The Beacon

Florida Fusion Center #17-008 | Cyber and Critical Infrastructure Report | January 2017 Issue #12

Summary

Unwrapping the Internet of Things - You may have recently received a smart device as a gift. We discuss what security risks are involved.

Cyberbullying and Social Media - Bullying isn't new, but check out how social media sites are trying to fight back.

iOS App Permissions - Before you accept permissions on that cool new app, know what information you might be giving away.

Biometrics: Can We Depend on our Bodies? - The neat futuristic tech from movies is in the here and now… but there are hazards!

Social Media and Terrorism - We discuss social media and its recent impact on malicious acts of terrorism.

FDLE Provides Online Security Awareness Toolkit - If you See Something, Say Something. Find out how to get resources to educate others about reporting suspicious behavior.

Raster and Vector: Why You Should Care - File format is an important issue in cybersecurity, but is also important when making polished products. Here's why.

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's Crystal Ball: What's in Store for 2017

The past year certainly had its fair share of cyber issues, but we at Secure Florida wanted to share our predictions for cyber issues in 2017. Here's what we see in the coming year.

DATA BREACHES

Last year had some major data breaches, such as the University of Central Florida (63,000 student, faculty, and staff records), Yahoo (one billion user accounts), and of course the Democratic National Committee's email leak that generated weeks of news headlines.

The bad news for 2017? Data breaches will still be a problem. The good news? The value of compromised data is much lower. The biggest change is in stolen medical records: in 2012, an individual's medical record was worth around $50 on the dark web, but now they're selling for as low as $1.50 to $10. Security experts attribute this dramatic decrease to supply and demand. In 2015 alone, 112 million medical records were stolen, so the glut of content has driven down prices.[1] This may signal a decrease in data theft for profit.

RANSOMWARE

Because of falling rates of return for stealing data, hackers have instead turned to ransomware to make money. Cyber criminals have made millions from ransomware, and continue to develop new variants.

In 2017, we may even see the rise of the "ransomworm." Currently, ransomware propagates as a virus, infecting only the victim computer and any files to which it has access (like a shared drive). But last year, Microsoft warned about a ransom*worm* called ZCryptor that copies itself onto removable drives like USBs.[2] Although ransomworms don't appear to be as popular as ransomware right now, we can expect that cybercriminals are working to develop ransomware that acts as a worm and infects as many computers as possible… so that they can increase their payday with a single infection.

We also expect to continue to see Ransomware as a Service (RaaS). With RaaS, cybercriminals write the malware, sell the ransomware to someone else to use, and then take a cut of those profits. This greatly expands the market for those who would use ransomware, and more attractive to those criminals who may not have much cyber expertise.

PHISHING

Virtually every type of cyber incident, attack, or breach includes some type of phishing. As the saying goes, if it ain't broke, don't fix it. This attack vector has been successful for the last few decades, so don't expect phishing emails to disappear anytime soon. For ways to protect yourself from phishing, ransomware, and data breaches, check out our resources at secureflorida.org.

[1] http://www.csoonline.com/article/3152787/data-breach/black-market-medical-record-prices-drop-to-under-10-criminals-switch-to-ransomware.html?idg_eid=56d641ca26c6134c16a2abcee62eb3d4&utm_source=Sailthru&utm_medium=email&utm_campaign=CSO%20After%20Dark%202016-12-27&utm_term=cso_after_dark

[2] https://blog.kaspersky.com/zcryptor-ransomware/12268/

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

Cyber Threats

Unwrapping the Internet of Things

As we begin 2017, the Internet of Things (IoT) continues to expand into more areas of our lives. The IoT specifically refers to the ever-growing network of physical objects connected to the Internet via wireless and wired connections,[1] and goes beyond the standard computer to things like that new Wi-Fi enabled coffee maker you purchased during the holiday season. IHS Technologies predicts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020.[2]

One of the largest concerns shared by security researchers is that the average consumer does not appropriately secure these devices. In October 2016 malicious actors exploited this lack of security, and used hacked IoT devices in one of the largest cyber attacks to date. They directed a botnet of devices infected with Mirai—a malware strain that infects vulnerable IoT devices such as poorly-secured routers and IP cameras—to conduct attacks on Dyn, an Internet infrastructure company that provides critical technology services to some of the top destinations on the Internet. These included Netflix, Amazon, Twitter, and PayPal.[3] Devices in the Mirai botnet (without the owner's knowledge) searched the Internet for other devices that still used default usernames and passwords. Once located, the botnets infected the new devices and then forced them to attack still other devices, overwhelming them with legitimate traffic requests and forcing them offline. This technique is known as a distributed denial of service (DDoS) attack.

[1] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
[2] http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#607cc2df4ba5
[3] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

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

For security-conscious consumers who want to change the default usernames/passwords on their IoT devices, many find it's simply not an option. The login information is hardcoded into the firmware itself, preventing alterations by future owners. US Senate Intelligence Committee member Senator Mark Warner voiced concern over this vulnerability: "Manufacturers today are flooding the market with cheap, insecure devices, with few incentives to design the products with security in mind, or to provide ongoing support."[4] In December, Austrian security firm SEC Consult unearthed a pair of "backdoor accounts" in more than 80 different IP Sony cameras. A scan of the web by security researchers using freely available IoT search engines indicated that at least 4,250 devices were reachable as of last month.[5] At the outset of the Mirai attack, researchers concluded that more than 500,000 devices contained vulnerabilities that made them susceptible to infection by Mirai.[6]

Ultimately, there is no way to avoid becoming the target of a DDoS campaign from Mirai botnets. However, it is important to use the following mitigation strategies to reduce the potential damage:

- Research devices before purchase to ensure that settings are editable upon acquisition.
- Change the default usernames and passwords, and place devices behind network firewalls.
- Consider retaining DDoS protection services and establish alternate channels for critical Internet traffic.

As the IoT grows, we expect botnet campaigns such as Mirai to continue. It is important for security professionals and consumers alike to recognize possible vulnerabilities with the smart devices that are quickly becoming part of our everyday lives.

[4] http://www.reuters.com/article/us-cyber-attacks-china-idUSKCN12P1TT
[5] https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons/
[6] http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet

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

Cyber Highlights

Cyberbullying and Social Media

As with most things, technology has had a modernizing effect on bullying. Thirty years ago, bullying could be "controlled" by managing the time a child spent in the physical company of others and ensuring confrontations were kept cordial. Nowadays, however, children are much more connected though social media platforms and can talk, or be talked to, with ease at any time. The convenience of being able to talk with friends unfortunately comes packaged with an easy avenue for bullies to exploit. No social media platform wants to see their service being used for malicious purposes, so most platforms have implemented precautions to keep the spaces bully-free.

Facebook offers blocking and reporting functions to remove malicious content and prevent users from viewing more content from a source from then on. Blocked users are not notified they have been blocked, so as to keep any backlash to the blocker minimal. Reported content will be removed by Facebook if it meets the requirements of Facebook's Community Standards found here: https://www.facebook.com/communitystandards. Facebook also hosts a Bullying Prevention hub which contains information, tools, and resources to children and parents.[1,2]

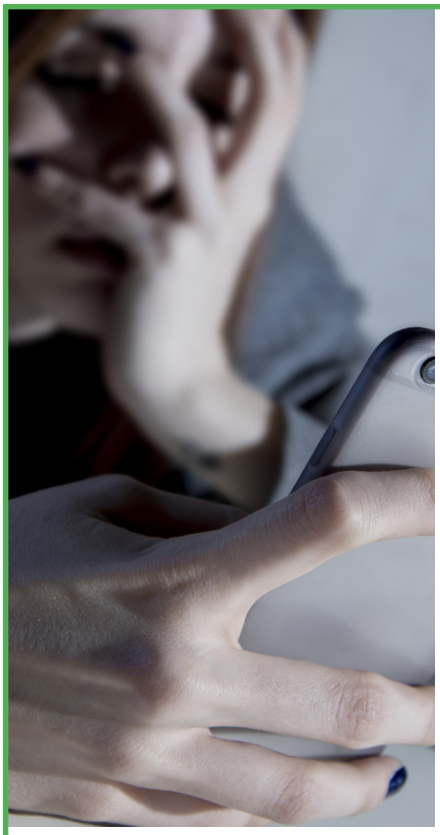
Twitter offers blocking and reporting services also. Users can be unfollowed and blocked, preventing their content from being seen in your feed as well as preventing them from following you. If activity persists, the issue can be reported to Twitter directly and handled on a case-by-case basis. Reports can even be made by others on behalf of the abused.[3]

Instagram offers similar services to Twitter; pictures can be reported and users can be blocked. The platform is also specific in ways to report accounts that may be impersonating as others. Instagram also offers a feature that allows users to filter the comments they see, with comments containing words Instagram has deemed "deplorable" removed. The list can be customized by the user to include their own additions as well, such as personally triggering nicknames or terms.[4]

[1] https://www.facebook.com/safety/bullying/
[2] https://www.facebook.com/help/420576171311103/
[3] https://support.twitter.com/articles/15794
[4] http://www.theglobeandmail.com/technology/instagram-moves-to-battle-online-abuse-with-new-filters/article31824457/

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



YouTube also offers reporting services. If uploaded content violates their harassment policy, it will be removed if reported. Videos can also be flagged, queuing it for review by YouTube's 24/7 review. If a specific user is deemed toxic enough, their entire account can be terminated.[5] YouTube is also spearheading a new program titled "YouTube Heroes," in which users are rewarded for good moderation activity, such as flagging toxic content so it never reaches an audience.[6]

To only name a few, Facebook, Twitter, Instagram, and YouTube each offer methods of keeping bullying to a minimum while on their platforms. But while content can be removed and users can be blocked, damage may already have been done. Many campaigns have been launched to prevent the bullying from happening in the first place, such as the US Department of Health & Human Services stopbullying.gov. Until such a time as bullies don't bully, social media platforms will strive to keep their virtual space as safe as they can for their users.

[5] https://www.youtube.com/yt/policyandsafety/reporting.html
[6] https://support.google.com/youtube/answer/7124236?hl=en
[7] https://www.stopbullying.gov/

iOS App Permissions

In the past couple of issues, we have presented tips on mobile device safety (*Mobile Computing Safety 101: Apps* and *Android: App Permissions Made Simple*). Since the last issue covered Android apps, we didn't want to exclude our readers who use Apple devices.

The big difference between Android and iOS app permissions is that the former will tell you before you download an app what permissions it will access. When you download an iOS app, you get pop-up alerts to enable certain features once the app is on your device.

The following pages contain descriptions of iOS permissions. As with Android, most apps have legitimate reasons for the permissions, but the Possible Risks paragraph notes what bad things could happen if more dodgy apps include these permissions.

Keep in mind that in Settings, iOS does allow you to disable certain permissions for individual apps. Although it may affect the app's functionality, you may choose to disable certain things (such as Contacts) if you are concerned about sharing that information.

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

Permission	Description
Location services	Allows tracking your device based on its GPS coordinates; used by countless apps: Google Maps, Yelp, and 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.
Contacts	Required for messaging apps, apps like Twitter for sharing tweets, and many gaming-with-your-friends apps. **Possible risks:** *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.
Calendars	May be used for task management or organizational apps. **Possible risk:** *Privacy.* Your calendar may include sensitive or personal information about you.
Microphone	Allows access to your microphone for recording purposes. **Possible risk:** *Privacy.* An unscrupulous app might covertly turn your microphone on and off, recording without your knowledge.
Photos	Allows access to photos and videos stored on your device. **Possible risk:** *Likely none.* Theoretically, an unscrupulous app might steal this data.
Camera	Allows access to photos and videos stored on your device. **Possible risk:** *Likely none.* An unscrupulous app might take photos or record video without your knowledge.

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

Reminders	Allows you to set alarms, create location-based alerts, and can sync with your calendar. **Possible risk:** *Privacy.* Since Reminders integrates location-based data and syncs with your iCloud, it may have access to information you may not want to share.
Bluetooth Sharing	Allows identifying and connecting to Bluetooth devices. **Possible risk:** *Likely none.* It may affect your battery life slightly.
Speech Recognition	Sends recorded voice to Apple to process your requests. **Possible risk:** *Likely none.* A third party app could access that data without your knowledge.
HouseKit	Works with Internet of Things devices such as Apple TV and smart thermostats to allow operation through your device. **Possible risk:** *Likely none.* Compromised compromised or devices could allow someone to control these smart devices.
Media Library	Allows access to your media library or downloaded music. **Possible risk:** *Likely none.* An app may use this content to target advertising.
Background App Refresh	Allows apps to refresh when on Wi-Fi or cellular data. **Possible risk:** *Likely none.* However, this may affect your battery life (or cellular data limit!).
Motion & Fitness	Allows apps to access sensor data such as body movement, step count, and stairs climbed. **Possible risk:** *Privacy.* Theoretically, an unscrupulous app might take this data for their own purposes.

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

Biometrics: Can We Depend On Our Bodies?

Biometric data is increasingly being used as a secondary or even a primary form of identification. As biometric identification is integrated even more into our lives, the associated risks are becoming clearer.

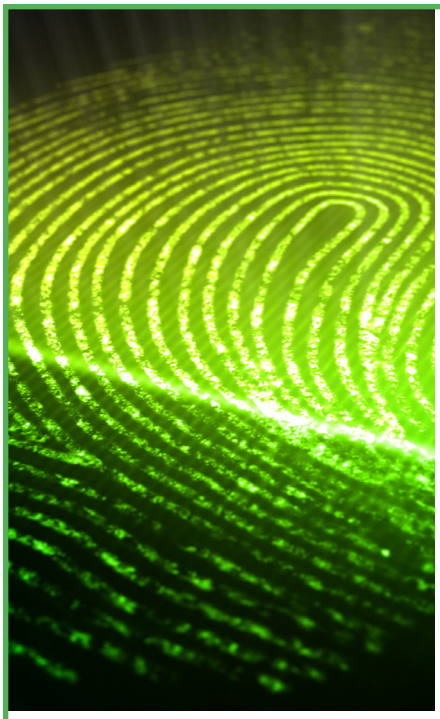
Biometric identification refers to the science of identifying humans by measuring some physiological characteristic related to the shape of their bodies. (It falls into the "something you are" category of the three identification factors. The others are something you know—like a password, and something you have—like a swipe card.) Examples of biometric identifiers include fingerprints, facial recognition, DNA, palm prints, and retinal scans.

Biometric identification risk is directly related to the "security v. privacy" debate. This relationship makes things problematic as the line between them differs from person to person. The list below highlights several risk factors you should be aware of before you turn over your biometric data to a third party.

1. Biometric data can be stolen, compiled and aggregated without your knowledge, and then used without your consent. A fingerprint lifted from a glass, saliva from a cigarette, or even dandruff from a coat collar is not just the stuff of movie thrillers.
2. Biometrics are YOU. You can't change your fingerprint the way you can a password. If that information is compromised, the thief could get access to anything you use biometric identification for.
3. Who has access to your biometric data and how will they use that information? This opens the door to government tracking, business tracking, or persistent marketing. Imagine walking into a store and being bombarded with ads related to information based on your body mass index, weight, height, or previous purchase information.
4. How do you withdraw access after you have previously allowed it? Once it's exposed it can never again be confidential (see Tip 2). You have to depend on the word of the security personnel that it won't be used again.
5. Biometric technology is not inherently secure; can be hacked or reversed engineered just like other types of data. It takes an expert, but someone with knowledge and experience can bypass or fake biometric identification.
6. The technology is not perfect. What are acceptable failure rates? False rejects (denying access incorrectly) and false accepts

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



(allowing access incorrectly) have different impacts depending on the situations in which they are being used. Failing to get access to your phone using a fingerprint may be quite annoying; however, receiving the wrong medication from an emergency room could be catastrophic.

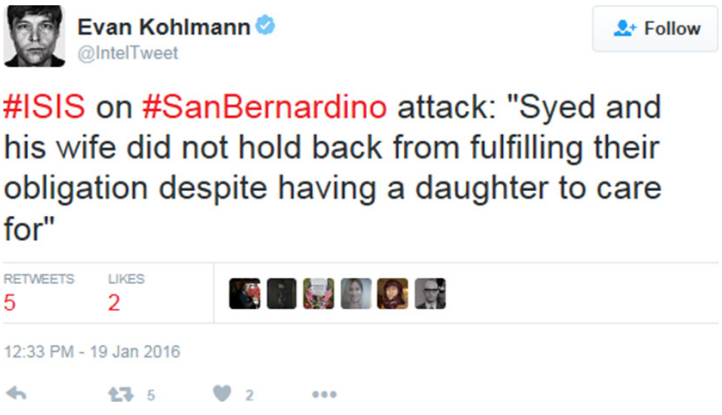
The use of biometric data may soon become so widespread that de facto standardization will lead to its use being mandatory.[1,2,3] It is important to understand biometric identification's role and the steps we can take to secure our own data as best we can. The above items list a few, but not all, of the risks that you should take into account as biometric identification continues to become embedded into our everyday lives.

[1] https://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137
[2] https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits
[3] https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf

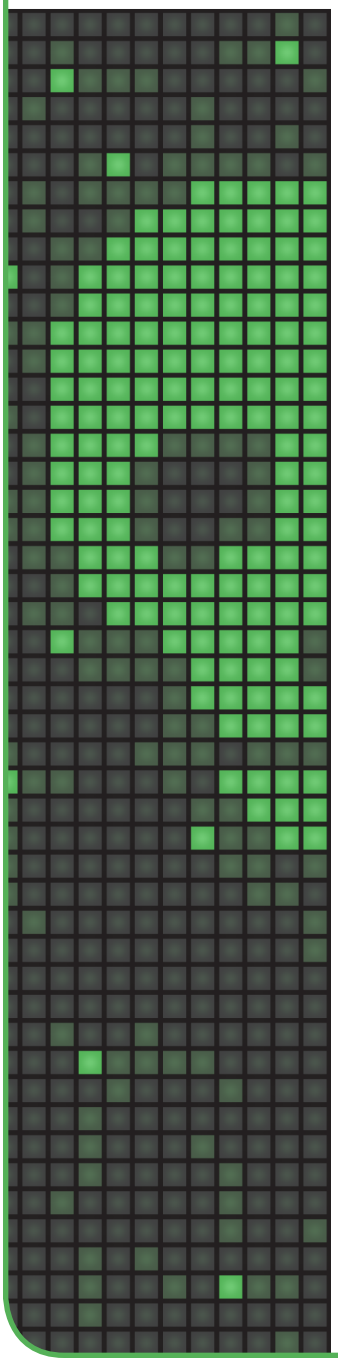
Fighting Terrorism on Social Media

Early last month the news broke that Facebook, Twitter, YouTube, and Microsoft are joining forces to "curb the dissemination of terrorist material online."[1] The announcement comes on the heels of a criticism from the UK Parliament's Home Affairs Select Committee, claiming that the companies are "consciously failing" at keeping their sites free from extremist content.[2]

More than a year ago, President Obama referred to the Islamic State Group (IS) as "a bunch of killers with good social media."[3] Less than two weeks later, Syed Farook and Tashfeen Malik murdered 14 people at a holiday party in San Berbardino, CA. Immediately, IS jumped on social media to appeal to the hearts of other potential followers by capitalizing on the now-famous picture of their daughter's empty crib.



Far from keeping plans secret, IS prefers to crowd source its violence—making it both more dreadful and harder to prevent. The truck-attack scenario, suggested and described on IS social media, resulted in the killing of more than 80 people in Nice (July 2016), and 12 in Berlin (December 2016) with 48 injured. The Tsarnaev bothers, responsible for the Boston Marathon bombing in 2013, learned the "pressure cooker" technique on social media. According to 2015 report by the Quilliam Foundation, IS releases, on average, "38 new items per day—20-minute videos, full-length documentaries, photo essays, audio clips, and pamphlets, in languages ranging from Russian to Bengali."[4]



But is it the Internet's fault?

In the US, the Communications Decency Act of 1996 provides immunity from liability for providers of websites who publish information posted by others. There are similar regulations in the European Union (EU), but with several restrictions limiting the immunity.[5] However, in both jurisdictions, this immunity is increasingly tested by the governments, politicians, and the populace for each terrorist attack that finds its origins on Twitter or Facebook.

In addition, individuals are turning to the courts, suing the so-called Internet giants for failing to curb the spread of the terrorist propaganda posted on their sites. There are several suits currently pending in the US and the EU.

Now, with increasing pressure from the EU, as well as the pending lawsuits, Facebook, Twitter, YouTube, and Microsoft are creating a shared industry database of violent imagery and other recruitment materials. Once such material is posted, it will be identified, added to the database, and removed from the site. Each item will be tagged with its unique "hash value," which can be used by anyone to identify similar content on their site. Other companies will be encouraged to join the initial four.[6]

There are a couple of issues that still need to be resolved. First, each tagged image and video needs to be reviewed by a human before removal, which is very labor intensive. But no site owner wants to leave to a software program such a blatant limit on free speech. Which brings us to the second issue: the fine—and blurry—line between "controversial but legal" and "plainly unacceptable." The four companies want to stay as far away from censorship as they can, stating, "We are committed to protecting our users' privacy and their ability to express themselves freely and safely on our platforms."

[1] http://arstechnica.com/tech-policy/2016/12/twitter-facebook-microsoft-youtube-terrorist-material-removal/
[2] http://www.washingtontimes.com/news/2016/aug/25/uk-reports-accuses-social-media-companies-conscious/
[3] http://www.businessinsider.com/barack-obama-isis-social-media-2015-11
[4] https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/
[5] http://www.americanbar.org/content/dam/aba/publishing/communications_lawyer/pinto.authcheckdam.pdf
[6] http://www.kolotv.com/content/news/Facebook-Google-Twitter-accused-of-enabling-ISIS-408011125.html

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

Critical Infrastructure

FDLE Provides Online Security Awareness Toolkit

Terrorism in the United States in 2017 is likely to originate from homegrown violent extremists who already reside in our communities.[1] Because these individuals develop their targets and tactics based on views inspired by other violent extremists, the consequences of future violent attacks are expected to vary greatly.[2] Terrorists weigh the results of a planned attack against what it takes to obtain the most desired outcome, choosing actions that cause substantial damage with minimal risk of failure. This explains why some recent attacks have occurred using vehicles and explosive devices, usually in public places with little security.

Attacks by inspired individuals are difficult to stop. However, when citizens report information about suspicious activities such as increasingly irregular or bizarre interactions or purchasing bulk items that may be used for bomb making, that may be the tip to successfully quash a terrorist attack before it happens.

In 2017, the general public remains a key component to stopping terrorism, through efforts like the "If You See Something, Say Something™" program as well as through direct reports to local law enforcement. In an attempt to raise security awareness, the Florida Department of Law Enforcement has created an "If You See Something, Say Something™" online toolkit for students, the general public, and select business sectors (such as retail and healthcare). This toolkit provides a variety of fact sheets, training videos, and flyers that can raise awareness on how to identify and report suspicious activity.

You can find these resources here:
http://www.fdle.state.fl.us/cms/FFC/S4/Tools.aspx

[1] George Selim, Department of Homeland Security Director of Community Partnerships, Statement for the Record, for a Senate Committee on the Judiciary, June 28, 2016, accessed December 9, 2016, https://www.dhs.gov/news/2016/06/28/statement-record-dhs-ocp-senate-judiciary-subcommittee-oversight-agency-action.
[2] Schmid, Alex P., Radicalization, De-Radicalization, Counter-Radicalization: A Conceptual Discussion and Literature Review, International Center for Counter-Terrorism Research Paper, March 2013, ICCT, The Hague.
[3] Miller, Gregory D., Terrorist Decision Making and the Deterrence Problem, Studies in Conflict and Terrorism, 36: 132-151, 2013, Routledge Taylor and Francis Group.

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

Design 101

Raster and Vector: Why You Should Care

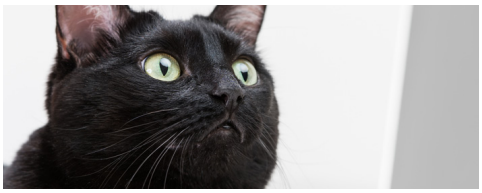
Raster and vector are words you might've heard around your workplace, but unless you're the designer or someone extremely interested in design in your spare time, chances are you don't know what they mean or why they matter. Understanding the differances between raster and vector can be a big advantage to you, saving you time and making for sharper looking work.

The image to the left is an example of a **raster image**, the name given to images that are built with pixels. Thousands upon thousands of tiny squares in various colors are stacked on top of each other in such a way that the eye stops seeing squares and starts seeing shapes. When you're making raster images, you tell the computer, "these pixels are X color, these pixels are Y color, etc." Once a pixel is coded for a color, it stays that way, so stretching an image out moves those pixels around, making them *resolution dependent*. This means that the state of the image is *dependent* on its dimensions and resolution. Scaling a raster image will affect the image's appearance because the pixels were moved around.

Vector images, like the one to the left, are made with algorithms. Instead of building an image up with individual pieces, vector images are built with points. You tell the computer where the points are and to fill the space between them in certain ways. For instance, to make a blue square, you would give the program the coordinates for the four corners of the square and instruct the program to fill the space within the points with blue. The "fill" is embedded in the algorithm that built the shape, so a mathematical instruction replaces individual pixels. Since there are no pixels, vector images can be infinitly scaled; the algorithm will simply be multiplied to the appropriate size.

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

Raster



Pros:

- Lots of detail to work with; each pixel is editable
- Much easier to manipulate effects with
- Tends to be more accessible

Cons:

- Cannot be enlarged without sacrificing the sharp appearance
- Tend to contain larger file sizes than vector files
- Time-consuming to edit

Common uses:

- Photographs
- Adding effects and filters

Common file extensions:

- .JPG, .PNG, .GIF, .TIF

Vector

Pros:

- Highly scalable in any direction while retaining sharp appearance
- Smaller file sizes since only the points take up digital space
- Easier to edit

Cons:

- Limited use of effects and filters
- Difficult to achieve the level of detail that can be achieved in raster images
- Less accessable

Common uses:

- Type
- Logos

Common file extensions:

- .EPS, .SVG, .PDF, .AI

Now all that sounds interesting, but how does it help you? If you do any work with images, it'd be nice to know what kind of images you have at your disposal. Even better than that, you can learn how you can use that information to your advantage.

If, for instance, you decided that you wanted the main color in your logo changed, but you knew that you had a time limit on how long you had to see that done. If you knew that there was a vector version of your logo on hand, you'd know that something like changing color would be a quick and easy job. If all you had was a raster version, you'd know you'd need more time since changing colors on a raster image is much more time consuming.

Or, if you were told that you had access to a billboard for an upcoming project, you would know the benefits of considering vector artwork since you are aware of vectors' scalability. Scalability is a major benefit of vector images, so if you ever find you need an image that'll be used in various sizes, having a vector version would be a good idea.

That's not to say that raster images are inferior, they are just better suited to instances when you know what size you need them in and they stay that size. Scalability doesn't always make up for the level of detail you can get in raster images. Since vectors don't support filters well, they aren't that great for photographs either. It all comes down to how and where the image will be used.

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

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.

Be careful, there's a fake Google out there

http://mashable.com/2016/11/21/fake-google-domain/#kAd9Eqk4Taqa

- In November, a news site noticed some strange traffic when reviewing their site analytics: a spam site was redirecting traffic to the domain ɢoogle.com.
- Google Analytics found that the first character is coded as a special character for the Latin small-capital G, but had tricked users across a variety of websites into thinking it was google.com.

Analyst Note: This is another cautionary tale about why it is important to always pay attention to a link before clicking on it, because all it takes is a tiny change to make something look authentic and trustworthy.

A beginner's guide to beefing up your privacy and security online

http://arstechnica.com/security/2016/12/a-beginners-guide-to-beefing-up-your-privacy-and-security-online/

- The other articles in this section highlight some of tactics cybercriminals are using to target their victims. This article contains some of the necessary steps you should take to keep them at bay.

Analyst Note: Strong passwords, updating software patches, and maintaining a healthy suspicion of links and attachments when surfing the web: these are all vital components to maintaining a good cybersecurity posture.

91% Of Cyberattacks Start With A Phishing Email

http://www.darkreading.com/endpoint/91—of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

- Phishing emails have been around for a number of years, but hackers are still using them very successfully to dupe people.
- PhishMe, a company that trains users to avoid falling for phishing emails, found that most people fall for phishing emails that are personalized, grammatically correct, and written consistently with business functions.

Analyst Note: If it's not broken, don't fix it: people still fall for phishing, so criminals will continue to use it as a tactic. Always maintain a healthy suspicion about every email you receive.

14 eyebrow-raising things Google knows about you

http://www.computerworld.com/article/3148794/personal-technology/14-eyebrow-raising-things-google-knows-about-you.html

- Google stores a great deal of information about its users from browser/search history to location based data.
- You can view for yourself what types of data Google maintains about you—and no one else can see it unless they get access to your account.

Analyst Note: While there is a lot of convenience to Google crunching the numbers on your habits to create a better user experience, it highlights the importance of good security protections such as strong passwords and two-factor authentication to keep prying eyes from getting access to your account (and that content).

Massive cybercrime infrastructure demolished

https://www.helpnetsecurity.com/2016/12/02/massive-cybercrime-infrastructure-demolished/

- Last month, an international cybercrime ring was taken down as part of a joint multi-year operation with more than 30 US and European law enforcement agencies.
- The Avalanche network used hundreds of servers and human "mules" to spread malware that infected as many as 500,000 computers a day, resulting in hundreds of millions of euros in monetary losses over four years.

Analyst Note: Although a sophisticated criminal enterprise, the attacks usually started with a simple phishing email. Always be suspicious of emails with links or attachments.

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 anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure analysts who work to protect Florida's infrastructure.

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

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

The Beacon

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

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

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

The Dispatch

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

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

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

Class topics include:

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