The Beacon

Florida Fusion Center #16-143 | Cyber and Critical Infrastructure Report | October 2016 Issue #11

Summary

Securing the American Election - America is electing a new president, which makes the elections system an attractive target for hackers.

(Hacking) From Russia With Love - Russia has allegedly been behind some recent high-profile hacks against the US. We discuss how this matters.

GovRAT V2.0: Time to Call the Exterminator - A nefarious new type of malware has been targeting governments. We tell you what it's all about.

Android: App Permissions Made Simple - Mobile apps often require numerous permissions. Do they put you at risk?

Why Phish When You Can Whale? - A twist on the phishing email is on the rise; so how can you protect yourself?

What Phishing Emails Mean for You - Some new trends and risks associated with the traditional phishing scam.

Type Basics - We work hard to ensure content is delivered effectively and attractively. Here are some tips we've picked up along the way.

Contents

About *The Secure Florida 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).

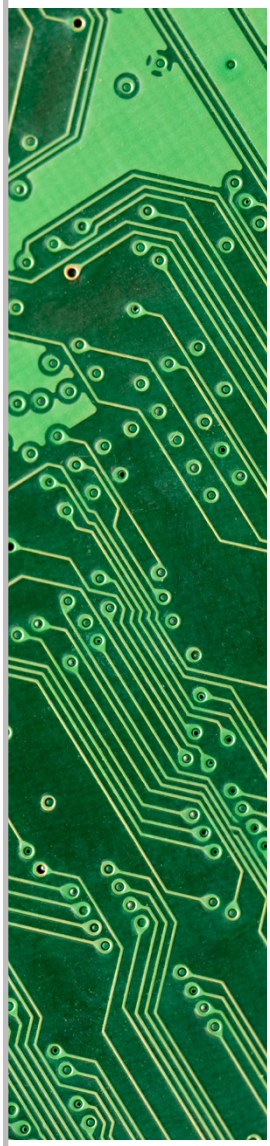
The Florida Infrastructure Protection Center (FIPC) was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters.

Contact Secure Florida at:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Editor's Corner

Cyber Security Awareness Month 2016

This October has once again been designated by the Department of Homeland Security as National Cyber Security Awareness month. The month comprises weekly themes, each addressing a different aspect of cyber security:



Week 1: *STOP.THINK.CONNECT.: The Basic Steps to Online Safety and Security*

1 The first measure to protect yourself online is to pause and think before you click, connect, or download. We should all take care to know the best practices for staying safe online.

Week 2: *From the Break Room to the Boardroom: Creating a Culture of Cyber Security in the Workplace*

2 Organizations large and small, public and private, use computers and the Internet every day. This means they can be targets of malicious actors for data theft or other cybercrimes. This week focuses on ways everyone in the workplace can keep their organizations safe.

Week 3: *Recognizing and Combatting Cybercrime*

3 Criminals are increasingly seeing the Internet as a vehicle to commit crimes of all kinds. Whether it's stealing personal information, cyber-bullying, state-sponsored hacking, or child exploitation, citizens should be aware of the different types of cybercrimes and the steps you can take to protect yourselves or to report crimes when they occur.

Week 4: *Our Continuously Connected Lives: What's Your "Apptitude?"*

4 Technology has evolved so that we are constantly connected to the web. It is essential to keep abreast of the privacy and security issues that accompany 24/7 access via mobile computing and the Internet of Things.

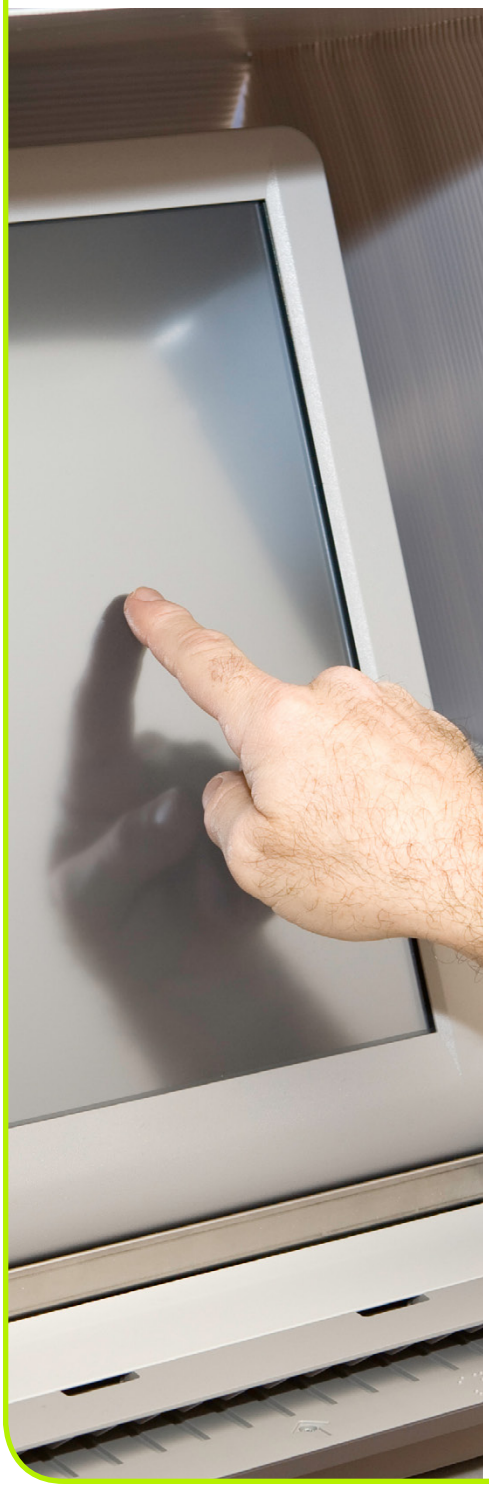
Week 5: *Building Resilience in Critical Systems*

5 It's not just desktop computers and smartphones that access the Internet; many critical infrastructure systems also use the Internet to function normally. This access makes them prime targets for malicious actors, and this week highlights ways to ensure these systems stay secure.

This month's issue of the Ledger contains articles that discuss issues related to each of these themes, as well as ways to increase your cyber security. For additional resources, or to learn more about National Cyber Security Awareness Month, please visit https://staysafeonline.org/ncsam/.

Cyber Threats

Securing the American Election



The upcoming November presidential election has sparked a renewed interest in a number of topics that have implications for our country's national security. One of these issues is the actual process through which voters across the US may submit votes electronically through each state's voting systems.

Over the past year, three states have already reported compromises to data within their election systems, affecting several hundred thousand records.[1] These compromised databases housed voters' names, addresses, sex, and birthdays in addition to other information. Some of the records across these incidents include either four digits of a voter's social security number or even drivers' license numbers. Much of this data, despite dating back ten years, is likely still in use today.[2]

According to an alert issued by the FBI,[3] unknown actors used widely available hacking tools, including Acunetix, SQLMap, and DirBuster, to infiltrate these systems. The FBI traced the attacks to eight IP addresses, which appeared to originate from companies based in Bulgaria, the Netherlands, and Russia.[4] However, it has been difficult for government officials to attribute these attacks to specific entities, identify if they were state-sponsored, or conclusively determine a motive. A number of foreign actors have claimed responsibility for these intrusions.

Because of these attacks, there is more attention on how the two presidential candidates plan to address recent cyber failures so that they are not doomed to repeat them. It is logical for the public to conclude that if foreign actors are capable of exfiltrating data on thousands of American citizens, there is a chance they can interfere with the actual process of deciding our next leader.

Florida is tied for third place (with New York) in the greatest number of electoral votes in the country. Given the

[1] http://www.washingtontimes.com/news/2016/aug/29/election-systems-hacked-in-illinois-arizona-the-fb/

[2] http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/

[3] http://www.washingtontimes.com

[4] http://www.csoonline.com/article/3117647/security/election-exploits-what-you-need-to-know-infographic.html?upd=1473368716243

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

significant number of votes, along with our state's checkered past in contributing an accurate voter count (think Bush/Gore 2000), it is likely that all eyes will turn toward Florida this November as a potential swing state to ensure that all systems are secure.

Vulnerabilities in our election systems are now at the forefront of open source reporting and have led a number of organizations to begin making improvements in their cyber security. Since we are now just weeks away from the general election, officials hope that there is sufficient time to implement best practices or new safeguards.

Additionally, the Department of Homeland Security (DHS) is considering adopting our country's election systems as a sector of "critical infrastructure." This proposal is a direct result of the above incidents as well as others directed at other US entities. This change would elevate these systems to the same level of priority that other critical infrastructures receive, such as electrical systems and financial services. However, voting systems are primarily the responsibility of their applicable state and local governments, and many of these systems operate using paper ballots. According to DHS Secretary Jeh Johnson, it will take a great amount of coordination and effort by DHS to standardize some 9,000 systems.[5]

[5] http://www.wsj.com/articles/u-s-considers-classifying-election-system-as-critical-infrastructure-1470264895

(Hacking) From Russia with Love

Over the past few months, there has been substantial media coverage about hacking activities, allegedly by Russian actors. Here is a brief overview of the major events affecting the US, and what it may mean for the future.

Democratic National Committee

What happened?

The US Democratic National Committee (DNC) reported in mid-June that malicious actors had compromised its network and stolen numerous documents, including opposition research on Donald Trump, email and chat records, donor information, and other strategic internal communication.[1]

[1] http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?_r=0

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

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Security research firms assessed that Russian Advanced Persistent Threat (APT) groups, codenamed "Cozy Bear" and "Fancy Bear," were the likely culprits.

Why might it be Russia?

The day after the DNC reported the leak, some US-based news sites posted PDF files of the stolen documents. Some of the metadata remaining in these documents included messages in Russian, indicating that although the original documents were in English, a likely Russian-speaking actor saved the files and converted them to PDFs before they were published.[2]

Cozy Bear and Fancy Bear are presumed to be affiliated with the Russian government, and US intelligence agencies have reported that "they have 'high confidence' that the attack was the work of Russian intelligence agencies."[3] A hack of this kind could damage or embarrass the Democratic Party, which would be a good way for Russia to inject additional mayhem into an already contentious presidential campaign.

State Election Data

What happened?

US Intelligence officials reported in late August that hackers attempted to breach multiple states' voter registration databases. These breaches may have resulted in the theft of over 200,000 voter records and the infection of state systems with malware.[4] While some security experts have indicated that the actors may have been looking to alter voter registration data or otherwise manipulate voter records, the US Department of Homeland Security (DHS) has indicated that these hacks have not affected the integrity of the voting systems themselves.[5]

Why might it be Russia?

As with the DNC hack, Russian hacking groups might be motivated to compromise US elections to attempt to further throw the election cycle into chaos. To thwart these efforts, DHS Secretary Jeh Johnson has offered assistance to states for the November elections (*see: Securing the American Election, pg. 3*) to protect against any further hacking attempts by malicious actors.

Olympic Athlete Medical Data Hack

What happened?

In early September, members of the "Fancy Bears Hack Team" (yes, probably the same folks as the DNC hack) posted on social media that they had hacked into the World Anti-Doping Agency (WADA) and leaked confidential medical data on four US Olympic athletes.[6] According to the

[2] (U/FOUO) DHS; iSIGHT Partners; 'Guccifer 2.0' Leak of DNC Documents Most Likely Part of Russian Disinformation Campaign; Intel-00009500; 2; DOI 17 JUN 2016; (U); Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

[3] http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?_r=0

[4] https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

[5] (U/FOUO) DHS National Protection and Programs Directorate Office of Intelligence and Analysis. "Cyber Threats and Vulnerabilities to US Election Infrastructure." 2016.

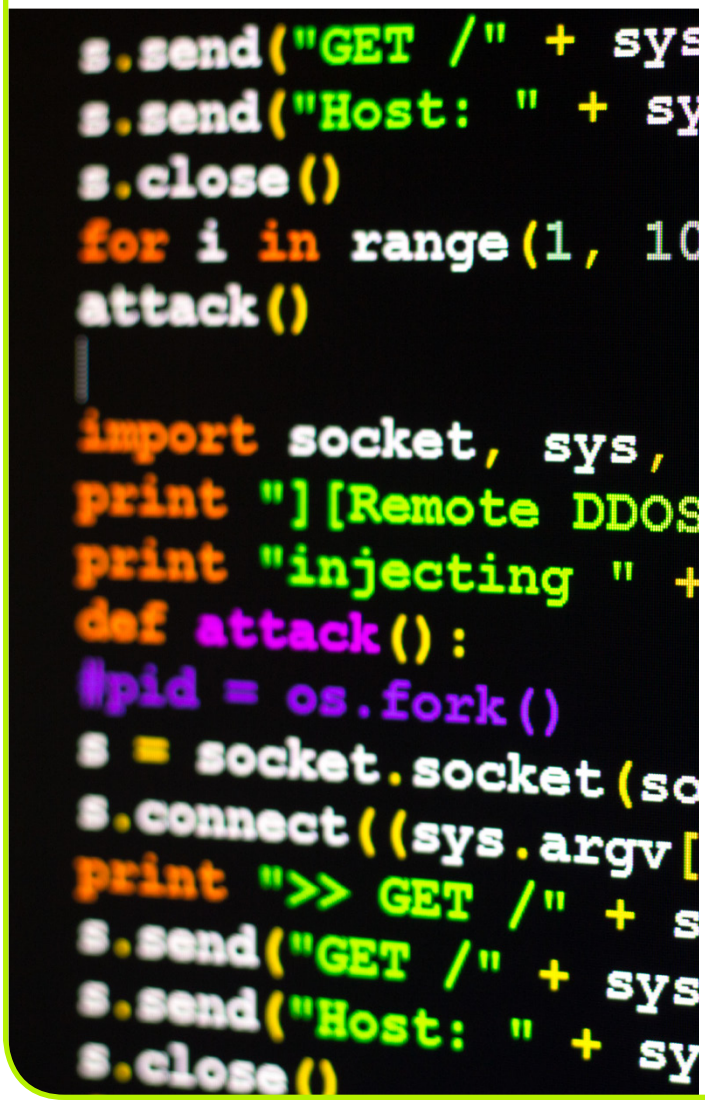
[6] http://www.usatoday.com/story/sports/olympics/rio-2016/2016/09/13/wada-confirms-us-athletes-data-hacked-blames-russians/90306006/

actors, this leak was orchestrated to maintain "fair play and clean sport," as they exposed information that these athletes had been medically cleared to use otherwise banned substances. This leak was likely in response to the ban on a large number of Russian athletes from competing at the 2016 Rio Olympics, after they were found to have participated in a state-sponsored doping program.[7]

Why might it be Russia?

Although the social media posts used images commonly associated with the hacktivist community, no other well-known hacktivist social media accounts shared or endorsed the leak, something that would have been likely to occur if the group were associated with the hacktivist community.

Further, given Russia's currently hostile relationship with the WADA due to their ban of Russian athletes at the Olympics, Russia would be motivated to target the WADA for perceived preferential treatment of other countries' athletes.



Why should average citizens care about these events?

Nation-state sponsored espionage isn't revolutionary; what is new is deploying cyber tools as the weapon, particularly since some consider these activities as attacks on another government.

Whether it's to expose or manipulate political activities in another country, or simply to embarrass a rival country on the world stage, we can expect to see cyber weapons wielded more frequently. In the future, because cyber attacks are increasing, it is likely that state-sponsored malicious actors will continue to target not just information systems, but critical infrastructure and high profile targets.

[7] (U/FOUO) DHS; iSIGHT Partners; Fancy Bears' Hack Team Leaks US Athlete Medical Records from WADA; Intel-00013900; 19 SEP 2016; DOI 19 SEP 16; (U); Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Cyber Highlights

GovRAT V2.0: Time to Call the Exterminators

GovRAT V2.0 is the newest malware threat that has already attacked US military institutions and government websites.[1] Using this new platform, hackers have extracted personal information (passwords, emails, first names, etc.) of government officials and possibly even military personnel from the National Institute of Building Sciences. GovRAT V2.0 is an advanced piece of malware that uses stolen digital certificates to bypass antivirus programs. The newest feature is the ability to spread to external drives like USB devices, behaving much like a worm.[2]

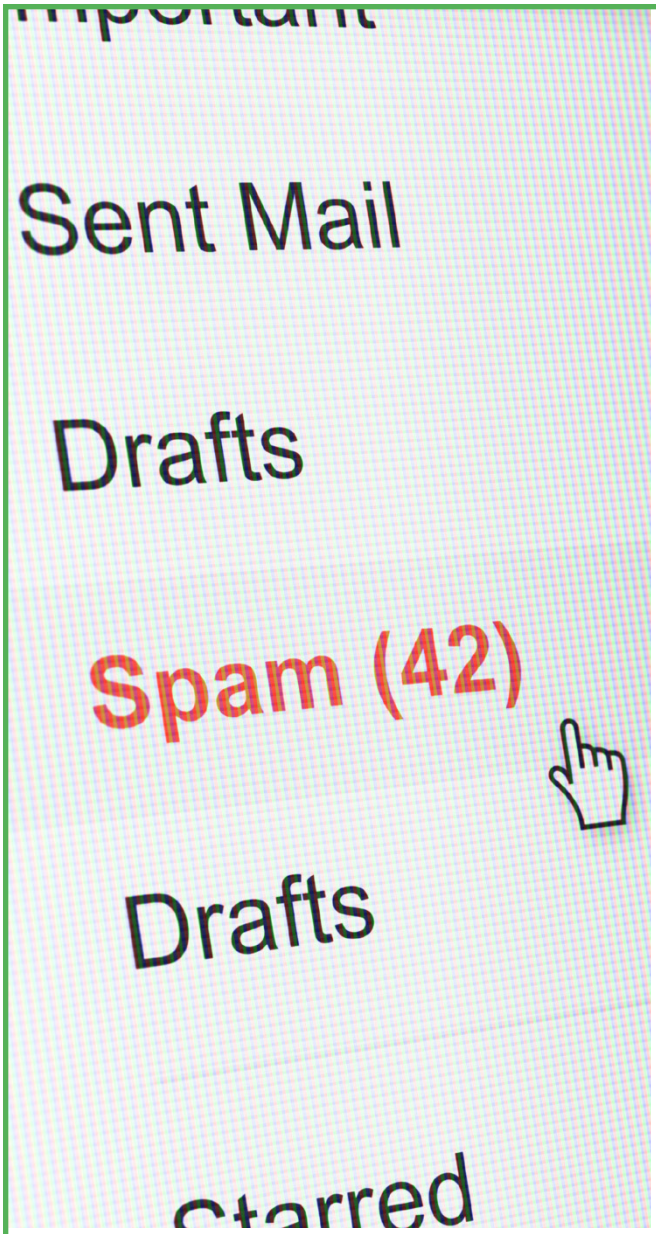
A bad actor that goes by the name of "PoM" is selling 33,000 records with credentials for US federal, state, and local government agencies, as well as several research and educational establishments. PoM is a new actor who is working with another known hacker, "Poporet." The report isn't clear but is possible that PoM probably was "tasked" to retrieve a list of government and military employees (NASA.gov, Army.mil, and Navy.mil specifically). According to the security firm, it appears that much of the data was stolen from the National Institute of Building Sciences (http://www.nibs.org/). The duo have focused primarily on collecting data from law enforcement, military, education, and government agencies in general. If they have a specific target, it's clear that they didn't want us to know. Some of the federal agencies included in the list of records are:

- Nasa.gov
- NSA.gov
- FBI.gov
- Navy.mil
- US.Army.mil

[1] Kan, M. (2016, September 9). Network World Inc. Retrieved from Network World From IDG: http://www.networkworld.com/article/3118768/crafty-malware-is-found-targeting-us-government-employees.html

[2] Paganini, P. (2016, September 13). Security Affairs. Retrieved from Security Affairs: http://securityaffairs.co/wordpress/51202/cyber-crime/govrat-2-0-attacks.html

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org



Among the list of affected agencies, the only state or local entities affected were:

- dgs.ca.gov (Department of General Services – California)
- talgov.com (City of Tallahassee website)[3]

Although it appears that the actors are only looking to sell the information, it is possible that they or others may use the compromised data in future attacks using social engineering and phishing campaigns.

If your agency has been affected by GovRAT V2.0, it is important to maintain a good cyber security posture to avoid any further damage in the event of future malicious attacks. The best way to prevent additional harm is to be aware about what emails might arrive in your inbox. Don't click on links that appear fake or originate from suspicious sources. If your credentials are compromised in a data breach, consider changing your password, which may prevent hackers trying to access more information or other accounts.[4]

[3] Komarov, A. (2016, September 7). Infoarmor, Inc. Retrieved from Infoarmor: https://www.infoarmor.com/wp-content/uploads/2016/09/GovRat-2-FINAL2.pdf

[4] Komarov, A. (2016, September 7). Infoarmor, Inc. Retrieved from Infoarmor: https://www.infoarmor.com/wp-content/uploads/2016/09/GovRat-2-FINAL2.pdf

Android: App Permissions Made Simple

In our last Ledger issue, we presented tips on mobile device safety (*Mobile Computing Safety 101: Apps*). Among our tips, we recommended that you check which permissions are required for an app you are thinking of installing. Unfortunately, sometimes that doesn't tell you much. App permission descriptions aren't always self-evident.

The following table presents real-world descriptions of some of the more common or risky Android permissions. Keep in mind that most apps have legitimate reasons for these permissions; the Possible Risks paragraph details what *unscrupulous* apps might do with them.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

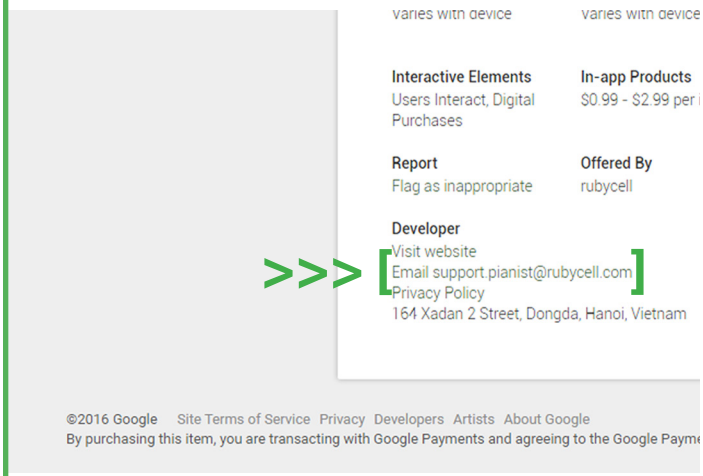
Permission	Description
Full network access	Allows the app to send and receive information via the Internet, for communicating and downloading content; also necessary for displaying ads. **Possible risk:** *Privacy.* If there is nothing to download or communicate from the Internet, and no ads to display, this permission may represent a risk to privacy.
Directly call phone numbers	Allows the app to make phone calls without any action from you; used on apps like Skype. **Possible risk:** *Money.* This permission can be used to call pay-to-talk phone numbers.
Read your contacts	Required for messaging apps, apps like Twitter for sharing tweets, and many gaming-with-your-friends apps. **Possible risk:** *Annoyance, and a lesser risk to Privacy.* Your list of contacts may be considered sensitive, so we recommend extreme caution when agreeing to share it. Plus, apps could start spamming your friends with ads and messages.
Track your location (GPS)	(Of the two main types of location tracking [GPS and network based], this is the more precise.) Allows tracking your device based on its GPS coordinates; used by countless apps: Google Maps, Waze, Gas Buddy, Yelp, and—of course—Pokémon Go. Also required for any app that displays location-based ads. **Possible risks:** *Privacy and Safety.* In addition to sending you unwanted ads, poor app coding could allow this feature to be used to stalk or harass you.
Track your location (network-based)	(Considered more "coarse" compared with GPS tracking.) Tracks your general location based on which cell tower your device interacts with; seen as less invasive than GPS tracking. **Possible risks:** *Similar to those of the GPS tracking (above), but with less precision.*

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Read and send (text/SMS/MMS)	Includes receiving, reading, editing, and sending text, SMS, and MMS messages; necessary for any messaging app. **Possible risk:** *Privacy and Money.* If the app is not specifically designed to send and receive these messages, it can violate your privacy and even cost you money, especially in data charges.
View Network status/ Wi-Fi state	Informs you when a Wi-Fi network is near. **Possible risk:** *Likely none.* None, with the permission itself, but be careful to connect only to networks for which you have approval.
Find and use accounts on the device	Finds accounts (like Facebook, Google, and Twitter) and logs into them; common with social media apps and the many Google services, such as Gmail and Google drive. **Possible risk:** *Privacy.* Theoretically, the app might be able to access any information within your account.
Phone status and identity	Allows the app to know when a call is coming in, pausing the activity so you can answer. **Possible risk:** *Privacy.* Each mobile device carries an International Mobile Equipment Identity (IMEI) number, which is normally unique for each device. Though not likely, it could be used to spy on your activity and preferences.
Modify, delete, and read storage	Allows the app to save and edit files, as well as keeping temporary logs; most apps require this permission. **Possible risk:** *Privacy.* Any app with this permission can also access any public folders on your device, such as the photo gallery.
Bookmark web pages and read web history	Allows apps to read your web viewing activity as well as which sites you have bookmarked; common with browser apps. **Possible risk:** *Privacy.* Could spy on your browsing behavior for targeted ads.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

In-app purchases	Allows buying additional content or services within the app; common in games. **Possible risk:** *Money.* Children especially might (by accident) misuse this permission if they play games on your phone, or on their own. Make sure that password protection is turned on for this permission.
Create Bluetooth connections	Allows identifying and connecting to nearby Bluetooth devices. **Possible risk:** *Likely none.*
Take photos or video	Exactly what it sounds like; used by alternative camera apps. **Possible risk:** *Likely none.* Theoretically, an unscrupulous app might secretly take pictures.
Prevent phone from sleeping	Exactly what is sounds like; keeps the phone "awake" for required app processes. **Possible risk:** *Likely none, but it may affect your battery life.*
Control vibration	Exactly what it sounds like; allows the app to make use of the device's vibrator. **Possible risk:** *Likely none, but it may affect your battery life.*



https://play.google.com/store/apps/details?id=com.rubycell.pianisthd

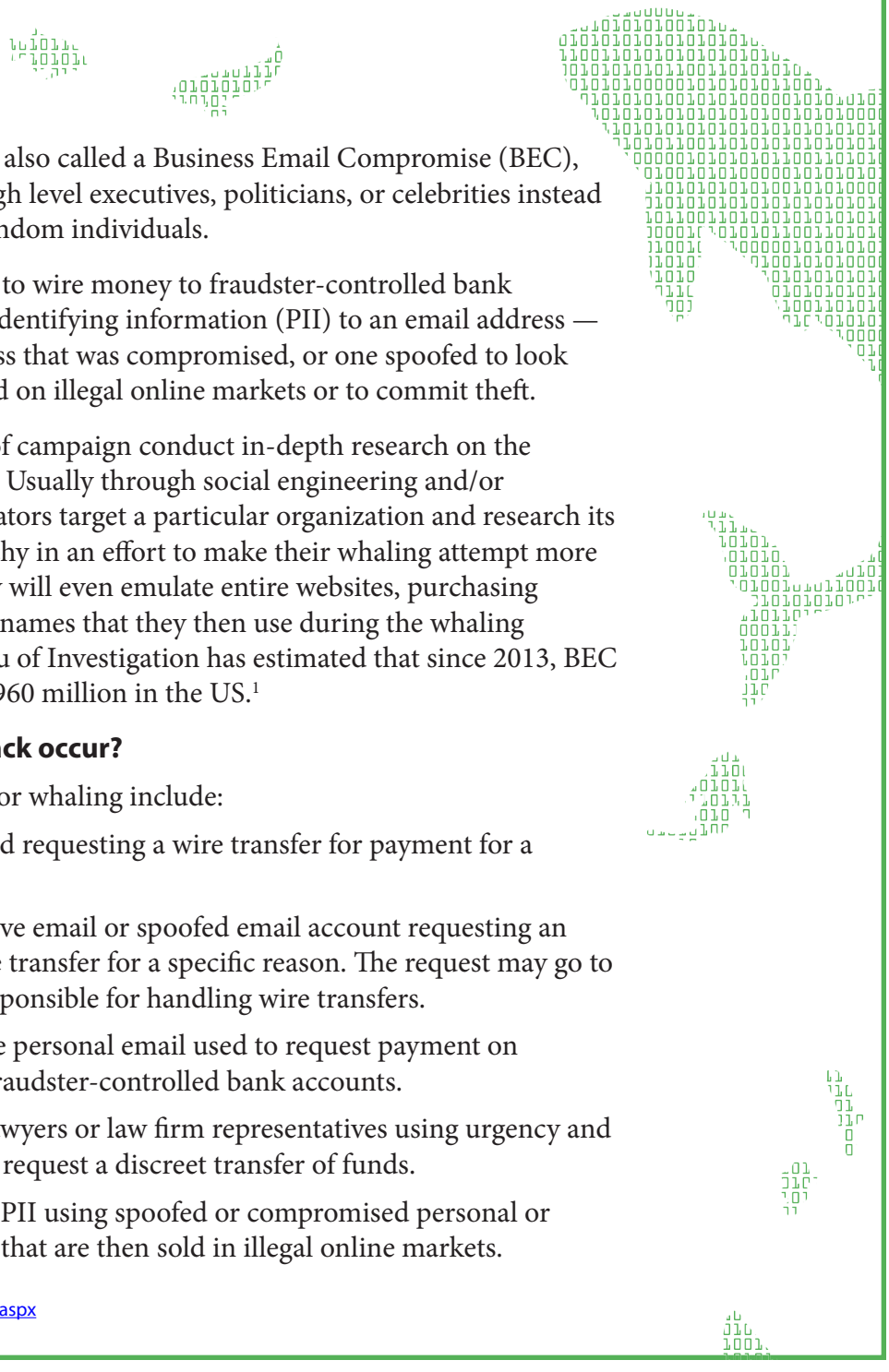
Sometimes, it simply comes down to trust.

And an old Russian proverb advises us to "trust, but verify." Before using any app on your phone do your homework. In addition to reading the comments in the app store itself, check what opinions a Google search turns up—from other user,s security experts, and even rival app makers.

If none of those answers your concerns, *email the developer.* There is a link for doing just that at the bottom of each app page in the Google Store (*See image on left*). Detail your issue and ask for an explanation.

Why Phish When You Can Whale?

Phishing scams have been around since the dawn of the Internet, but over the past few years malicious actors have turned to whaling, which is a twist on the traditional phishing scheme that seeks out bigger targets and bigger "phish."



What is whaling?

Whaling is a type of phishing, also called a Business Email Compromise (BEC), scam that primarily targets high level executives, politicians, or celebrities instead of lower level employees or random individuals.

These scams involve a request to wire money to fraudster-controlled bank accounts or to send personal identifying information (PII) to an email address — either an internal email address that was compromised, or one spoofed to look legitimate. This PII is later sold on illegal online markets or to commit theft.

The perpetrators of this type of campaign conduct in-depth research on the entities they attempt to whale. Usually through social engineering and/or malware deployment, perpetrators target a particular organization and research its culture, processes, and hierarchy in an effort to make their whaling attempt more believable. In some cases, they will even emulate entire websites, purchasing domains with similar looking names that they then use during the whaling campaign. The Federal Bureau of Investigation has estimated that since 2013, BEC losses amount to more than $960 million in the US.[1]

So how does a whaling attack occur?

The common scenarios used for whaling include:

- Emulating a supplier and requesting a wire transfer for payment for a fraudulent invoice.
- A compromised executive email or spoofed email account requesting an urgent confidential wire transfer for a specific reason. The request may go to the person normally responsible for handling wire transfers.
- Compromised executive personal email used to request payment on fraudulent invoices to fraudster-controlled bank accounts.
- The impersonation of lawyers or law firm representatives using urgency and confidentiality issues to request a discreet transfer of funds.
- Fraudulent requests for PII using spoofed or compromised personal or internal email accounts that are then sold in illegal online markets.

[1] https://www.ic3.gov/media/2016/160614.aspx

Ways to Avoid Becoming a Victim

The good news is you can take steps to protect yourself and your business from these types of fraud.

1. Be suspicious of requests for secrecy or urgency that involve fund transfers or disclosure of PII.
2. Consider implementing Two-Factor Authentication for corporate email accounts.
3. Use "forward" instead of "reply" when responding to emails. If someone is spoofing an email address, forwarding a response forces you to manually enter an email address rather than auto-filling that field and potentially replying to the fake email.
4. Establish other communication methods or procedures, such as requiring secondary authorization or phone confirmation for fund transfers/ disclosure of PII.
5. Beware of sudden changes in business practices, especially if they have not been made company-wide.

What Phishing Emails Mean to You

Bad actors frequently see events that are widely publicized by the media as a great opportunity to start a new scam, because their ruse becomes more believable.[1] Recently, we have seen new scams involving Zika, the mass shooting at Pulse nightclub, and even Pokémon Go™.

In September, a phishing email with false statistics about Zika surfaced. Although it contained a link with information about Florida Zika cases, the email was actually a hoax. Such emails can lead to infecting a computer with malware.

In addition to emails with fraudulent links, there have been numerous fake charities (such as GoFundMe accounts) associated with the Pulse shooting.[2] Be wary of anyone asking for money with a vague story. Keep in mind that

[1] https://kb.iu.edu/d/arsf

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

as a donor, you have the right to ask how the funds will be used.

Some Pokémon Go™ users were put at risk when a fraudulent email was sent out in June stating that the application was no longer free to use. The email told users that they had to set up a payment method to pay $12.99 a month for access to the game. After victims sent their personal information, scammers would go on to steal some victims' identities.[3]

Criminals prey on opportunity. After Hurricane Katrina, more than 60% of the 4000 sites created for relief efforts were fraudulent. In addition to just stealing what you believed to be a legimitate donation, these bad actors may also seek to steal your identity. Having your identity stolen could mean a loss of thousands of dollars, damaged credit, and a time-consuming hassle to fix.

How to Protect Yourself

Be wary of any email that does not look quite right. The difference in the ending of an email .com or .gov can make all the difference as to whether or not it is authentic. Remember, legitimate companies such as Microsoft or your bank will not contact you via email about your account. Also keep in mind that these types of scams are more prevalent during the holiday season.[4]

When in doubt, a good rule of thumb is to never give out your personal information via email or phone to someone whose identity you cannot verify.

[2] http://gofraudme.com/lets-talk-gofundme-pages-pulse-nightclub-shooting/
[3] http://www.bbb.org/council/news-events/bbb-scam-alerts/2016/07/pokemon-go-players-fall-for-phishing-con/
[4] http://www.forbes.com/sites/lisabrownlee/2015/10/07/top-10-new-phishing-scams-how-you-and-your-company-can-thwart-them/2/#7d69e6417b77

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Design 101

Type Basics: How to Chose and Combine Typefaces

Smartly using typefaces is one of the simplest but most effective methods of adding quality to your work. Not everyone has access to specialized software when creating products, but the appropriate use of type can add an edge of professionalism that can set your work apart from others.

However, a lot more goes into typefaces than most people realize. Typefaces have a larger impact than most will give them credit for, since most of their effects are usually quite subtle. Here's a dramatized example of how a typeface can alter the perception of its text:

vs.

I'm coming to see you.

This may be an over-the-top example, but the point remains that altering a typeface can drastically alter your perception of the message. This can be advantageous if done on purpose, but it can be detrimental if done by accident. As such, it's important to understand typefaces and how they are perceived before picking them for your products.

To start with, you should be aware of the broad categories of typefaces. The different categories are distinguished from each other by the various ways different parts of the characters are "drawn." The number of categories will vary depending on who you ask, but these five usually show up consistantly:

Serif
- Serifs are the "feet" the characters have
- Frequently used for printed body copy; easy for the eye to read
- Variations in serif size can create different "feels"

Sans-serif
- Named for the "feet" they don't have
- Used for digital body copy; easier to read on screens than serif
- Good for size extremes - very large or very small

Script
- Simulate hand-written text
- Not good for bodies of text; difficult to read in blocks
- Great for titles; the large size increases readability

Display
- Distinguishable letters, but much more decorative
- Mainly for titles and headings
- Not good for bodies of text either: not good in small sizes

- Symbols and dingbats; no distiguishable letters
- Used before Unicode, our current text standard system
- Can be used as bullets in lists to create flair

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

In addition to the broad categories that font typefaces fall into, most will usually have a selection of styles and weights that can be applied to them as well. These can affect the type almost as much as a different font. Using the typeface Myriad Pro as an example, the most common are:

Weight

Myriad Pro Light
Myriad Pro Regular
Myriad Pro Semibold
Myriad Pro Bold
Myriad Pro Black

Styles

Myriad Pro Condensed
Myriad Pro Italic
Myriad Pro Oblique
Myriad Pro Small Caps

Now that you know the different types of typefaces and some basic effects you can apply to them, you should learn about how these effects interact with each other. Choosing a single typeface is important, but equally important is choosing groups of typefaces, since they will work with each other and can greatly increase the aesthetic appearance of your work. Typefaces can have one of three relationships, with one to avoid and two to strive for:

Contrasting
Eye-catcing

- Using typefaces that contrast with each other
- Accomplished by selecting fonts from different categories
- Very eye-catching
- Multiple methods: heavy/light, curly/straight, wide/narrow

Concordant
Calming

- Mostly the use of styles/weights within same typefaces
- Creates a calming effect
- When choices are limited, this can still create energy
- Easy to overdo; try to alter only one or two effects at a time

CONFLICTING
Avoid this

- Using different typefaces that look too similar
- The similar-but-not-quite effect can be jarring to the eye
- Not unique enough for contrast or alike enough for concord
- If your typefaces conflict, pick new ones

There are many things to consider when deciding what typefaces to use. Readability and mood are your chief concerns when selecting typefaces, preferably in that order. Ask yourself, "Can I read this?" If the answer is no, start looking at alternatives. Consider the options within the typeface you picked, its weight and styles, and if you still can't read your text comfortably, find a new typeface. Maybe you need a serif instead of a sans-serif.

If your first choice reads fine, ask yourself, "Does it fit the mood of my content?" Curly display typefaces wouldn't be appropriate for a funeral announcement and formal black styles don't fit a birthday invitation. Even if your typeface reads perfectly, it might not be the right fit.

To make your work really stand out, try to create some nice energy between your typefaces by finding ones that work well with each other. Strive for concord and contrast and avoid conflict. It takes a little extra work that can get tedious the further into detail you get, but it pays off in the end.

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 and fill out the sign-up sheet 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.

How A Computer Outage Can Take Down A Whole Airline

https://www.wired.com/2016/08/computer-outage-can-take-whole-airline/

- Delta became the latest in a series of airlines who have suffered network outages over the past year.
- Airline networks are layered and complex, which means that one outage could have a ripple effect that has global implications.

Analyst note: Technology has streamlined so many parts of our life, so when something like an airline network outage occurs, it amplifies how dependent technology is to keep things running correctly.

This data-stealing Trojan is the first to also infect you with ransomware

http://www.zdnet.com/article/this-data-stealing-trojan-malware-is-the-first-to-also-infect-you-with-ransomware/

- Ransomware continues its trend of being the worst of the worst types of malware.
- Creators of ransomware have innovated with a new variant, which not only infects your device with ransomware, but also infects it with a password-stealing Trojan.

Analyst note: As always, we remind our readers to be wary of suspicious links, emails, and downloads. When in doubt, don't click.

98 personal data points that Facebook uses to target ads to you

https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?tid=sm_tw

- To provide marketers with the best information to target consumers, Facebook released a list of all the types of data it records for each of its users.
- Some of the data is obvious, like birthdays, while other data points are more surprising (like how many credit lines you have).

Analyst note: Keep in mind that if a service doesn't cost anything, it's because you are the product. If you don't want your personal information used by third parties, do your best to keep it off the Internet.

10 year-old teaches hackers a valuable lesson in privacy

http://www.csoonline.com/article/3108500/security/10-year-old-teaches-hackers-a-valuable-lesson-in-privacy.html

- As a school project, a young student decided to test how many people would connect to an unsecured wireless network in public places.
- Approximately half of those who connected also agreed to the very broad and scary Terms of Service.

Analyst note: The lesson here is that even the most seasoned security experts can fall prey to the lure of free wi-fi. Always verify that what you're connecting to is safe and secure.

Online fraud: Top Nigerian scammer arrested

http://www.bbc.com/news/world-africa-36939751

- Earlier this year, a hacker believed to be the ringleader of an email scam network was arrested in Nigeria.
- The global scam, which included over 40 individuals and was worth more than $60m, used malware and social engineering to trick its victims.

Analyst note: Although the "Nigerian scammer" email scheme is typically used as a joke to describe fraudulent email, the size and worth of this network shows how lucrative, and dangerous, these scammers continue to be.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Secure Florida's Best Practices for Office Security

1 Be suspicious of email links and attachments.

Emails designed to trick you into clicking links and downloading files come to inboxes daily. It is a practice called phishing and it's surprisingly effective. The easiest way for someone to get unauthorized access to your network is for you to give it to them. Never click on email links and never download attached files unless they are from trusted sources.

2 Use strong passwords and keep them private.

Your password is one part of the information security process that you control. Remember that you are protecting your accounts not only from someone trying to guess your password, but also from someone who steals password files to crack them. A strong password can take so much time to crack that it's not practical to keep trying, so the stronger your password is, the safer you are.

3 Back up your files regularly.

That spinning plate on your hard drive is an accident waiting to happen, and Florida is the lightening capital of the country. Hard drive crashes, electrical surges, and operator errors lead to many lost files. So do stolen laptops. Make sure you have backups of your important files.

4 Be careful when using public Wi-Fi.

When you connect to public Wi-Fi, or an "open network," anything you transmit can be seen by others. This includes usernames, passwords, account numbers, and confidential work information. Using a "secure" connection (such as HTTPS, SSL, or VPN) helps lessen the risk.

5 Use password protected screen savers.

It can only take a few minutes for someone to take advantage of a computer left idle.

6 Download only from approved sources.

As with email attachments, never download files from untrusted sources. Be especially suspicious of free software; it often has malicious software bundled with it.

7 Don't give out information to unverified individuals.

Social engineers try to fool you into giving out confidential information. Sometimes the information they ask for seems harmless, so their request doesn't raise any red flags. Before giving out any office-related information, be sure the person making the request is authorized to receive it.

8 Know and follow your organization's information security policies.

Your organization has its own security rules on matters such as using USB drives and personal devices on your work computer. Follow them carefully.

Information Resources

The Florida Infastructure Protection Center was established in 2002 to antipcipate, 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