Summary

**Cracking Down on KRACK:** Are your secured Wi-Fi devices vulnerable? Find out what you can do to stay safe.

**Mobile Malware:** The Play Store was supposed to be the safest place to download apps, but malware is challenging this.

**Ransomware Not For Ransom:** Could recent iterations of ransomware have a more nefarious purpose than making money?

**Keep Your Tickets to Yourself:** A fun life event can become a headache when you share too much on social media.

**Deepfaked:** Technology is making video editing easier, but there are downsides. We take a look at possible uses and ramifications.

**Bluetooth Beware:** Whose job is it to delete our data after we’ve disconnected our devices? How to stay safe while connected.

**How Terrorists Are Using the Internet:** Terrorists are making bombs in their kitchen, but where are they learning how?

**Color Me Successful (Part 2):** Picking up from last issue, we continue discussing color and how to make it work for you.

Contents

Summary

Editor’s Corner ........... 2
Cyber Threats ............ 3
Cracking Down on KRACK
Mobile Malware
Cyber Highlights ........ 7
Ransomware Not For Ransom
Keep Your Tickets to Yourself
Deepfaked
Bluetooth Beware
Critical Infrastructure .... 13
How Terrorists Are Using the Internet
Design 101 ............... 14
Color Me Successful (Part 2)
Dispatch Highlights .... 16
What is TLP? ............. 18

About The Beacon

*The Beacon* is the Florida Fusion Center’s cyber and critical infrastructure publication, produced by the Florida Infrastructure Protection Center (FIPC). Designed to highlight information of interest, *The Beacon* features events and trends that occur in Florida or specifically affect Florida.

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

Contact the FIPC
Phone: (850) 410-7645
Email: FIPC@fdle.state.fl.us

This addresses the DHS Standing Information Need HSEC-SIN-1 and FDLE SIN-1
So far, 2018 is has been devoid of the headline grabbing cyberattacks that dominated 2017, but that doesn't mean that the year hasn’t been eventful. Here’s a look at 2018 so far, as well as some predictions for the rest of the year.

Ransomware has been a hot topic as of late, with growth topping 2,500% in 2017 alone.¹ Last year, outbreaks of WannaCry and NotPetya made news as they bypassed security measures to infect networks and cause lasting damage. The world entered a new phase in cybercrime with the rise of wiper malware, designed to destroy rather than generate revenue. (See the article Ransomware Not for Ransom for more analysis on this topic.) These menacing variants are still making the rounds, infecting systems that have yet to patch for them.² Ransomware is still a threat in 2018, but its rate of infection has slowed somewhat as attackers shift to using the software to deliver covert cryptominers.³ These programs can be hard to detect, allowing for the mining of currency using a victim’s computing power and resources.

Speaking of cryptominers, you may have seen news of different cryptocurrencies (such as Bitcoin and Litecoin) surging in popularity and value. Their ability to mask and anonymize transactions make them a viable revenue stream.⁴ Cryptocurrency value has fluctuated wildly in the first part of the year, but as prices stabilize and climb again, demand will only increase and fuel further attacks.⁵

Phishing has always been the reliable mainstay of bad actors attempting to access information. No matter how much technology advances, social engineering remains the most effective method of attack. It used to be easy to spot a phishing email, with its misspellings and grammatical mistakes, but today’s phishing emails are getting more sophisticated, better targeted, and using spellcheck. The volume of phishing emails keeps increasing year after year, with phishing attempts to software-as-a-service vendors exploding as such services become popular.⁶ It has become more important than ever to be vigilant of what makes it into our inboxes.

All eyes are currently forward-facing to the election in November, and cybersecurity is front and center. Though there were no confirmed breaches during the 2016 election that were shown to alter the outcomes of the election, there are concerns that bad actors could get more bold this time.⁷ Cyber hygiene and good security posture are encouraged to prevent incidents that would undermine the trust in the voting system.

The year is only half over, but already there is much to examine and even more to anticipate.

⁴ https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/2/#5aeb01d6144

2nd Quarter 2018
Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)
Cyber Threats

Cracking Down on KRACK

Why is it scary?

All technological devices that support Wi-Fi are at risk of the KRACK attack. It affects the Wi-Fi protocol—not specific products or implementations—and "works against the modern protected Wi-Fi networks." The KRACK attack hacker tricks the victim into reinstalling an already-in-use key. Every key should be unique and not re-usable, but a flaw in WPA2 means a hacker can tweak and replay the ‘handshakes’ carried out between Wi-Fi routers and devices connecting to them; during those handshakes, encryption keys made up of algorithmically-generated, one-time-use random numbers are created. It turns out that in WPA2, it's possible for an attacker to manipulate the handshakes so that the keys can be reused and messages can be silently intercepted.

If you think that using a VPN server is a quick fix to maintaining your privacy, you are wrong. "When you use a VPN service, you reroute all your internet traffic to a VPN server in a data center somewhere. An attacker can’t see what you’re doing on your Wi-Fi network, but a VPN company can log all your internet traffic and use it against you.” Certain companies do keep logs of user activity, which they can store on their servers. Again, be very careful trusting any VPN company. Unless you’re willing to rebuild your own VPN server, a VPN service is not a total solution.

What is it?

In October 2017, a new type of security flaw appeared in countless Wi-Fi networks. This security flaw is known as KRACK. KRACK stands for Key Reinstallation Attack and targets the third step in a four-way authentication ‘handshake’ performed when your Wi-Fi client device attempts to connect to a protected Wi-Fi network. The KRACK vulnerability is a flaw in Wi-Fi Protected Access (WPA) and WPA2 security protocols that makes it possible for attackers to eavesdrop on your data when you connect to Wi-Fi, or rather exposes your private web use.

What can the end user do to protect themselves?

There are simple things a person can do to protect themselves from a KRACK Attack. Recommended actions to protect yourself and your devices:

- Update all your routers and Wi-Fi devices (laptops, phones, tablets, etc.) with the latest security patches. Do not ignore your devices security updates.
- Make sure to turn on auto-updates for future vulnerabilities as this will not be the last one.
- Your router’s firmware needs regular updating. You can make sure your router is up-to-date by browsing the administration panel.
- For phone vulnerabilities, disable Wi-Fi on your device and use cellular data until you know your Wi-Fi is safe.5
- Actively check your devices for updates as well.

These suggestions and patches are simple to do and won’t take a lot of time. It does not take much to prevent this type of vulnerability except avoiding the software updates that are required by your devices.

For anyone who uses Android as their operating system, the Google Play Store is a familiar site. It contains every authorized app under the sun; from games to social media apps. By default, many Android devices are set to only allow downloads from the Google Play Store, which is an attempt to keep downloads secure by making it pass through Google's Play Protect gatekeeper. This setting can be changed, allowing users to download from third party sites, though this is generally not recommended.

It may come as a surprise to some, then, that 2017 was full of reports that some apps downloaded from the official app store were plagued with malware. Researchers uncovered several malicious apps that bypassed the Play Protect safeguards in subtle, multi-step processes and hid within innocuous-looking applications. Most insidiously, all of these processes seem to happen in the background, with very little interaction from the end-user. Many of the apps were found to be installing banking trojans, but could feasibly be equipped to download any type of malware.\(^1\) As of November of 2017, those apps had between 10,000 and 17,000 downloads, but a fake app impersonating popular encrypted messaging service WhatsApp had well over 1 million downloads before it was removed.\(^2\) Though the app seemed to only be used to deliver advertising to its users, the outcome could have been much worse.

And yet others seemed even more dangerous. In December 2017, the Loapi trojan was spotted on the Play Store and its effects could literally be explosive. Researchers studying the malware noted that it is used in cryptocurrency mining, and when they left a cell phone running the

---


program for two days, it heated the battery to such an extent that it warped and deformed the cover noticeably.³

How does malware make it onto Google's trusted app service? Many of the apps that act as carriers for the malware purport to be programs that clean up your files and speed up your phone. Once downloaded, the requested app permissions don’t ask for anything out of the ordinary and the app will eventually request an update. This update, though, comes from a third party server. This isn't unusual even for legitimate apps and allows developers greater control over their product. Unfortunately, it also circumvents the Play Protect check for malware and allows the program to be installed without the user noticing.

With most internet activity occurring over mobile devices these days, safety protocols for a secured site for app downloads are very important. Android devices made up 81.7% of the market share of new devices in the fourth quarter of 2016,⁴ meaning that potentially millions of users could be affected. Though Google has taken steps to try to root out malicious apps, malware developers have found ways around them.

As with all software downloads, keep good security hygiene in mind: only download from trusted developers and read any permissions that the app requests carefully. App stores also make reviews of apps available to the public, and reading these testimonials can reveal other users’ experiences. It is best to stay vigilant, as it does not seem that malware for mobile devices is going anywhere any time soon.

³ https://arstechnica.com/information-technology/2017/12/currency-mining-android-malware-is-so-aggressive-it-can-physically-harm-phones/
In June of 2017, the ransomware ‘Petya’ (or variant notPetya) wormed its way across the world, wreaking havoc in transport, energy, and banking software. The bug demanded a low ransom, only $300 in bitcoin, but appears to have been written with a wiper component that did not allow for files to be recovered.

Ransomware is a form of malicious software designed to lock down infected devices until a specified “ransom” has been paid to the creator. So far this year there have been several high profile cases of ransomware, including WannaCry and Jaff, but there was a new trend making its rounds in 2017 involving a new strain called Petya. Petya is not a traditional ransomware program that restores your device’s data once the ransom has been paid. With other variants of ransomware, files on the infected device are encrypted one by one leaving data unusable until the victim pays for a unique key to unlock their files. Petya, on the other hand, reboots targeted devices and encrypts the master file table (MFT) and renders the master boot record inoperable. One theory that has gained traction in the cyber community that explains Petya’s differences from other ransomware attacks is that it was not designed to be a ransomware scheme at all, but rather it was created as a destructive device disguised as ransomware.

Experts believe Petya is not traditional ransomware because data retrieval is very unlikely. As of this writing, there have been more than 40 cases of individuals paying a total of $10,500 in Bitcoins to recover their device and so far none of them have been restored. What is unusual about the way Petya collects the ransom from victims is that every device receives the same Bitcoin address while others usually create a different address for every device. Victims were encouraged to communicate with extortionists by a provided email address in the ransom note, but the email address was deactivated by its provider, further complicating file recovery. Generally, for sake of anonymity, attackers urge victims who wish to pay or

This instance of ransomware being used as a destructive tool rather than a financial opportunity could prove troubling in the future. Petya, and other recent ransomware variants, have been making use of the tools reportedly pilfered from the NSA, such as EternalBlue, that make them particularly effective at infiltrating networks. With the possibility of data loss being permanent, it is important to keep general ransomware recovery tips in mind. An increase in this type of cyberattack could potentially be disastrous for many industries.

- Regularly back up your files and test those files for recovery success.
- Keep your antivirus and operating system software updated.
- Beware of suspicious emails and do not click any attachments or links in them.
- Do not pay the ransom! You are not guaranteed to get the decryption key or they can demand more money.


Keep Your Tickets to Yourself

Imagine this: You’re waiting in line for the concert. You bought your tickets months ago and the show is sold out. You took the day off from work, meticulously picked out your outfit, and even painted your face. You’re set for a night of fun and relaxation, and all that’s left is to post a picture on social media to let your friends and family know how excited you are. What better way to share than to post a picture of your tickets, which includes the band, the venue, the date and time, your seats, and proves that you actually have access to the show? You made a post earlier that day about this exciting piece of your life with hundreds, or even thousands, of people. Finally, the ushers start allowing people into the venue while scanning tickets at the door. The moment arrives and you pull out your ticket, but after its scanned the usher
informs you that you’ve already been checked in and the ticket you’re holding is not valid.

As tempting as it can be to post tickets or event identification cards on social media, it’s wise to keep in mind that they can contain sensitive information that can easily be stolen. All a bad actor needs to swipe away your fun is a good picture of a barcode and a little bit of personal information.¹ Any thief could take your barcode and easily print it on a new ticket for themselves, or they could print it on many tickets to sell to unsuspecting buyers.

While an eventful evening being ruined is bad enough, unscrupulous characters could take more than that from you. A popular pastime of travelers everywhere is to post pictures of their airplane boarding passes before they disembark. An observant identity thief could lift the six-digit booking code, also known as the Passenger Name Record (PNR). The PNR, along with a passenger’s last name, can be used to access the online check-in portal to get free flights or access to other sensitive information. Due to codesharing agreements between many carriers, it’s possible to use this information to log into the websites of multiple airline companies.²

So what can you do? The easiest and most obvious answer is to not post event and travel tickets online for others to see. If you find yourself in a situation where you must share a life event, try to obscure any personal information on the ticket (name, personally identifying numbers, etc.) and obscure, blur, or crop out the entire barcode. Even if your social media profile is secure and your audience is limited to just your close friends and family, there is the chance that someone might be tempted by the information you are freely giving out.

Take our advice: Post a text update about your activity or a picture of the event that doesn’t include your tickets and personal information. Don’t ruin a fun evening by giving your ticket away!

“Deepfakes” is a term used to describe an application that can use an image of a subject's face and place it on someone else's body to create a convincingly modified video. This application can also use audio clips to create a seemingly authentic video. It was supposed to be a fun tool but it has turned into something darker.\textsuperscript{1,2} It is an easy application that anyone can use, including bad actors.\textsuperscript{3} The method has commonly been used to create “revenge porn,” or pornographic videos of actors and actresses, usually without their consent or permission. Cyber-stalkers could use this program to create an altered pornographic video to blackmail and torment victims. There are other possibilities for the use of Deepfakes and the ramifications could go further.

While the damages to reputation from a maliciously created false video seem bad enough, Deepfakes can be used in ways that can be equally devastating to society as a whole.\textsuperscript{4} Imagine a faked video that causes political unrest or protests and riots, or a video or audio clip that calls into question the integrity of a government official.\textsuperscript{5} The ramifications for the release of such a video can be far-reaching, with reputation being the least of concerns. In an age where written false news stories are already hard to combat, video footage is a troubling addition to an already pervasive problem. Once a video or

audio clip is shown, it may be hard to convince people that it is not genuine. Even if the video or audio clip is proven false, the damage to someone's life or career can be hard to repair. Unless there is an investigation with an audio/video expert, it is hard to prove that the subject did not do the behavior shown.

Fighting back against the perpetrator may not be an easy task. There are laws regarding libel and slander on the books, but currently no law dealing directly with Deepfakes, and it might be expensive and possibly hard to win. The perpetrator may be located overseas or they may be difficult to locate. Exposing the audio or video clip as fake makes it hard to prosecute because the perpetrator is not technically divulging private details of the victim's life. This video may also receive some protections due to First Amendment considerations. The site hosting the video is not liable for the content uploaded to its servers, nor do they have to remove content unless the request is made by the original copyright holder. Major sites such as PornHub and Twitter are banning Deepfake videos as a precaution and as a sign that they side with protecting victims.6


Bluetooth Beware

Staying connected has never been easier. Our personal vehicles have hands-free Bluetooth and navigation systems that allow for a safer commute. Rental cars are now getting into this technology by allowing drivers to connect or ‘pair’ their smartphones to the rental car’s Bluetooth for a safer traveling experience. When pairing your smartphone to your car, you are able to accept and make calls over the audio system, respond to text messages, stream music, and receive directions through navigation. Connecting your device to the car’s Bluetooth also stores personal information like address books, call logs, text messages, and previous route destinations. Just one problem: All that information is saved inside the system and just sitting around for the next renter to find.1

It is important to remember that modern cars are computers on wheels and computers can be hacked. A 2015 report released by the Senate’s Commerce, Science and Transportation Committee showed as proof-of-concept that almost every new car was hackable—meaning hackers not only had the potential to take control of some vehicles, but also could hack into the navigation system to steal valuable information about their owners.2

Connecting your smartphone to a rental car can leave your smartphone vulnerable to viruses. If the car’s system was compromised by a hacker or previous renter, hooking up your phone would give a hacker access to everything on it.3 Forgetting to disconnect or ‘unpair’ your smartphone from the car’s infotainment system can lead to possible identity

1 https://www.usatoday.com/story/tech/columnist/komando/2015/07/03/komando-car-rental-mistakes/29614165/
2 https://www.consumeraffairs.com/news/rental-car-drivers-take-these-important-steps-to-protect-your-privacy-071315.html
3 https://www.komando.com/tips/310741/one-huge-mistake-people-make-when-renting-cars/all
theft and data thefts if the information gets in the wrong hands. The Federal Trade Commission warns consumers to beware of new ‘connected car’ features that allow rental car customers to connect their mobile phone to other devices to in-vehicle infotainment systems. The FTC advised customers to delete data before returning the car; otherwise people can view it including future renters, rental car employees, and even hackers. If you decide to rent a car that gives you hands-free access to your technology, here are some steps you can take to protect your personal information:

- Avoid connecting your mobile phones or devices to the infotainment system just for charging. It’s safer to use a cigarette lighter adapter to charge devices, instead of the car’s USB port. Why? In some cases, the USB connection may transfer data automatically.

- Check your permissions. If you do connect your device to the car, the infotainment system may present a screen that lets you specify which types of information you want the system to access. Grant access only to the information you think is necessary—if you just want to play music, for example, you don’t need to okay access to your contacts.

- Delete your data from the infotainment system before returning the car. Go into the infotainment system’s settings menu to find a list of devices that have been paired with the system. Locate your device and follow the prompts to delete it. The owner’s manual and the rental car company may have more information about how to delete your data.

- Delete your trip information. If you used the car’s built-in GPS or navigation system rather than your own, you may want to wipe the stored information clean before returning the car.

Privacy concerns with car infotainment systems should be going away in the future as Android Auto, Apple CarPlay, and similar systems become standard on more cars. These systems do not store any information and when you take your smartphone out of the car, your information goes with you. Until then, take time to clear your data and personal information in a rental car to protect your privacy.
Critical Infrastructure

How Terrorists Are Using the Internet

From the perspective of foreign or domestic terrorism, critical infrastructure includes hardened and secured targets like power plants and soft targets like schools or religious centers. Although plans to attack these differing types of facilities vary, they are all potential targets of those that would utilize explosive or incendiary devices. To successfully employ such devices, knowledge and skill about how to construct and trigger them is necessary.

One way to obtain the required knowledge is on the internet. Foreign terrorist organizations publish magazines on the internet that contain instructions to build and deploy explosive and incendiary devices. The Rumiyah magazine, produced by the Islamic State in the Levant and Iraq, and the Inspire magazine, produced by al-Qa’ida, are examples of publications readily available over the internet. In particular, the article in the Inspire magazine, *How to Build a Bomb in the Kitchen of Your Mom*, has been found to be part of the planning used by some homegrown violent extremists.

The two brothers that attacked the Boston Marathon on April 15, 2013, utilized pressure cooker devices, the type described by al-Qa’ida on the internet. During the FBI investigation into the bombing, the FBI located numerous articles, including *How to Make a Bomb in the Kitchen of Your Mom* from Inspire, which describes the pressure cooker bomb. On September 17, 2016, “Chelsea Bomber” Ahmad Khan Rahimi carried out terrorist attacks in New York City and New Jersey, utilizing pressure cooker bombs as well as other devices. One device placed under a dumpster exploded and another did not, but the aftermath left 31 people injured. The devices were determined by the Department of Homeland Security to be similar to those described in Inspire.

In addition to the magazines and the manuals, the internet is utilized by foreign and domestic terrorist organizations to directly exchange information in secure and open applications. Finding and infiltrating these information-sharing rings can take considerable time and effort. Although there is no new credible threat information that an explosive device will be employed against critical infrastructure, it remains a possibility that should be considered. Continued vigilance related to suspicious activity by persons and suspicious packages both delivered and abandoned should remain an important part of security routines.

Analyst Note

While this information is readily available online, it is not recommended to search for or view this content. If you have stumbled onto suspicious content or activity online, contact your local law enforcement or call the “If You See Something, Say Something®” line at 1-855-FLASAFE.

Design 101

Color Me Successful: Understanding Color (Part 2)

In Color Me Successful: Understanding Color (Part 1), we talked about the RGB and CMYK color models and how they work. We established that the RGB model deals with light, which means it's at work on your computer screens, and that the CMYK model deals with pigments, like the ones in your hard-copy printouts. In this issue, we're going to take it a few steps further and look at how you interact with these models more closely, how color models create color spaces, and how these spaces work with each other and with you.

To start off, let's expand a bit on what we learned last issue. We now know that the RGB model works with colored light. The source of colored light you're all familiar with is your computer screen. A computer monitor is built of thousands of tiny squares called pixels, as you can see in the picture to the left, and each pixel is made of sets of red, green, and blue light. The varying intensity of R, G, and B results in the eye seeing different colors. As an example, when the red, green, and blue lights in a pixel are all at maximum intensity, we see a white pixel. That makes sense because we now know about the additive nature of light; red light + green light + blue light = white light.

On the flip side, the CMYK model is at work in your prints. A printer works by distributing thousands of tiny dots at varying levels of saturation in cyan, magenta, yellow, and black. By altering the size, spacing, and saturation of the dots, the eye is tricked into seeing a variety of colors. Like in the picture to the right, a close-up of a magazine print reveals the CMYK dots. The combination of varying sizes, degree of saturation, and printing angle of just cyan, magenta, yellow, and black creates a surprisingly wide spectrum of colors in print. That spectrum, however, is much smaller in comparison to the that of the RGB model spectrum, which we'll discuss next.

https://www.pinterest.com/pin/575264552374953026
We know a color model is a way of describing colors by their interactions with each other. Now we need to talk about color spaces, independant ranges of colors that follow a certain model. As an example, RGB is a color model. sRGB (“s” for “Standard”) and Adobe RGB are examples of color spaces that follow the RGB model. These spaces specify a gamut, a range, of colors that exist within the space. Devices also have gamuts; a computer monitor has a much wider gamut than a printer. This is because, as you now know, computer monitors work with lights. Lights are used in the RGB model and, by extension, RGB color spaces. Printers work with pigments in the CMYK model, so they also work in a CMYK color space. Colored lights are capable of making more colors than colored pigments, so RGB color spaces have wider gamuts than CMYK color spaces.

The image to the right visualizes this concept. The yellow triangle encloses the color gamut of an RGB color space. The black line encircles the gamut of a CMYK color space. As you can see, there are quite a few colors that exist outside the CYMK color space that are within the RGB color space. This is the main reason colors don't always print the way they look on screen: your printer's working in a different color space than your monitor. It's almost like they're speaking different languages; your printer speaks Spanish, but your monitor speaks English. When the printer receives instructions to print a color outside its color space, it does its best to find an approximate replacement, but it's not going to be exactly what you see on your monitor. Your Spanish printer will try to speak English, but you'll be able to tell it isn't its native language.

So let's review what's been discussed and how you can use that information to your advantage. The colors on your screen exist in an RGB color space (because they're made of lights) and the colors on your prints are in a CMYK color space (because they're made of pigments). There are some colors that you'll be able to see on your monitor that you can't reproduce in print because sometimes ink just can't make the kinds of colors light can. This is why some colors look wrong when they print; your printer is giving you the closest match it can make. To work around this, if you know you're making something that you'll be printing, some programs can work in CMYK color spaces or will accept CMYK values for colors. This can give you a better idea on-screen of what your colors will look like when they print. Additionally, different printers have different gamuts, so one printer's product could look vastly different to another's. If you don't like what one printer gives you and you have access to another, try using a different printer.

If you know what you're working on will only ever be viewed on-screen, you don't have to even consider working in CMYK. You may have to consider the gamut limitations of different monitors (Retina display vs. standard display, for instance). At the very least, this color discussion should explain the discrepancies between screen and print. Hopefully, it's also given you some new things to think about while you're working.
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 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.

Bad romance: catphishing explained


- Catphishing is the phenomenon of having a relationship with someone who turns out to be someone else (known as “catfishing” is modern lingo) with the added pain of this imposter sending a phishing email to gain access to information.
- Catfishing (with an f) is only illegal in Oklahoma, but there are other avenues for legal recourse, including charges of copyright violation, criminal impersonation, defamation, identity fraud, and espionage.

Analyst Note: What could hurt more than finding out your crush isn’t who they say they are? Having them infiltrate your network, of course. Sometimes it’s good to treat emails from friends with a healthy dose of suspicion, too.

Millennials Twice More likely to Fall for Phishing Scams Compared to the Elderly


- One in ten subjects aged 18-24 admitted to falling victim to phishing, compared to one in twenty aged 55 or older.
- Younger people appear to pay less attention when opening their email, and admit to clicking on links or responding to suspicious emails more often.

Analyst Note: Always be suspicious of suspect email and don’t click on any links or attachments. Take the time to examine things carefully and look for obvious social engineering. Pay attention to who is sending you mail and why.
Ransomware is now big business on the dark web and malware developers are cashing in

http://www.zdnet.com/article/ransomware-is-now-big-business-on-the-dark-web-and-malware-developers-are-cashing-in/

- The total value of ransomware sales on dark web marketplaces has gone from $250,000 to over $6m in just a year.
- Prices range from just a few dollars to thousands of dollars.

Analyst Note: This represents a troubling turn in acquisition of ransomware, as threat actors can now have their malware tailor-made for a specific target. Over-saturation of the market with product may lead to its collapse, though.

YouTube to crack down on inappropriate videos targeting kids


- YouTube has a separate site dedicated to programs for children. Unknown actors have been uploading videos with cartoon characters that are also spliced with disturbing images. The actors appear to also be making money off ads placed in the videos.
- YouTube is taking steps to try to flag and remove the videos, but this still requires someone seeing the video.

Analyst Note: It’s always good to supervise children on the internet, which can be full of content that is not suitable for them. Even in these spaces designed for children, some scary things can make their way in.

74% of All Bitcoin-Related Sites Suffered a DDoS Attack


- Nearly three out of four Bitcoin exchanges suffered a DDoS attack in the third quarter of 2017.
- Imperva recorded 144 attacks in the third quarter, up from 6 in the first quarter of 2017.

Analyst Note: Bitcoin appears to be a victim of its own success, being worth over approximately $6,500 as of April 6, 2018. As long as cryptocurrency continues its rise it will be a big target; something to keep in mind if investing.
What is TLP?

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

This Beacon is **TLP: White** and is intended for wide distribution. If you would like to read past issues of the The Beacon, visit the Secure Florida website.

www.SecureFlorida.org/The_Beacon

The following is from the United States Computer Emergency Readiness Team (US-CERT):

- **RED** Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

- **AMBER** Recipients may only share TLP: AMBER information of their own organization who need to know, and only as widely as necessary to act on that information.

- **GREEN** Recipients may share TLP: GREEN information with peers, partner organizations, and with their sector or community, but not via publicly accessible channels.

- **WHITE** TLP: WHITE information may be distributed without restriction, subject to copyright controls.
The Florida Infrastructure 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 Florida Infrastructure 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 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 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  » Identity Theft
» Family Online Safety  » Mobile Communications
» Combating Cyberbullying  » Email Safety
» Online Safety for Seniors  » Internet Laws & Regulations