The Beacon

Florida Fusion Center #15-002 Cyber and Critical Infrastructure Report January 2015 Issue #5

Summary

On Beyond Clip Art — Beginning December 1st 2014, Microsoft Office discontinued its Clip Art and image library. Fear not, those with copyright concerns—the search engine Bing has an image search to help you.

Smartphone Security — Smartphones are increasingly becoming our lifelines to the world. Learn about ways to maximize the security of your mobile devices.

Social Media - Your Digital Footprint — We can now chronicle our entire lives online through social media, but that can carry unforeseen consequences. We put together some best practices for knowing your digital footprint.

Data Breaches, The New Normal — In the Age of the Data Breach, how do you protect your credit card information? We offer our tips for protecting yourself and your wallet.

Industrial Control Systems Targeted — Industrial control systems are high value targets for terrorists both foreign and domestic. Here are some best cybersecurity practices for system administrators and end users.

Drone's Threat to Critical Infrastructure — From colliding with airplanes to delivering explosive payloads, unmanned aircraft systems present several concerns. So far, though, we have seen only near-disasters.

Contents

About *The Beacon*

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

Secure Florida is an Internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC). The FIPC was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure protection analysts. FIPC analysts work to protect Florida's infrastructure through FDLE's Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

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

We welcome your feedback.
www.survemonkey.com/s/TheSFBeacon5

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

Editor's Corner

On Beyond Clip Art: Bing Image Search

Hooray – no more clip art![1] Clip art has been the bane of many a brochure, presentation, and poster since 1993.

In the early years, of course, we were constrained by the lack of digitally available images, copyrighted or otherwise. Clip art was virtually everywhere, legal to use, and simple to insert into any file. For more than a decade, however, we have had instant access to thousands (probably millions) of images with a simple right-click/copy. And yet, there was still that pesky, little copyright snag….

So how do we protect our organizations and ourselves from a copyright infringement suit while still generating briefs, reports, and analyses that don't look like an ode to the '90s? Microsoft has provided an alternative: the revised **Bing Image Search** (www.bing.com/images/) now includes several search tools, including size, color, type… *and license*.

Suppose, for example, you want to illustrate a report on drug trafficking. You'd type "drug trafficking" into Bing's Image Search field, hit Enter, and get several pages of applicable images. However, you can refine your search by sorting on "License." The option "Free to share and use" will still return several pages of images, but these images can be used by anyone for any non-commercial use, as long as they aren't modified.

Bing has categorized their images with five *Creative Commons*[2] copyright licenses. The link "Learn More" provides more detailed definitions.

- Public domain
- Free to share and use
- Free to share and use commercially
- Free to modify, share, and use
- Free to modify, share, and use commercially

Google Images also has added a copyright filter to their image search (under Search-Tools/Usage-Rights), but the labels are not quite as self-explanatory. In any case, both Bing and Google will provide you with visually pleasing —and legal— illustrations, photographs, and tables.

For those feeling some CAN (clip art nostalgia), you might appreciate this eulogy: http://www.theatlantic.com/technology/archive/2014/12/a-eulogy-to-clipart-in-clipart/383322/.

---

1 **http://www.dailytech.com/RIP+Microsoft+Clip+Art+1993+to+2014+Youll+be+Missed+Sort+of/article36958.htm**

2 **Creative Commons is a non-profit organization devoted to expanding the range of creative works available for others to build upon legally and to share. Learn more about them here: (http://en.wikipedia.org/wiki/Creative_Commons).**

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

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

Cyber Highlights

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

Contents

Smartphone Security

As mobile devices become bigger parts of our lives, we increasingly carry our personal information around in our pockets. Most of us keep our smartphones and tablets linked to our online accounts, and if someone gets access to our devices, they gain access to information allowing them to steal our money or our identity. But there are several steps you can take to help protect your information.

The first layer in protecting your information is a **lock screen**. Lock screens take several forms—from no security (swipe-to-unlock) to higher levels (passcodes or fingerprints). The latter insure that someone who steals, or happens upon, your device cannot access your information. Each locking method has pros and cons so it's best to find a balance between security and convenience. If a lock screen is so tedious that you disable it, it won't do any good.

Encrypting your device is another great way to secure your information. Encryption encodes information so that it requires a key, usually a password, to unlock. Encrypting your devices means that even if someone accesses the data, it would look like gibberish without the key. Both iOS and Android now have built-in encryption on their devices.[1] If you have a micro SD card or other external storage media, you should also be sure to encrypt those if they contain important or confidential information.

Don't stay logged into your accounts or let your mobile browser "remember" your passwords, especially on email and social media. You can also get third-party apps that require a password to open certain files or apps that usually don't require passwords (such as messages or photos).

Set up remote wiping ability to erase all information if your device is lost or stolen. You can trigger it to execute automatically if too many incorrect passwords are tried, or remotely through iCloud[2] (for iOS devices) or Google Device Manager[3] (for Androids).

Back up your data regularly. This becomes much more important if you have a remote wipe active on your device; you might be more reluctant to wipe a lost tablet if there are files on it that you can't recover.

There are many lost or stolen device recovery apps available. Some can tell you the GPS location of a misplaced device or take a picture when someone unsuccessfully tries to unlock the phone. These can help you locate the device or identify a thief, but it's best to let law enforcement recover a stolen device.

Which leads to the last point: if your phone is lost or stolen, **report it to law enforcement**, as well as to your wireless provider as soon as possible so that they can deactivate service to the phone[4].

1 http://mobileoffice.about.com/od/mobile-devices/a/How-To-Encrypt-The-Data-On-Your-Android-Phone-Or-Iphone.htm

2 https://www.apple.com/icloud/find-my-iphone.html

3 https://support.google.com/accounts/answer/3265955?hl=en&ref_topic=3100928

4 http://gizmodo.com/the-nationwide-stolen-smartphone-database-is-complete-1473076340

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

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

Social Media - Your Digital Footprint

In the twenty-first century, social media has become a virtual microcosm of the real world. No longer just a few weblogs or message boards, social media include a wide array of communication platforms, including messaging, photos, microblogging, games, wall-sharing, music-sharing, and crowdsourcing, among others. And social media has greatly increased the Internet's presence in our daily lives: more than 87% of adults and 95% of teens report that they regularly use the Internet, with 74% of adults and 81% of teens using social media[5].

In an instant, we can share photos, milestone events, and casual musings with virtually anyone on earth, greatly removing many of the barriers between the physical and online worlds. While this helps keep us closer to friends and family, unlimited online sharing also gives complete strangers glimpses into our physical world. There are good and bad consequences to such widespread sharing, and so it is important to take a few basic steps to help maintain a separation between your social media presence, or "digital footprint," and real life.

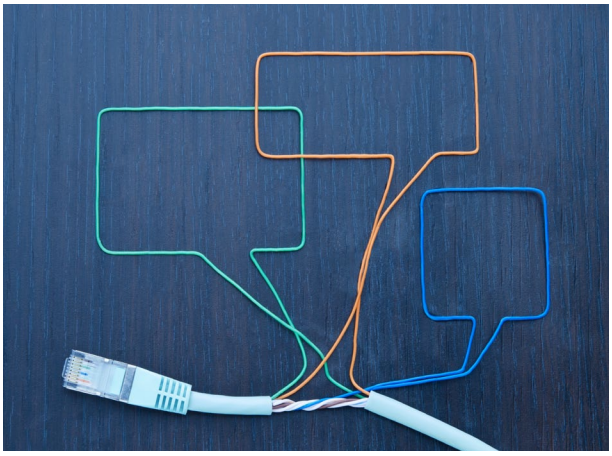
The most important step is to **limit what you put online**. You should do your best to refrain from sharing everything– if you don't want a stranger (or your employer…or mother) to see it, it's best not to put it on any social media. Once something is online, you can't guarantee it can ever be permanently deleted.

5 "Social Media and Young Adults," http://www.pewinternet.org/2010/02/03/part-3-social-media/

The next most helpful thing to keep in mind when assessing your web presence is **privacy settings**. Restricting access to your social media content is the best way for strangers to stay strangers. Default privacy settings can sometimes change without your knowledge, so you should regularly verify your accounts to ensure that they are set to maximum privacy.

You should also regularly do Internet **searches on yourself** so you know the reach of your web presence. You may be surprised to learn the web journal you stopped using a decade ago still appears alongside results for your Facebook or LinkedIn accounts. Deleting old or unused accounts gives you control over your digital footprint.

Anonymity on the web may be going the way of the dodo, but privacy is still important– and controlling your social media accounts is the best way to maintain privacy.



Data Breaches, The New Normal

In late 2013, the retail chain Target was the victim of a widely publicized network intrusion that resulted in the theft of 40 million credit card numbers. In 2014, Home Depot was victim with the theft of 56 million card numbers and 53 million email addresses. Sprinkled around these two major breaches where numerous others, including the US Postal Service, P.F. Chang's, and even a major parking garage operator in the US.

We live in the Age of the Data Breach. It's the state of the world. We hear about new breaches so often that we are no longer surprised. And, by and large, you shouldn't be surprised. Major computer networks, as well defended as they are, attract a lot

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

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

of attention from very capable attackers who stand to make very good money dealing in stolen card numbers.

In the past, if someone wanted your money they had to physically take it by robbing your bank or stealing your wallet. Now someone can literally steal your money, your credit, and your good reputation from another country or continent.

A moving target is the hardest to hit. Unfortunately, the computer networks supporting retail establishments are firmly static and terribly prone to attack. Those who defend computer networks have a frenzied job, requiring constant anticipation and adjustment. Their foe, often hidden in the shadows of the Internet, only has to be right once. With enough attempts they will meet success and they will steal your information.

So, what do you do? You can't protect Target and Home Depot, but you can protect yourself. It may seem like a hopeless case, but it is not. What happens if someone steals your credit card number? The good news is, probably very little for you. Often the credit card companies, or the credit card companies in conjunction with the victim companies, are working in the background to mitigate the damage. You will likely get a new card in the mail without taking any action, sometimes even before you know you have been a victim. Recently, the trend has been to also offer you free credit monitoring for a time.

In general, it is a good idea for you to routinely monitor credit card transactions for suspicious transactions. If you find something you know to be fraudulent—no matter how insignificant— contact the credit card company. The sooner you report it, the quicker it can be resolved.

At some point, no matter what steps you take, your credit card information will probably be compromised— that is an unfortunate byproduct of the world today. Thankfully, there are safeguards in place by credit card companies and businesses to help minimize the effects to your wallet. For more detailed information about consumer protection laws in Florida, please visit the Attorney General's website at myfloridalegal.com.

Industrial Control Systems Targeted

The last year has exposed a dramatic increase in cyber attacks against industrial control systems (ICS) both domestic and international. These systems represent *über* high value targets to foreign threat actors due to the potential for direct control of critical infrastructure facilities such as water, power, gas, and other large-scale manufacturing and production services. The motive for these threat actors is not to engage in hacktivism, steal credit card data, or gain access to industry secrets for competitive advantages; rather they patiently wait for the right moment to initiate wide scale economic disruption and potentially become a public safety threat.

ICS traditionally have been difficult to target due to several factors including the large number of security protections required by regulatory entities and the relatively obscure technologies employed in their design. But as the systems modernize, and hackers become better funded, opportunities increase for exploiting these valuable and sensitive systems. The Stuxnet malware is a prime example of how devastating a successful ICS campaign can be—it destroyed hundreds of uranium enrichment centrifuges in Iran in 2010 and effectively crippled that country's nuclear program. The success of that attack may have acted as a catalyst for the increase we are seeing today in ICS malware campaigns.

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

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

Of particular concern currently are two malware campaigns specifically targeting industrial control systems: *Havex* and *BlackEnergy*. Both are highly sophisticated and gaining successes by leveraging security flaws that need to be addressed.

Such malware campaigns highlight the need for good security practices by end users and systems administrators alike. Some appropriate best practices here are:

- Know your vendors and install updates and patches from trusted sources only.
- Consider validating updates and patches with hash values from the respective vendors (not obtained through the same mechanism as the patches themselves).
- Conduct security awareness training for end users, especially in the areas of:

  Phishing attacks. Phishing emails are a primary attack vector for many of the ICS attacks.

  Watering hole attacks. Here the attacker observes which websites the group often uses, and infects one or more of them with malware.

  Threats associated with portable media storage devices, such as USB thumb drives.

The Department of Homeland Security's ISC-CERT (Industrial Control Systems Cyber Emergency Response Team) provides updates concerning these sophisticated malware campaigns aimed at compromising industrial control systems. ISC-CERT strongly encourages that owners and operators look for indicators of compromise within their environments. The links below provide details, indicators of compromise, and specific products and vendors affected. In addition, ICS-CERT provides customized YARA rules to assist in determining if a system is infected. YARA is a multi-platform tool used by security researchers to identify patterns of malware activity.

ICS-CERT also requests any findings be reported to ics-cert@hq.dhs.gov.

Havex: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

Black Energy: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

Siemens S7-300 system | Uranium enriching centrifuges

Systems like these were targeted by the Stuxnet worm.

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

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

Critical Infrastructure

Drones Threat to Critical Infrastructure

Contents

According to Security Solutions International, more than a million small drone aircraft, or Unmanned Aircraft Systems (UAS), have been sold worldwide in the past few years. They have become commonplace due to their accessibility and affordability. Experts expect the industry to grow from $2.2 billion in 2015 to more than $10 billion by 2025, including more than 100 thousand new jobs.

Why should this concern us? There are several reasons:

- Their use in restricted airspace potentially causing collisions with aircraft.
- The technology has the capability for use in terrorist activities.
- Often UASs are made of plastic or composite materials, and thus are not visible to air traffic controllers.
- UASs can be outfitted with toxic substances, firearms, or explosive devices.
- The technology has the ability to capture photographs and video footage of critical infrastructure facilities.
- UASs can also be effective in drug smuggling into prisons, spying, and cyber intrusion.

The U.S. must be capable of tracking these drones using infrared thermal imaging systems capable of detection over a vast expanse of land. Equally important is the ability to track them any time of day and in varying weather conditions.

Some recent incidents include:

- In 2011, a Massachusetts man devised a plot to fly three explosive-packed drones into the Pentagon and U.S. Capitol.
- In March 2014, a Canadair regional jet nearly collided with a camouflage-painted drone (still unidentified) near Tallahassee, Florida.
- In April 2014, the FBI discovered a plot by a Moroccan national in Connecticut to fly bombs on drones into a school and federal building.
- In October 2014, more than a dozen UASs were spotted around nuclear plants in France.

These items present a threat to all critical infrastructure in the U.S. including stadiums, ports, airports, borders, nuclear power plants, and offshore oil platforms. Speaking on this point, Senator Dianne Feinstein declared, "We shouldn't wait for a major disaster to take action to protect the airspace."

Sources:

http://www.homelandsecurityssi.com/news/entry/ap-exclusive-drone-sightings-up-dramatically
http://www.kcentv.com/story/27441243/unauthorized-uavs-above-french-nuclear-plants-spark-critical-infrastructure-security-concerns
http://www.lansingstatejournal.com/story/news/local%0B/michigan/2014/11/22/state-police-hope-faa-permission-use-drones-soon/19422533/
http://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html?_r=2
WaterISAC November 2014 issue: Spread of Drone Technology May Pose Significant Risks for Critical Infrastructure

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

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

Dispatch Highlights

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

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

Contents

Anonymous Messaging App Yik Yak Gets Popular — and Controversial

http://mashable.com/2014/11/25/yik-yak-popular-and-controversial/

- A February study found 35% of all violent threats to schools from August 2013 to January 2014 came via texting or social media.
- 14 words, written on the anonymous sharing app Yik Yak, caused a Los Angeles high school to go into lockdown mode.
- The app is used as a forum for sexually explicit messages and has also been linked to bullying.

Analyst Note: Concerned parents, school administrators, and law enforcement officers often ask cyber analysts at FDLE about apps like Yik Yak. Anonymous messaging apps fill a niche market, one that will always be popular for both personal protection reasons and nefarious purposes. We offer this advice: know that technology allows for anonymous messaging apps, there is a perceived need, and we have to be alert to the changing mobile messaging landscape.

How to Delete Your Old, Embarrassing, Now-Much-Easier-To-Find Tweets

https://nakedsecurity.sophos.com/2014/11/20/how-to-delete-your-old-embarrassing-now-much-easier-to-find-tweets/

- November 18, 2014 Twitter announced that every single tweet ever sent —all hundreds of billions of them— are now indexed.
- Search.twitter.com allows you to search for specific tweets and delete them now.
- Be wary or third-party services that promise to delete time-specific tweets: they may not be trustworthy.

Analyst Note: This ties in to our article on Social Media (Page. 5). In addition to embarrassing tweets, you might want to also consider deleting tweets that give strangers too much personal information.

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

www.surveymonkey.com/s/TheSFBeacon5

The FIPC Ledger

Editor: Kevin Wiggins
Design: Chris Kenworthy

SecureFLORIDA.org

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

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