying a message demanding payment to "unlock" the device. In addition, the message falsely claimed that the malware encrypted files on the device.



"Simplocker," or Trojan-Ransom.AndroidOS.Pletor.A, is a newly-discovered malware created specifically for Android devices. Simplocker is very concerning, in that it successfully encrypts files stored on the device, including the SD card.

The age of innocence is over when it comes to mobile device applications and malware. The next time you find a new app, think twice before you install it. You could very well be the first victim of the latest mobile device malware. Maybe not, but know that the world is changing as more mobile devices enter the market.

It pays to spend some time researching apps before you install them. Go to Google, see what people are saying, be suspicious, and verify. It could save you the headache of having to reset your device after losing your data.

[1] https://www.securelist.com/en/analysis/204792326/Mobile_Malware_Evolution_2013

[2] http://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99

[3] https://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

Do you really have to give up on Windows XP?

Sorry, but yes.

Everybody loved Windows XP!

Well…at least after Service Pack 2 we did. Before that, all Windows products had the same cycle. We hated it—they tweaked it. We hated it less—they tweaked it more. Finally, we were willing to work with it…and Microsoft discontinued support. Only then did we declare our undying love. (Note, please, that with Vista, all bets are off.)

And yet, after 13 years of use, XP really did seem like the Windows workhorse. Not since 3.11 did so many people come to depend on a Windows operating system (OS). Now that Microsoft is no longer supporting XP, users must move to another Windows operating system.

But XP still works just fine – why not keep it?

Simply because, as of April 8, 2014, Microsoft no longer supports it. That means not only does it withdraw its technical support; it also no longer issues patches to fix newly-discovered XP vulnerabilities. And there WILL be vulnerabilities. Anyone currently using XP is already using an OS with two months' worth of vulnerability discoveries, each of which may lead to a new exploit for hackers. As XP ages, it will be less and less secure and hackers will soon "own" it. Which means they might own your computer and all your data as well.

How difficult is it to install a new operating system?

Note: Back up your files before attempting any operating system upgrade!

It's not technically difficult, but it involves a lot of steps and is time consuming. Microsoft has provided step-by-step instructions, covering everything you need to know about installing Windows 7.

http://windows.microsoft.com/en-us/windows7/help/upgrading-from-windows-xp-to-windows-7#T1=tab01

You might decide to let a computer professional do it for you. However, *The Beacon* staff encourages you to try it yourself, because the very act of installation will likely teach you a lot about how your OS works.

Is the Windows 7 upgrade free?

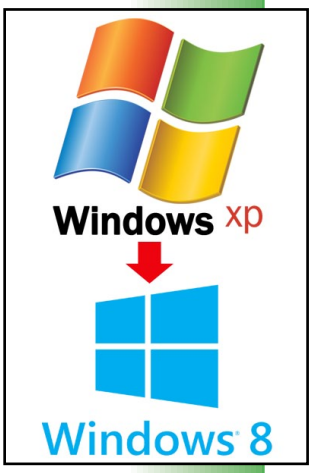
Unfortunately, no. The cost of the upgrade can vary significantly, depending on where you purchase it, and which edition you get. The vast majority of people will be happy with the Home Premium edition, with online prices of around $70. Before you commit, make sure you know which edition is right for you. CNET has provided a chart that makes the decision easy.

http://www.cnet.com/news/which-windows-7-is-right-for-you/

You keep talking about Windows 7. What about Windows 8?

Seriously? How can they issue a version with no Start Menu?!

Seriously, Windows 8 has gotten a bad rap that it probably doesn't deserve, especially with the 8.1 upgrade. The main problem is that the user interface is designed to work well with both a PC and a tablet, and the drastic change in format makes many users uncomfortable (*cough*the author*cough*).



Here are a couple of articles from Lifehacker that help with a number of questions.

http://lifehacker.com/5955229/why-does-everyone-hate-windows-8-should-i-upgrade

http://lifehacker.com/5954904/how-to-prepare-your-computer-for-windows-8

The cost to upgrade to 8.1 is a little higher than for Windows 7, but with some online searching, you can find a good deal.

Will I have to buy a new computer?

If your current computer is several years old, you will probably have to buy a new one, or at least upgrade some of your components. Keep in mind that the "minimum" requirements are just that—minimum, and your computer will operate adequately. If you want a faster machine, you will need to invest in an upgrade.

SecureFLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7400
Admin@SecureFlorida.org

BUSINESSAFE

Critical Infrastructure

Contents

BusinesSafe has a whole new look!

The *BusinesSafe* program provides business owners with information pertaining to the safety and security of their businesses, timely safety tips, and opportunities to learn more about specific preparedness techniques. Businesses can sign up to receive alerts and advisories via email or text message.

We have been working hard to update the content and provide relevant and up-to-date information. In addition to the alerts and suspicious activity indicators you have received in the past, we will provide resources outlining protective measures for businesses shared with us from our partners.

If your agency has an information page or site designed to provide warnings, tips, or best practices for businesses, please share it with us so we may feature it on our *BusinesSafe* site.

Come visit us! www.secureflorida.org/businessafe

The Physical Side of Cyber Security

Focus: Security Management

In the past, security managers overseeing physical access, surveillance, and safety training never had to consider cyber security. However, developments in security technology dictate that physical and cyber security personnel must work together to defend their realms. Modern security components regularly exist on some form of Internet connected infrastructure. As security hardware has changed in recent years, security policies have largely failed to keep pace. It is common for physical security personnel and cyber security personnel to be "stove piped" by policy and organizational structure. This divide can cause security gaps.

In April 2014, the security-consulting firm Red Tiger reported that many critical infrastructure facilities they evaluated did not have well integrated physical and cyber security personnel. In fact, they found physical and cyber security management often worked independently and were not communicating with one another. Red Tiger noted, "In one of our recent projects, we were able to leverage RFID technology to physically walk into very sensitive data centers, corporate offices, industrial sites, and engineering labs. Physical access allowed our team to directly connect our laptops to computer networks that would normally be behind firewalls."[1]

[1] http://www.redtigersecurity.com/serve_content.cfm?Page=Briefings-April2014

SecureFLORIDA.org

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

The Business of Federal Technology recommended in an article published December 2013 that a "unified cyber security program would enable organizations to leapfrog a decade of incremental progress." While the focus of their argument was specific to federal IT, this concept may be implemented down to the smallest agency or business. "Consolidation increases technology's total return on investment, capitalizes on innovative technologies and processes to achieve department and mission objectives, and uses data analytics to make more informed strategy and process decisions."[2]

The IT department, as well as building security, and risk management, must create all-inclusive safety, security, and emergency management policies by working in concert. Regular meetings between the different groups insure a unified approach to physical and information security efforts. Physical security managers not only need to understand what and where the vital cyber assets are, but how their own systems (electronic door locks, camera systems, etc.) are vulnerable to cyber exploit.

2 http://fcw.com/Articles/2013/12/19/DrillDown-Converging-physical-and-cybersecurity.aspx?Page=2

Viewing Schools as Critical Infrastructure

People hear *critical infrastructure* and they envision power and water plants, telecommunications centers, and roadways. But, what about schools as critical infrastructure? They might not represent lifeline infrastructure services but they do perform an exceptionally critical service.

Schools tend to be high occupancy facilities making them attractive physical and cyber targets and particularly prone to natural disaster. When disasters strike schools and render them inoperable, how broad is the effect? How will continuity of services continue to the community? What are the economic and psychological consequences of a loss? Is the facility a desirable target for malicious actors?

School closures have a ripple effect through the community creating childcare challenges that tend to cascade into the work force. The potential for community impact increases the longer a school is closed. Florida's schools are particularly vulnerable in that they have the highest average elementary and middle school enrollment per school in the nation, with public high school enrollment nearly twice the national average according to data published by the National Center for Education Statistics.[3] School

3 www.fldoe.org/eias/eiaspubs/word/enroll1112.doc

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

facilities house large numbers of students and staff for one-third of each day, five days a week, for a large portion of the year.[4]

School protection efforts require robust multi-discipline planning such that school administrators must work with fire departments, health officials, emergency management personnel, law enforcement, and, increasingly, information security personnel when planning for potential disruption.

Consider the impact potential:

Pandemic: One third of Florida's population lives in a three-county area in the southeastern corner of the state. The region's demographics, geographic characteristics, and population density make it particularly vulnerable to the spread of infectious disease.[5] In April 2009, the Department of Health and Human Services (HHS) issued a nationwide public health emergency declaration in response to the H1N1 virus. Florida followed with a Declaration of Public Health Emergency in May. The following Fall, Florida school districts braced for anticipated absenteeism rates of 30 percent, with the possibility of completely closing schools to limit the spread of the flu. Additionally, the Centers for Disease Control released guidance to businesses to help address employee absenteeism related to school closures.

Natural disasters: Enterprise High School, hit by tornado March 1, 2007, took more than three years to rebuild at a cost of $86 million.

Gun violence: One study estimates average societal cost of a single gun homicide at $5 million when factoring in lost work, medical care, mental health treatment for survivors, criminal justice expenses, employer losses, pain and suffering, and lost quality of life.[6]

Information Security: High population density in schools makes them likely targets for hackers. Information technology infrastructure in education facilities potentially houses a wealth of personal information, numerous public facing websites, and intellectual property related to research and development at colleges and universities. In October 2012, hackers stole about 76,000 student records from a college in Florida's panhandle, and an additional 200,000 records for students across the state.[7]

---

4 **Department of Homeland Security, National Infrastructure Protection Plan, Government Facilities Sector, Education Facilities Subsector Annex, 2007.**

5 http://www.floridahealth.gov/diseases-and-conditions/influenza/pandemic-influenza.html

6 http://www.bloomberg.com/news/2012-12-21/shootings-costing-u-s-174-billion-show-burden-of-gun-violence.html

7 http://www.wctv.tv/news/headlines/Massive-Security-Breach-Involving-Nearly-300000-Records-173632551.html

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7400
Admin@SecureFlorida.org

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**.

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

Contents

Risky Business: Protecting US Energy Supplies

http://www.cnbc.com/id/101534808

Summary:

- The energy industry's delivery systems are vulnerable to attack and disruption.
- Cyberattacks are eclipsing terrorism as the primary threat facing the United States.
- Defending North America's sprawling and complex power grid from cyberattacks is difficult.

Analyst Note: The power grid, like nearly all of the utilities we depend on daily, rely on intricately networked and highly automated systems. Systems, by their nature, are vulnerable to failure. This article highlights the need to defend the increasingly interconnected systems that maintain efficient delivery of utilities. Disruption of lifeline utilities by cyber-attack is an increasingly real possibility.

Heartbleed's Silver Lining: New Passwords!

http://www.computerworld.com/s/article/9247975/Heartbleed_39_s_silver_lining_New_passwords_

Summary:

- Internet users who previously did not consider their online passwords are now changing them.
- The Heartbleed scare may have made computer users smarter about security.
- Heartbleed got account security into the forefront of people's minds; however, it may have been temporary.

Analyst Note: Heartbleed was easily the most significant information security story in recent years. The silver-lining to Heartbleed was the attention it caused people to pay to their passwords. Many finally understood the importance of using different passwords on different accounts. While such a breach represents a costly disruption and that is scarcely a good thing, we figure you take the good where you can get it.

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever

http://www.wired.com/2014/04/dark-wallet/

Summary:

- Government regulators around the world are scrambling to prevent bitcoin from becoming the currency of choice for money launderers and black marketeers.
- A collective of politically radical coders released a bitcoin application designed to better protect bitcoin user identities.
- Bitcoin software records every transaction in a public ledger, known as the Bitcoin Blockchain, not offering the anonymity that many bitcoin users desire.

Analyst Note: Bitcoin is relatively new, trending toward volatile, and presently unregulated. As such, almost no one fully understands the intricacies that make the system work. This article highlights the fog surrounding bitcoin. The fact that there is a market for further anonymizing an already nearly anonymous currency indicates that law enforcement will see bitcoin increasingly in the coming years.

Iranian Spies Pose as Reporters to Target Lawmakers, Defense Contractors

http://www.wired.com/2014/05/iranian-spying/

Summary:

- Iranian spies appear to be engaged in an effort to collect intelligence by duping lawmakers, journalists, and defense contractors into revealing information.
- By using fake accounts on popular social network sites the attackers built an elaborate network of fake personas to gain the trust of their targets.
- The attackers have targeted members of the U.S. military, Congress, and various think tanks, along with journalists, defense contractors in the United States and Israel, and members of U.S. and Israeli lobbying groups.

Analyst Note: This article highlights cyber espionage believed to be the effort of Iran. However, it is a good example of tradecraft used by many nation states and groups to collect information via publicly available social networks. This type of activity works because so many people do not realize that their jobs make them a target. For the most part, few suspect that they would be the target of an Iranian espionage campaign. Truth is, it is hard to determine; you might be a target simply because you represent a foothold in your organization.

Help us improve *The Beacon*. Please take a moment to complete our survey.

https://www.surveymonkey.com/s/SFBeacon3

The Beacon | Editor: Kevin Wiggins | Design: Chris Kenworthy

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org