The Beacon

Florida Fusion Center #16-094 | Cyber and Critical Infrastructure Report | July 2016 Issue #10

Summary

Mobile Computing Safety 101: Apps -
Here's some tips and tricks to make sure you're keeping your mobile device safe.

So Your Smartphone's Been Stolen? -
No one wants to think about losing their device, but here's how to handle it if it happens to you.

Death of the Password -
It's not gone yet, but we discuss some new technologies that have begun to replace/augment the password.

Insider Threats: Catastrophic Damage -
We cover why and how Bad Actors on the inside can be the most dangerous threat to critical infrastructure.

Resolution: From Screen to Print -
Ever wondered why images look great on screen but terrible when printed? Here's why.

Dispatch Highlights -
Here's a summary of a few of The Dispatch's most popular articles.

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

Cybercriminals and Emergency Scams

It's not necessarily a new phenomenon, but with the tragic shootings at the Pulse Nightclub last month in our home state, we would like to remind our readers about phishing email scams. And these aren't the typical "Prince of Nigeria" phishing email scams—these are emails that use some kind of disaster or terroristic activity to trick you.

As we have discussed in past issues, phishing and other scam emails use some type of social engineering to trick people into opening an email. Social engineering capitalizes on a person's inclination to trust the legitimacy of what is being told to them—if it is an email about how to help someone after a natural disaster, shooting, or some other kind of disaster event, scammers are betting that a lot of people will be eager to help in whatever way they can. Unfortunately, these criminals capitalize on a natural tendency to want to aid in the event of a disaster.[1,2]

We have seen examples of these types of scams over many recent disasters. After terrorist attacks in Paris in late 2015, scammers sent out emails purportedly soliciting charitable donations for victims. Similarly, following a typhoon in the Philippines[3] in 2013, the United States Computer Emergency Response Team (US-CERT) issued an alert to citizens about scammers who sent out emails trying to extort money under the guise of fundraising for typhoon victims.

To date, there have not been any reported instances of false emails trying to extort money while pretending to help victims of Pulse Orlando.[4] However, we would like to remind readers of some important tips to keep in mind if you receive an email related to donations or assistance following some kind of emergency.

- Don't click on pop-up links or email links in suspicious emails. Links may appear to be for a charity, but could navigate you to a fake site that steals your money.
- Never give out personal information to unsolicited individuals. Even if they seem to be calling for a good cause, always verify before giving them your information.
- Watch out for scammers. They may pretend to be for an advocacy group (e.g. gun rights), or for a victims' rights group. Whatever the cause, always validate who they are before providing them your information, or worse, your bank account information.

[1] http://www.policypatrol.com/natural-disasters-and-your-email-security/
[2] https://blog.knowbe4.com/ftc-alert-dont-get-scammed-by-earthquake-phishing-emails
[3] https://www.us-cert.gov/ncas/tips/ST04-014
[4] http://www.freep.com/story/money/personal-finance/susan-tompor/2016/06/13/massacre-orlanda-night-club-could-trigger-scams/85826308/v

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

Cyber Highlights

Mobile Computing Safety 101: Apps

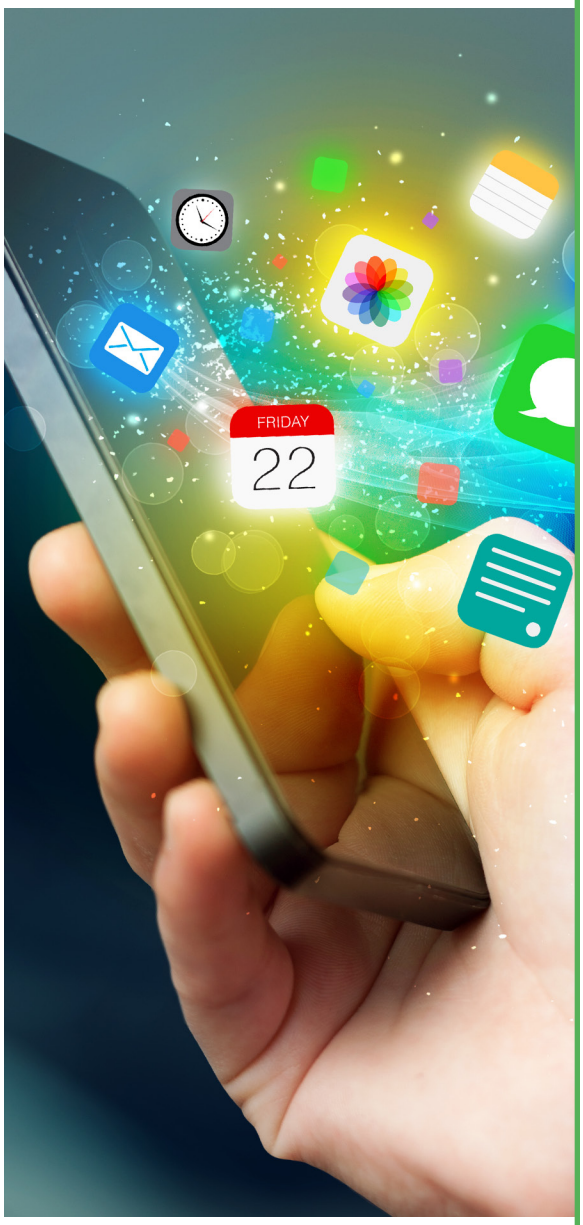
With nearly 500 million smartphones and tablets, Americans have turned to mobile computing in a big way.[1] But with thousands of apps, wireless networks to access, and the possibility of theft, hand-held devices present us with a whole range of new security risks.

This article presents a series of tips for assuring your apps are as safe and secure as possible.

Use a reliable app store.

The two primary sources for apps are **Apple's App Store** (iPhones) and the **Google Play Store** (Android). Although there are several other sources (including the **Amazon Appstore** and **Windows Phone Store**), these two are by far the largest, with millions of apps and billions of downloads. Although no source is completely free from malicious software, both Apple and Google have a thorough vetting process to keep their apps malware free.

If you are considering an app from a lesser-known store, make sure you do some research into both the store and the app before you download. You can't assume that all apps are safe: **security might not have been a priority for the app developer, but it should be for you.**



Check the settings.

Before using any app, check any settings carefully. Some options are merely decorative; others govern benign functions such as the music volume. However, many control privacy and security functions. Be especially careful with apps that track your location.

[1] http://www.emarketer.com/Article/US-Internet-Users-Rely-on-Mobile-Devices-Digital-Access/1013649

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

Check the ratings and reviews.

All app sources have ratings by users, usually expressed in stars (1–5). Many users also include a written description of their experience. Read these—not just the first few, but scan down the list: you might see some opinions that surprise you. For example, on the Google Play Store, Angry Birds has a 4.5/5 rating, but among those are many 1-star ratings because of the amount of advertising.

PARENTS:

Pay special attention to the Parental Guidance ratings. Each app is marked.

Apple App Store	Google Play Store
	E (Everyone)
4+	
9+	E10 (10 and over)
12+	T (Teens)
17+	M (17 and over)
	AO (Adults Only)

Check the permissions required.

Before an app can access certain features of your device (such as the camera or microphone), or before it can use other apps, it requires permission. Android apps list their permissions when you download them; if you don't want to grant the permission, you can refuse the app. Apple apps don't list the permissions when you download them, but ask you before each one they use; you can refuse permission any time.

If you've already installed the app...

Android:

Click on Settings > Application Manager. Click on each app to view the permissions required. If you have a device with the newest operating system (Android 6.0, also known as 'Marshmallow'), you now have the ability to disable specific permissions in individual apps. This can be accomplished by going to Settings > Privacy and safety > App Permissions. However, older operating systems have an all-or-nothing approach.

iPhone:

Click on Settings > Privacy. Each privacy category will have a list of which apps use them. You can disable any that you want.

PARENTS:

You might want to pay special attention to certain permissions such as accessing the contact list or location tracking. In addition, Android highlights which ones allow in-app purchases. Those are common on games. If a credit card is linked to your device, your child may be able to make purchases without additional approval.

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

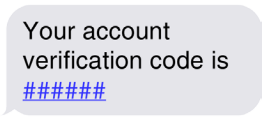
Death of the Password

The different password requirements for the online services we use are difficult to keep track of. Managing them all becomes impossible. New technologies are now focusing on using something you have (or are), such as smart cards or biometrics, as either a second layer of protection or even as the sole way of proving who you are and what you should have access to.

Smart Cards, which look like credit cards, have microprocessors ("chips") in them that dynamically interact with the system you are trying to access. There are two types: contact and contactless.

The "contact" type requires you to insert the card into a card reader. Think ATM. The system then reads the chip and waits for a password or PIN. Because the card knows what the password or PIN should be, it acts as a second layer of security. Newer credit cards have this technology.

The "contactless" cards require only that the card be in proximity to the card reader. Sometimes a PIN is also required, but frequently not. Often used for access to restricted areas, each contactless card is unique to one application, such as a place of business. Think of them as front door keys. They add little to security, as possession of the card as all that is required for access.



Short Message Service (SMS)/Texting Authorization is another secondary method of identifying yourself but requires a device with SMS or texting capability.

You typically see this feature on online services such as email or banking. When you log in, the service texts you a unique code to enter which proves that it really is you attempting to access their services.

***Biometrics* will soon become the most common element replacing or enhancing passwords.**

Biometrics is the measurement of people's physical characteristics and is what allows your unique physical traits to be used as a means of confirming your identity. Some examples of biometrics are voice recognition, facial recognition, retinal/eye scans, and fingerprints. The benefits of using biometrics are that they are difficult to counterfeit and they're always with you.

The three above technologies are not the only options but represent a good portion of password replacement or augmentation systems. All of the above methods can be combined with a traditional password or secondary identification to make it even more secure. While you should always have a strong password, secondary authorization means that if your password is compromised you still have another layer of security protecting your accounts.

So Your Smartphone's Been Stolen?

Our smartphones, tablets, and computers hold the keys to the details our lives. They contain email, social media accounts, phone contacts, financial information, fitness data, and pretty much everything else in between. So what do you do if your device is lost — or even worse — stolen?

If you discover your device is lost...

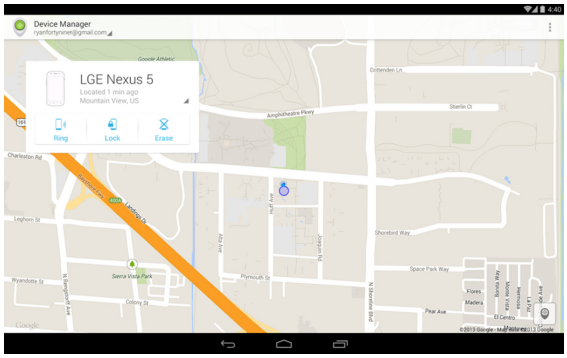
Once you discover your device is missing, here are the steps you should immediately take to protect the information contained on it.

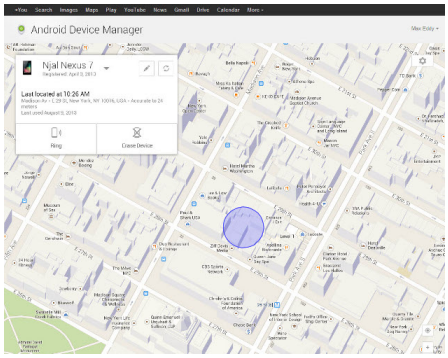
1 Track Your Device

Android and Apple products both have features built in to their operating systems to locate, and hopefully find, your device if it is lost or stolen.

Android

Android phones have a built-in feature called Android Device Manager (ADM) that allows you to communicate with your phone/tablet remotely, without ever installing an app. To use ADM to locate your device, use another device (a computer, or even a friend's smartphone) to open a web browser and do a search for "Android Device Manager." Click on the first web result, and log in with your Google credentials. This will bring you to a screen that looks something like this:





If you have more than one device, there is a drop down tab that lets you choose which device you're looking for. From here, you can:

- See the last known location of the device on a map.
- Activate the ringer for five minutes, so if it's nearby, you can find it.
- Lock the device with a screen displaying another phone number to call if someone finds the device.
- Erase the contents of the device.[1]

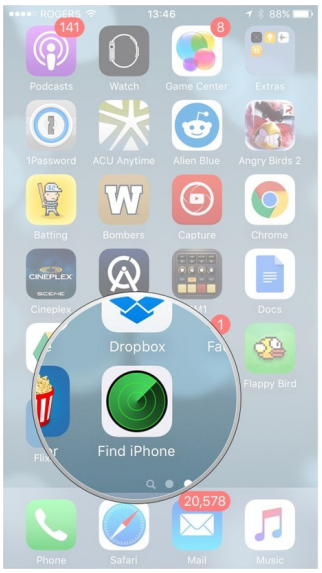
[1] http://www.pcmag.com/article2/0,2817,2423375,00.asp

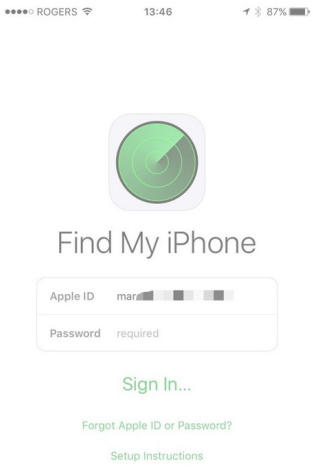
Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

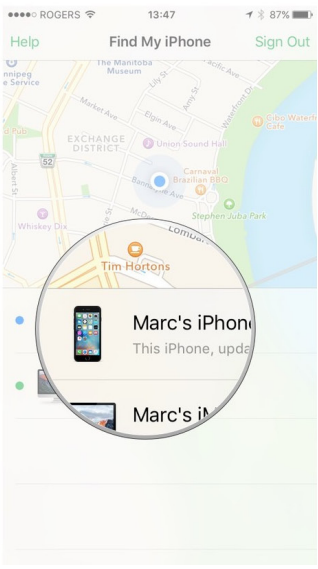
iPhone

The iCloud includes software called Find My iPhone that helps you find and protect any of your Apple devices. Unlike Android Device Manager, Find My iPhone must be set up on your device before something happens to it.

Once you have set it up on your iCloud account, if your device is lost/stolen you can log onto your account from any web browser and access Find My iPhone. From there you select which of your devices you wish to track.







You can find the last known location on the map. Additionally, Find My iPhone allows you to interact with your lost/stolen device to:

- Play a tone to locate if it's nearby.
- Enable "Lost mode," which lets you display a phone number to call if someone finds the device. Lost mode also plays a tone to draw attention to the device.
- Remotely erase the contents of the device.[2]

2 Log Out of Everything

Most mobile applications have ways of remotely accessing them in the event you can't get to them from your device.

Using another device, visit the sites for all of the applications on your phone. See if there is an option to logout or de-register other devices. If that is not an option, you can change the password for the application. This way, if someone else has possession of your device, they can't simply open up an app or website and use saved login information to access your data.

[2] http://www.imore.com/find-my-iphone

3 Tell Friends and Family

Letting those close to you know you've lost your device is a good idea even if they can't help you find it.

If someone else has your device, you will want to make sure to tell others. If that person is able to get access to your contact list, email, or social media, they may use that information to impersonate you. Telling others to be wary of odd communications purportedly from you could prevent them from becoming a victim of fraud.

4 Contact Your Cell Phone Provider

When you lose your credit card, you call the bank. Contacting your service provider when you lose your device is much the same.

If the device you have lost is a phone, make sure that you contact your cell phone provider as soon as possible. If a thief can unlock your phone, they may rack up a lot of charges on your account in a short amount of time. Some providers will deactivate your device completely from your network, which means that the thief won't be able to simply reset the device and replace the SIM card.

Keep in mind, however that if you have an iPhone, deactivating your service will mean that you can't communicate with your iPhone using Find My iPhone, so consider trying the Find My iPhone process before deactivation.

5 File A Police Report

Letting law enforcement know your device isn't with you is also a good idea; you never know where your device might end up.

Especially if you know your device has been stolen, make sure that you contact your local law enforcement agency and file a police report. Even though finding your device might not be their top priority, if they do find your device, they know how to get it back to you.

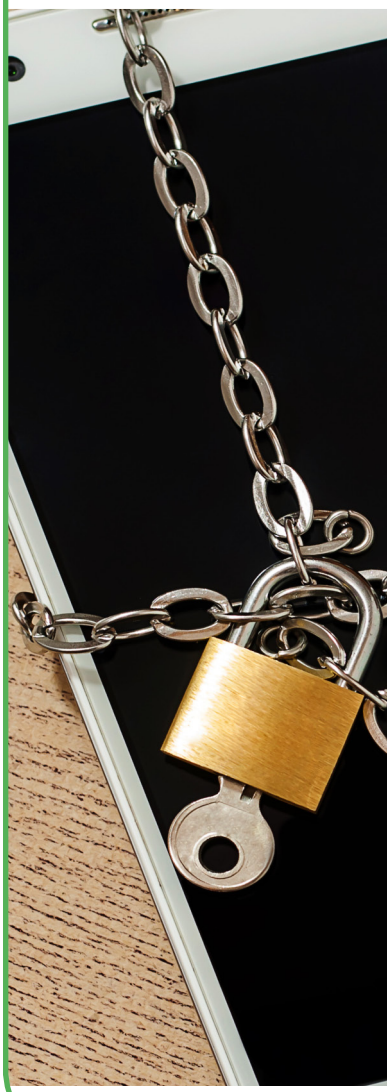
6 Check Classified Ad Websites

Keep an eye and ear out for any advertisements for devices that look or sound like yours.

A lot of times, thieves don't hold on to the devices they steal. Instead, they find a way to make money off the stolen phone or computer, and a great way for them to do this is by posting a classified ad. If your device was stolen, look at the ads in your geographical area to see if a device matching yours suddenly comes up for sale.

If you do find that a crook is selling your device, having a police report already on file is handy. You can notify law enforcement of the post, and let them get your possession back rather than potentially putting yourself in danger.

What to Do BEFORE Your Device Is Lost...



Password Security:

If your device is lost or stolen, one of the best ways to prevent someone else from getting access to your data is through strong password security. Make sure that you have a lock screen on your devices. If you use a PIN on a smartphone or tablet, use a code that is not easily guessed; if you use a swipe pattern, make it a complex one. For computers, use a lock screen and create a password that is 15+ characters.

Back it Up:

Make sure that any vital information on any devices is regularly backed up onto a separate storage device. Regardless of the circumstance, if you never get your device back then having an extra copy of your data is the best consolation.

Keep Good Records:

Any time you acquire a new device, document its serial number. That number could be vital if at some point down the road you have to prove that the device is actually yours.

Recovery & Anti-Theft Services:

There are a number of apps on the market, aside from the tools built in to Android and Apple operating systems, that help you find a device that has disappeared. Some apps are free, while others require a subscription or in-app purchases. Make sure you do your research before installing one; more importantly, if you download one of these services, make sure you know how it works before you need to use it.

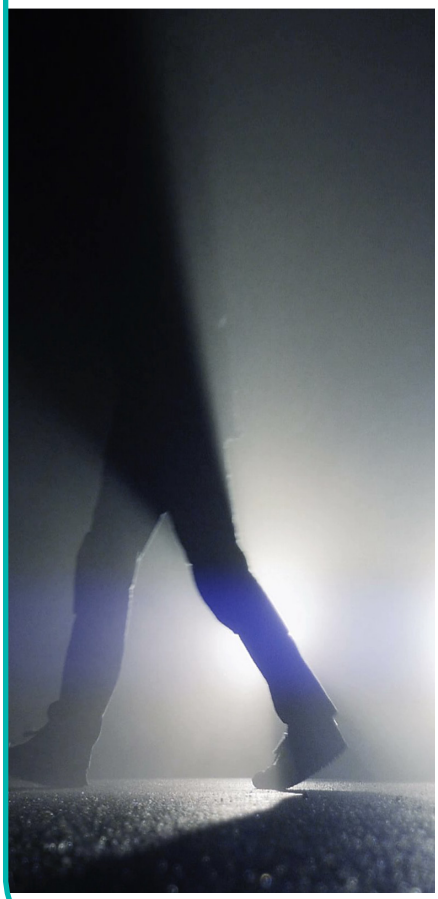
Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Critical Infrastructure

Insider Threats: Catastrophic Damage

Insiders will likely continue to conduct criminal acts or acts of terrorism that will cause loss of life, personal injury, and property damage. Insiders can be anyone with trusted access to the organization, its property, or employees. This includes employees themselves, family members, persons making deliveries, outside contractors with internal access, frequent and trusted customers, or others that have special access or unique knowledge. The Florida Fusion Center is not aware of information related to a specific or immediate threat currently to any sector, but organizations should be aware of the possibility of insider threats and take necessary steps for self-protection.

Most businesses understand that trusted insiders can be a threat to their financial well-being through embezzlement and other fraud schemes.[1] A large portion of thefts from warehouses, retail sites, and transport vehicles are committed by insiders,[2] as are many types of white-collar crimes.[3] Insiders also have the best chance of initiating cyber-crime and are often involved in stealing trade secrets.[4,5]



In addition to concern over the financial consequences however, public and private organizations should give serious consideration to insider threats that can lead to loss of life, personal injury, and property damage. Furthermore, while all organizations are potential candidates for workplace violence, some are likely at greater risk as targets of insider terrorists. Organizations where damage to the facility can cause even more damage (loss of life and property) to the surrounding area (e.g. West, Texas fertilizer plant) may be attractive targets to those trying to instill fear. Other similarly attractive targets are organizations that create large concentrations of visitors, spectators, or participants, as well as organizations that provide lifelines such as water or electrical services.

[1] Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse 2014 Global Fraud Study, accessed June 23, 2016 09:56, http://www.acfe.com/rttn-perpetrator-schemes.aspx

[2] RSI Insurance Brokers, November 2013, Cargo Theft in the Transportation Industry, accessed June 23, 2016 10:21, http://www.rsiinsurancebrokers.com/11_13cargotheft/

[3] Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Years 2010-2011, accessed June 23, 2016 10:05, https://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011

[4] Ic3, December 23, 2014, Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information, accessed June 23, 2016, 10:28, https://www.ic3.gov/media/2014/140923.aspx

[5] Federal Bureau of Investigation, The Insider Threat An introduction to detecting and deterring an insider spy, accessed June 23, 2016 10:12, https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

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

Below are examples of several recent high-profile insider terrorist incidents:

- A husband and wife team killed 14 people and injured 21 others in an act of terrorism in December 2015.[1] The attack occurred at the Inland Regional Center in San Bernardino, CA, during a county Department of Public Health training event and Christmas party. The husband was an employee of the health department and some victims were his coworkers.
- An explosion at a fertilizer plant in West, Texas in April 2013 was the result of arson.[7] The culprit is still unidentified, but was likely an insider that had trusted access. The fire and subsequent explosion killed 15 people, injured 300, and destroyed more than 500 homes.[8]
- In November 2009, a United States Army major, who was a licensed psychiatrist with fifteen years of military service, used his insider status at the Darnall Army Medical Center at Fort Hood, Texas to kill 13 people (12 of them soldiers) and injure 42 others.[9]

Employers should be wary of applicants who may be attempting to gain employment in order to commit criminal or terrorist acts. The process of legal background checks related to prior employment, community standing, illegal substance use, stable financial status, and prior criminal conviction history is an important tool in eliminating insider threats. For existing employees, employers need to be aware of behavior patterns that change during the so-named "radicalization process."[10] Useful information on this subject can be found through the Fort Knox Military Intelligence Group as well as other sites.

[6] Federal Bureau of Investigation, December 2015, *FBI will Investigate San Bernardino Shootings as Terrorist Act*, accessed online June 27, 2016 09:24, https://www.fbi.gov/news/news_blog/fbi-will-investigate-san-bernardino-shootings-as-terrorist-act

[7] Bureau of Alcohol, Tobacco, Firearms and Explosives, May 11, 2016, *ATF announces $50,000 Reward in West, Texas Fatality Fire*, accessed June 23, 2016 09:34, https://www.atf.gov/news/pr/atf-announces-50000-reward-west-texas-fatality-fire

[8] Bureau of Alcohol, Tobacco, Firearms and Explosives, May 11, 2016, *ATF announces $50,000 Reward in West, Texas Fatality Fire*, accessed June 23, 2016 09:34, https://www.atf.gov/news/pr/atf-announces-50000-reward-west-texas-fatality-fire

[9] The William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at fort Hood, Texas, on November 5, 2009, The Honorable William H. Webster, Chair, accessed June 23, 2016 09:27, https://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission

[10] 902d Military Intelligence Group, Fort Knox, Kentucky, *Insider Threat and Terrorism*, accessed June 23, 2016 11:05, http://www.knox.army.mil/partners/902d/threat.aspx

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

Recommended Actions

1. Organization leadership should take appropriate steps to develop operational plans to identify and respond to insider threats to protect employees, customers, and the surrounding community.
2. Employers can take the initiative to promote awareness among employees of the reporting resources that can provide outside assistance from law enforcement.
3. Finally, organizations should participate in the Florida See Something Say Something program. Suspicious activity can be reported through the Florida Department of Law Enforcement website (http://www.fdle.state.fl.us) or by phone at 1-855-FLA-SAFE (1-855-352-7233).

Insider Threat Resources

Rand Corporation

- Research on terrorism and homeland security
- http://www.rand.org/topics/terrorism-and-homeland-security.html

Stanford University Center for International Security and Cooperation

- Research on international security issues
- http://cisac.fsi.stanford.edu/

Software Engineering Institute CERT Program

- Research and data on cyber threats
- http://www.cert.org/

Department of Homeland Security Protective Security Advisor

- Insider threat programs and information
- https://www.dhs.gov/protective-security-advisors

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

Design 101

Resolution: From Screen to Print

Here's a scenario: you find a picture online you like. You print it out after getting the permissions you need, but it doesn't look quite like it did on the screen. Why? Probably a few reasons, but the main one has to do with resolution.

First we'll consider the starting point of your image: your computer screen. Everything on a screen is built out of many small squares called pixels, an abbreviation of "picture element." Pixels are stacked on top of each other to form the images you see, and on a computer screen, there are 72 of them for every inch, meaning the resolution of the screen is 72 pixels per inch (ppi).

On paper, however, there need to be more pixels in an inch for the human eye to stop seeing them as tiny squares. The number most people have arrived at as an ideal amount is 300ppi. So when you print an image you found online, it printed at 72ppi, a low resolution for paper. The difference between a printed 72ppi image and a 300ppi is one you won't notice until they're side-by-side, but it's a noticeable one and it can give your work an edge of higher quality. Here's an example:

3″ x 4.764″
72ppi
216 x 343 pixels

This image is roughly 3 x 4.5 inches. If you were looking at it on your computer, it would be displaying at 72ppi, which means it would have the pixel dimensions of 216 x 343 pixels. If the web was as far as this image was going to go, that's as many pixels as you'd need. But, if you wanted to print this image out and have it look as clear as it does on the screen, the pixels would need to be a lot smaller to create the effect of a sharp image with smooth curves. The shrinking of the pixels, however, means the image itself gets smaller.

0.72″ x 1.43″
300ppi
216 x 343 pixels

Now there's 300 pixels for every inch but the image measures at around .5 x 1.5 inches. To get the sharper quality, you gave up image size. If you simply try changing the resolution to 300ppi using a program like Photoshop, you'd end up with this next image:

Photoshop added all of the extra pixels but, because it had to "guess" what each one should look like, the result is a blurry image. Unfortunately, there's no real way to go from low resolution to high resolution without making the trade-off of size right now.

3″ x 4.767″
300ppi
900 x 1430 pixels

The question then becomes: how do you print images from the computer that are both not-tiny and not-ruined if you don't have an image editing program such as Photoshop? The easiest and most accessible answer is to start with big images. Make use of search-specific tools on sites like Google and specify that you want large images. The resolution of a large 72ppi image off a Google search can be changed into a nicely sized 300ppi image. Try to stay above 1000 pixels on all sides if you can; that'll get you about three to four inches of sharply printed image. If you don't plan on printing, 72ppi images are fine.

Take away: Images are probably not going to look the same in print as they do on screen, and the main reason is resolution. Once you understand that, you can use it to your advantage and make use of the right resolution for your task.

Contact us:
Phone: (850) 410-7645
Email: 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.**

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 Hacker Installs a Credit Card Skimmer in 3 Seconds

http://thehackernews.com/2016/03/credit-card-skimming-hack.html

- Hardware and software for credit card skimmers are becoming smaller and easier to use
- This video, real footage from a convenience store in south Florida, shows how easy it is for criminals to install skimmers

Analyst note: Always be aware of credit card terminals, because skimmers are great at tricking you into thinking they are real. Regularly check your accounts for suspicious activity or charges you do not recognize so that you do not become a victim of these scams.

CNBC taught a horribly botched lesson in password security

https://www.engadget.com/2016/03/30/cnbc-botches-password-security-lesson/

- The news site posted an article about how to make sure you have a strong password, and allowed readers to test their password in a text entry box
- Although the article said passwords weren't stored, researchers discovered that the site sent the password to a spreadsheet and multiple third parties
- The passwords were also transmitted unencrypted, which means they could have been intercepted by someone snooping

Analyst note: Although a hard lesson for this news site to learn, it just goes to show that you can never be too safe with how you share your password. Make sure it is strong, long, and secret.

Hackers only need your phone number to eavesdrop on calls, read texts, track you

http://www.computerworld.com/article/3058020/security/hackers-only-need-your-phone-number-to-eavesdrop-on-calls-read-texts-track-you.html

- Flaws in cell phone networks could be exploited by criminals to eavesdrop on you
- The vulnerability in the cell networks, Signaling System 7 (SS7) has been around for many years, but has never been fixed

Analyst note: Although we are assured that networks are completely secure, this article is a good cautionary tale about how a malicious actor could surveil others completely anonymously and secretly.

Beware of keystroke loggers disguised as USB phone chargers, FBI warns

http://arstechnica.com/security/2016/05/beware-of-keystroke-loggers-disguised-as-usb-phone-chargers-fbi-warns/

- In April, the FBI released an advisory warning about Wi-Fi sniffing devices disguised as phone chargers
- Wi-Fi sniffers may have the ability to secretly steal passwords or other input typed into wireless keyboards

Analyst note: Although this device was largely a proof of concept, the FBI's warning stemmed mostly from the fact that similar devices are easily programmable to sniff out data that isn't transmitted securely over Wi-Fi.

Uber fraud: Scammer takes the ride, victim gets the bill

http://www.csoonline.com/article/3059461/data-breach/uber-fraud-scammer-takes-the-ride-victim-gets-the-bill.html

- Criminals have started selling the log-in credentials for users of Uber, a popular ride-hailing web service, on the Dark Web
- Using these credentials, others can request rides, and pay for the ride with the credit card attached to the account
- Reports indicate that these credentials are selling for around $4 apiece

Analyst note: It is unclear if these credentials are the result of poor password security of users, a hack of Uber servers, or a combination of both. It is important to keep an eye on any apps you use that include credit card information, as they may be attractive targets for cybercriminals.

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