The Beacon

Florida Fusion Center #17-145 | Cyber and Critical Infrastructure Report | October 2017 Issue #15

Summary

AlphaBay Taken Down - The largest Dark Web Market in history was taken down. We give you the details.

North Korea's Dynamic Cyber Force - North Korea is not only trying to exert power physically, it is working to expand its cyber capabilities as well.

Facebook AI: What Really Happened? - Is Facebook spearheading the robot revolution? We look at the facts.

Comparing Cryptocurrencies - You've heard about Bitcoin; now we compare some of the other prominent types.

Cybersecurity Hygiene - Just like the dentist and flossing, it's always important to get a reminder of the best practices for good cybersecurity.

Hiding In Plain Sight - Steganography has been around for millennia, but we discuss how it plays a role in tech and cybersecurity today.

So Your Identity's Been Stolen - What to do if you are a victim of the Equifax breach.

Understanding Color - Part 1 of a 2 part discussion on color and how to work with it.

Contents

About *The Secure Florida Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness. Secure Florida is an internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC).

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

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

Editor's Corner

Cyber Security Awareness Month 2017

This month marks the 14th year that October has been designated National Cyber Security Awareness month. Each week focuses on a different cybersecurity issue, and so this issue contains articles with those themes in mind.

WEEK 1

STOP. THINK. CONNECT.™: Simple Steps to Online Safety

Good cybersecurity comes from three simple steps: STOP to make sure you have the appropriate security measures in place; THINK about what consequences come from your online activities (including something as simple as clicking on a link); CONNECT to the cyber space. Sometimes taking a few seconds to consider what you do online is all it takes to ensure your security.

WEEK 2

Cybersecurity in the Workplace is Everyone's Business

Just like cleaning the shared break room, keeping the workplace network secure is every employee's responsibility. Make sure that you take appropriate steps to secure the data in your workplace, and avoid introducing malware or other risks to the environment.

WEEK 3

Today's Predictions for Tomorrow's Internet

Increased interconnectivity in all aspects of our lives is happening more rapidly than ever. As we get closer to things like self-driving cars or smart healthcare devices, it's important to understand not only what's on the horizon, but how to appropriately secure them to maximize safety.

WEEK 4

The Internet Wants You: Consider a Career in Cybersecurity

Cyber is the new frontier, and companies of all sizes and types will be in need of savvy cybersecurity professionals. The Internet of Things has created a great demand for employees to understand and implement a strong cybersecurity posture across all sectors.

WEEK 5

Protecting Critical Infrastructure From Cyber Threats

Everything from traffic lights to water plants use the internet in some way. It's important for those in cybersecurity roles to understand the risks associated with critical infrastructure's integration of web-based functionalities, as well as how to mitigate against possible threats.

For additional resources, or to learn more about National Cyber Security Awareness Month, please visit https://staysafeonline.org/ncsam/.

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

Cyber Threats

Lights Out: AlphaBay Goes Down

Online shopping has changed the way many people around the world buy and sell goods and services. The black market is no exception. Ever since the site "Silk Road" was founded in 2011, the Dark Web has been host to numerous online black markets attempting to capitalize on Silk Road's revolutionary approach to buying and selling illicit goods.[1]

Recently however, authorities around the world struck a huge blow against this growing trend of buying and selling illegal goods and services online by shutting down two of the largest Dark Web Markets (DWM) in the world, AlphaBay and Hansa. AlphaBay, formerly the world's largest DWM, was only active for two years but managed to take the industry by storm; it had, on average, $600,000-$800,000 in revenue each day and there were over 300,000 active listings when it was shut down by the FBI on July 4, 2017.[2] At the time the site went down, it was unclear what the cause was, and many users thought it was an "exit scheme," where the administrators of the site shut it down and absconded with users' money.

When AlphaBay initially went down, it sent a huge wave of DWM "refugees" scuffling to similar sites such as Hansa. Shortly after AlphaBay went down, Hansa had an 800% increase in new accounts.[3] What the users did not know was that Hansa had been under the control of Dutch law enforcement since June 20th, and that thousands of Hansa usernames and passwords were recorded by Dutch officials for follow up investigations.[4]

The Dark Web will most likely see the return of other DWM in the near future, but it appears that law enforcement around the world have taken a proactive response to these new trends, and is eager to collaborate across the globe to locate and dismantle these sites.

[1] https://qz.com/481037/dark-web/
[2] https://www.wired.com/story/alphabay-takedown-dark-web-chaos/
[3] https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/
[4] http://thehackernews.com/2017/07/alphabay-hansa-darkweb-markets-seized.html

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

North Korea's Dynamic Cyber Force

A number of globally disruptive attacks have had a significant impact on the cybersecurity community throughout 2017. On May 12, 2017, at least 150 countries suffered the effects of a ransomware strain known as WannaCry. Reportedly, 300,000 users lost access to their computer systems and were forced to contemplate paying a ransom in order to recover their data.[1] It wasn't until several months later that the United States National Security Agency attributed WannaCry to cyber actors associated with North Korea (officially the Democratic People's Republic of Korea). The motivations of this small country have continued to perplex security experts over the last decade. Retaliation, coercion, espionage, and financial gain have all been identified by analysts of North Korean affairs to explain the nation's aggressive cyber posture.[2]

Despite having one of the smallest internet footprints in the world, North Korea has devoted significant resources to develop its capability to disrupt the cyber operations of other nations. A number of analysts consider the North Korean cyber threat to be exceeded only by those posed by China, Russia, and Iran, all countries with sophisticated offensive cyber programs. The size of North Korea's cyber force is estimated to be between 3,000 and 6,000 hackers.[3] Some research suggests that some students train internationally in Russia and China.[4] Defectors from North Korea have reported that hackers typically do their work abroad, taking legitimate software programming or other jobs in China, southeast Asia or Europe while waiting for instructions from the capital, Pyongyang, to mount a state-sponsored attack.[5]

There are ongoing debates about whether North Korean cyber capabilities are sophisticated enough to impact critical infrastructure in more technologically advanced nations. Some of the attacks attributed to North Korean actors over the past several years are considered unsophisticated (such as website defacements), requiring only limited access to foreign networks.
In May 2015 a North Korean defector, Professor Kim Heung-Kwang, who taught computer science at North Korea's Hamheung Computer Technology University, told BBC News that he estimated "between 10% to 20% of the regime's military budget is being spent on online operations [and] harassing other countries to demonstrate that North Korea has cyber war capability."[6] However, a number of cybersecurity firms have observed a major shift in the primary motivation of North Korean cyber operations over the past year. According to South Korea's Financial Security Institute, the focus seems to have shifted to raising foreign currency.[7] North

[1] Initial reports placed the number of affected computers at 200,000. See Goldman, Russell. "What We Know and Don't Know About the International Cyberattack," New York Times, May 12, 2017.
[2] https://fas.org/sgp/crs/row/R44912.pdf
[3] Ken Gause, "North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime," Center for Naval Analyses, August 2015.
[4] Donghui Park, "North Korea Cyber /Attacks: A New Asymmetrical Military Strategy," Henry M. Jackson School for International Studies post, June 28, 2016.
[5] North Korea Tries to Make Hacking a Profit Center. Sang-Hun, Choe. New York Times. October 27, 2017.
[6] Dave Lee and Nick Kwek, "North Korean Hackers 'Could Kill,' Warns Key Defector," BBC News, May 29, 2015, pp. http://www.bbc.com/news/technology-32925495.
[7] North Korea hacking increasingly focused on making money more than espionage: South Korea study. Kim, Christine. Reuters. July 27, 2017. https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO.

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

Korea is an isolated, impoverished nation that historically has had difficulty paying for the foreign import of goods. The country's renowned nuclear stockpile and unusually large military are expensive endeavors that have significantly reduced the nation's wealth. Analysts with the cyber intelligence firm FireEye have observed North Korean actors turning to cryptocurrencies as a method of payment, possibly to evade sanctions controls imposed by the international community on North Korea.[8] This motivation supports the alleged North Korean ties to the WannaCry campaigns and why the government there has likely begun to support the collection of bitcoin ransoms as a means to further economic growth.

General Brooks, recently inaugurated as the United States Forces Korea commander, said that North Korea has one of the world's most well-organized and able cyber forces, if not the world's best.[9] South Korea has suffered through the bulk of these attacks the past several years, but the international community is now being targeted as well. Given North Korea's shifted cyber priorities from politically motivated to financial, representatives of the private sector should maintain awareness, since the threat picture does not solely concern government/national security organizations any longer.

[8] FireEye Report Confirms North Korean Hackers Continue to Target Bitcoin Exchanges. Buntix, JP. The Merkle. September 12, 2017. https://themerkle.com/fireeye-report-confirms-north-korean-hackers-continue-to-target-bitcoin-exchanges/

[9] The Kim Jong Un Regime and the Future Security Environment Surrounding the Korean Peninsula. – Chapter 2. Boo, Hyeong-wook.2016. http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf

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

Cyber Highlights

Facebook AI: What Really Happened?

Since June, many articles have circulated about Facebook's Artificial Intelligence (AI). Facebook published a research paper stating that their chatbots diverted from understandable human language, and created their own language only understood by the bots.[1] Articles spread panic about possible technology being smarter than humans, comparing Facebook's chatbots to *Terminator* or *I, Robot*. People predicted that this could be an onset of what is called the technological singularity. This is the hypothetical moment in time when technology (primarily artificial intelligence) will have become so advanced that humanity undergoes a dramatic and irreversible change,[2] in worst cases actually causing dystopian futures like in *Terminator*. But what really happened? Is there really cause for panic and did Facebook really have to shut it down? Let's take a look at the facts and the likely implications of the situation.

Things misconstrued by the media:

- Facebook AI's invented language wasn't functional; rather, it deviated from the human script[3]
- Facebook did not shut it down because the AI was out of control[4]
- It was not live technology; in other words, this was never anything the public had access to or technology that was readily available to anyone but the researchers

The facts:

- Facebook's Artificial Intelligence Researchers were conducting research in a controlled setting
- The AI program was not shut down, but rather the algorithm was changed purposefully
- The unreadable language the AI bots used had no malicious properties or intent

So, what actually happened?

Facebook's AI team used chatbots to test a theory about artificial intelligence and negotiation. They wanted to introduce their chatbots to human language and see if the bots could pick it up and learn to negotiate. This definitely worked, and the bots were learning and evolving. This

[1] https://futurism.com/a-facebook-ai-unexpectedly-created-its-own-unique-language/
[2] https://en.oxforddictionaries.com/definition/singularity
[3] https://www.forbes.com/sites/tonybradley/2017/07/31/facebook-ai-creates-its-own-language-in-creepy-preview-of-our-potential-future/#2dae152292c0
[4] https://www.forbes.com/sites/quora/2017/08/16/why-facebook-shut-down-its-artificial-intelligence-program-that-went-rogue/#e04cc817105c

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

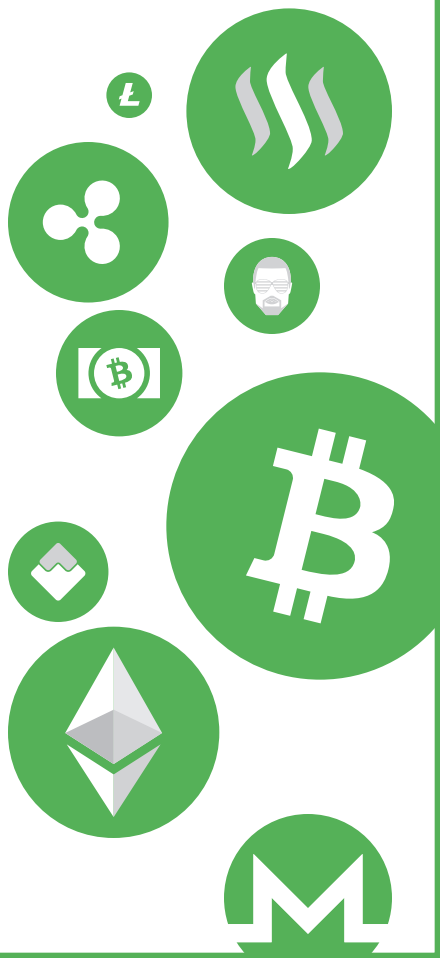
sounds scary – and it could be, if it turned into a scenario like in *Battlestar Galactica* – but it was the whole point of the research. The chatbots learned to pretend and practice deceit in order to later effectively come to a compromise.[5] What their research showed is that human language can certainly be learned by artificial intelligence, but cannot readily reproduce nuance like in human conversation. The researchers' conclusion was that human language does not come "naturally" in regards to artificial intelligence.[6]

While the implications certainly still seem daunting, it is important to know what really happened in the case of Facebook. It is a hard pill to swallow that artificial intelligence that we create can think and learn (and maybe outsmart us). The advanced language characteristics of humans are what set us apart from other species, but they aren't just ours anymore.[7] The silver lining is that researchers still have a way to go before robots can realistically employ sarcasm or humor.

[5] https://www.cnbc.com/2017/08/01/facebook-ai-experiment-did-not-end-because-bots-invented-own-language.html
[6] https://research.fb.com/wp-content/uploads/2017/08/lang-emergence-emnlp17.pdf
[7] https://futurism.com/a-facebook-ai-unexpectedly-created-its-own-unique-language/

Comparing Cryptocurrencies

Most people have at least heard the term "Bitcoin", but have you heard of Ripple, Ethereum, or Bitcoin Cash? These are all cryptocurrencies, specifically the biggest.[1] Cryptocurrency is a digital currency that operates independent of a central bank, using encryption to regulate and verify transactions.[2] But what exactly is cryptocurrency used for? It can be used by a consumer or by a business, for both legitimate and illegitimate means. Cryptocurrencies have attracted millions of users because it is fast, secure, and cheaper transactions allow the owner complete control over their funds.



Cryptocurrency technology has incorporated numerous authentication measures and security features to protect users. According to proponents of cryptocurrencies, the top seven benefits include: fewer instances of fraud, immediate settlement (meaning you can make large purchases without needing a third party such as a notary), lower transaction fees, lower chances of identity theft, decentralized authority, accessible to everyone, and can be used anywhere in the world.[3] While there are hundreds of different cryptocurrencies, let's take a closer look at the big four.

[1] https://www.nytimes.com/2017/08/03/style/what-is-cryptocurrency.html
[2] https://en.wikipedia.org/wiki/Cryptocurrency
[3] http://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html

Bitcoin

- Choose your own fees (lower fee means slower transaction)
- Most widely used cryptocurrency globally
- Multi-signature option for businesses for extra security
- Open-source, public network[4]
- First cryptocurrency, released in 2009
- Worth roughly $3,762*

Ripple

- Blockchain platform
- Connects banks, payment providers and digital asset exchanges
- Faster and easier international payments
- Track payments and attach invoices
- Processing for Ripple customers rather than personal wallets (Bitcoin)[5]
- Worth roughly $0.17*

Ethereum

- Runs on contracts
- Blockchain platform
- Can create markets and registries
- Personal wallet
- Can develop apps[6]
- Worth roughly $256*

Bitcoin Cash

- Split off Bitcoin, launched August 1, 2017
- Unrestricted growth
- Increased block size
- New way to sign transactions called SigHash
- Reliability surpassed Bitcoin (Bitcoin is restricted to about 3 transactions per second)[7]
- Worth about $443*

* Monetary value as of September 25, 2017

Amongst other cryptocurrencies are Litecoin (which has four times as many coins as Bitcoin), Monero (allows 100% untraceable payments), and Steem (a social media platform – share and comment to earn cryptocurrency). There are even niche currencies like WhopperCoin (Burger King currency in Russia) and Coinye (a now defunct variant that used Kayne West as its mascot)!

[4] https://bitcoin.org/en/
[5] https://ripple.com/company/
[6] https://www.ethereum.org/
[7] https://www.bitcoincash.org/

Good Cyber Security Hygiene

October is National Cyber Security Awareness Month and it's a great time to make sure you're practicing good security hygiene. The news is littered with reports of mass phishing attacks, global ransomware epidemics, and numerous hacks of large companies that hold personally identifiable information. It can seem like keeping yourself safe in an ever-changing cyber landscape may be a lost cause, but remembering to follow a few simple steps can go a long way to help mitigate these risks.

It's important to note that you may never be fully protected from every breach and the security of where your information is stored might be out of your hands. Recent high-profile hacks, such as the breach at Equifax that may affect one out of every three Americans,[1] have once again put security back in the national spotlight. While you can't control everything, remembering to follow a few simple steps can help keep you safe.

[1] Goodin, D. (2017, September 7). Equifax website hack exposes data for ~143 million US customers. Retrieved from Ars Technica: https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/

Passwords

Recently, the National Institute for Standards and Technology (NIST) convened to reassess the rules for digital authentication.[2] NIST sets the guidelines for the length and complexity of your passwords, and their work often influences password requirements for websites and databases at work and at home. NIST has concluded that the current framework for password construction isn't efficient at keeping users safe and often burdens users with cumbersome security requirements. They have proposed changing the rules so that more varied characters (including emojis) can be used, as well as removing the upper limit on password length.

Perhaps most drastically, NIST advised doing away with password expiration dates, meaning that your password will never change unless you decide to reset it (such as when you've forgotten what it is). We at Secure Florida agree: it is much safer to have a longer, more complex password that never changes as opposed to a shorter password that is reset every few months.

Best Practice #1: Remember to make your password at least 15 characters long and include capitalized and lower-case letters, numbers, and special characters.

Updating Software

It is important to keep up-to-date antivirus software on your computers, cell phones, and tablets to ward off potential threats. There are a number of both paid and free solutions to help keep you safe, and many are available via internet download. As with investment (time, money, effort) in any product, it's important to spend some time reading reviews to find the product that works best for you. No matter what antivirus you settle on, always keep the program updated with the latest virus definitions. Often, companies will release patches for malware currently impacting end users and ensuring you keep your software updated can keep you from becoming a victim.

Besides antivirus software, keeping your operating system software updated is also important. Malware often takes advantage of vulnerabilities in operating system software to bypass security controls and infect your computer. Updating your operating system software and the drivers for other hardware components not only keeps your computer running smoothly, it will prevent attacks from malicious entities.

Best Practice #2: Always make sure to keep software on all your devices up-to-date.

Social Engineering

Social engineering in all its forms is always a threat, even as the first quarter of 2017 saw a slight decline in phishing attacks.[3] It's always good to remember to be suspicious of everything.

[2] Wisniewski, C. (201, August 18). NIST's new password rules - what you need to know. Retrieved from Naked Security: https://nakedsecurity.sophos.com/2016/08/18/nists-new-password-rules-what-you-need-to-know/

[3] Darya Gudkova, M. V. (2017, May 2). Spam and phishing in Q1 2017. Retrieved from SecureList: https://securelist.com/spam-and-phishing-in-q1-2017/78221/

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

Scrutinize any strange emails that you receive, especially if you weren't expecting it, and use your antivirus software to scan any attachments in emails. Phishing scams are getting more clever than ever, and some emails don't have the usual markers (like bad spelling/grammar), so it's worth it to take a moment and really look at what you're receiving. Be wary of strange websites that might steal your information, and don't save credit card and other personal information in your online accounts.

Best Practice #3: Download only from approved sources.
Best Practice #4: Don't give out information to unverified individuals.
Best Practice #5: Be suspicious of email links and attachments.

It's best to always maintain a strong security posture, especially with the dynamic nature of threats on the internet. Being vigilant and cautious now can save a lot of trouble and work later.

Hiding in Plain Sight

Steganography, the art or science of hiding information within something else, has been around since the ancient Greeks.[1] It also has an equivalent in the digital world: digital steganography, a method of hiding data or messages in digital files or other digital structures.[2]

Unlike encryption which encodes messages, steganography attempts to hide the fact that there is a message at all. These messages are not limited to text only; they can be any file type, from images to spreadsheets. The inserted data, files, or messages can also be encrypted, which increases the security of the information.

There are several methods for hiding messages in data files and in this article we will cover three of the most common uses: hiding a message in a data file, an audio file, or in an image.

[1] https://www.wired.com/story/steganography-hacker-lexicon/
[2] http://aisel.aisnet.org/cais/vol30/iss1/22/

How to Hide Data

When hiding a message in a data file, there are two methods that can be used: adding bits to the file itself (in the file header), or after the "official" end of file marker.[3] The first way can be problematic, as adding data to the file causes it to increase in size, possibly tipping someone off that there is a message embedded in the file. The second method is using least significant bits inside the file itself. Each byte[4] in a file is made up of eight bits, but sometimes not all the bits are needed, and are essentially placeholders. Since these bits are not important to the overall file, they can be changed to hold a message while still allowing the file to function. This method is more covert as it doesn't add any size to the file, making it harder to detect a hidden message.

Audio files also have other ways of hiding messages: the typical hissing you sometimes hear in song recordings (most notably in older ones from record players) can be slightly changed to hold a message without significantly altering how the file sounds when played.[5]

Hiding a message in an image is probably the most involved and is usually done using available steganography programs. Individual bits in the image are randomly changed to hold the data. These changes are so small that the image appears to be a normal image. Each bit that has been changed holds part of the message. The higher the resolution in the image is, the more data or message the image can hold.

How This Affects Cybersecurity

Bad actors can use steganography to deploy malware or to smuggle information out of hacked databases, and because it is such a clandestine tactic, it is difficult for antivirus software to detect the activity. The best way to protect yourself is to remain aware of possible phishing attempts: if you avoid clicking on suspicious links or files, you greatly reduce the threat of becoming a victim. And while the potential for nefarious use is great, there are also a variety of practical applications for using steganography. For example, photographers can use it to watermark their work secretly without affecting the images.[6]

[3] https://www.itworld.com/article/2826840/crash-course-digital-steganography.html
[4] A unit of measurement for memory size of digital information
[5] https://www.itworld.com/article/2826840/crash-course-digital-steganography.html
[6] https://petapixel.com/2015/08/07/a-look-at-photo-steganography-the-hiding-of-secrets-inside-digital-images/

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

So Your Information's Been Stolen?

Usually, when you learn that your personal information has been compromised, you turn to something like a credit monitoring company to make sure your identity hasn't been stolen or compromised further. But what happens when the monitoring company itself is compromised, as consumers recently learned happened with Equifax?

In early September, the credit bureau company Equifax revealed that bad actors had stolen millions of individuals' personally identifiable information (PII) linked to credit reports. This appears to have occurred over a sustained period, beginning as early as May 2017. Reports suggest that approximately a third of Americans' information was compromised through the Equifax breach, which means that it is likely that you, or someone in your household, has been affected.

So many details of our lives are stored digitally, making them susceptible to theft by hackers. Unfortunately, situations like this continue to demonstrate that it is simply a matter of when, not if, your PII will be stolen. The Equifax breach may not be the first time you've had your information stolen, and it won't be the last. Below, we've gathered steps you should take to prevent the damage from the Equifax (or another breach) from becoming worse, as well as how you can protect yourself in the future.

How to Protect Yourself from Identity Theft

If you have been a victim of any compromise of your personal information, take these steps to help recover and protect yourself in the future.

1. **Check your credit reports.**

   Not just your credit score, your credit report shows all the accounts associated with you, and can reveal fraudulent accounts if your identity has been stolen. You can request your credit report from each of the three major credit bureaus (Experian, TransUnion, and Equifax) for free, once a year.[1] We recommend getting a report from one bureau every four months. This way, you can maximize the opportunities to check up on, and correct, any erroneous activity. Request your credit report here: https://www.annualcreditreport.com/.

2. **Freeze your credit.**

   If you aren't in the market to make any big purchases (think house or car, where your credit might be checked), consider freezing your credit. When you do this, your data is "frozen" by the credit bureaus, so no one can see the details of your credit report. If someone tries to fraudulently use your PII to open a new line of credit, the credit card or lending company is unlikely to approve it because they receive no information

[1] https://www.equifax.com/personal/education/credit/report/how-to-get-your-free-credit-report

about your credit history.[2] In Florida, it costs $10 to freeze your credit with each credit bureau – but it's free if you have been a victim of identity theft, or if you are over 65 years old. Get more information about how to freeze your credit here: http://www.freshfrom-florida.com/Consumer-Resources/Scams-and-Fraud/Identity-Theft/Security-Freeze-Credit-Report.

3. Place a fraud alert on your credit report.

If you don't want to go so far as to freeze your credit, you can place a fraud alert on your credit report. As a victim of identity theft, you can obtain a fraud alert for seven years; if you haven't been a victim, a fraud alert stays in place for 90 days (but you can renew it). By law, if you initiate a fraud alert with one credit bureau, it must extend to the other bureaus as well, so you'll only need to contact one bureau. Get more information about a fraud alert here: https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

4. Report it.

If you discover that you're a victim of identity theft, contact your local law enforcement agency. Even if they are unable to carry out an investigation and make an arrest, having a police report on file is helpful, and sometimes necessary, when trying to correct fraudulent activity (to waive the fee for a credit freeze due to identity theft, a police report is required).

It is also a good idea to report it to the Federal Trade Commission (https://identitytheft.gov/). Their website contains numerous resources to help you recover.[3] If you live in Florida, the Attorney General's office has an identity theft victim kit available on their website as well (http://myfloridalegal.com/identitytheft).

5. Think long term.

If bad actors have your compromised information, they may not immediately use it. The past few years have seen a spike in fraudulent tax returns filed with the IRS, and a breach like Equifax's may mean that your information could be used during tax season in the coming years.

A credit freeze does not prevent tax-related identity theft,[4] so be prepared for the next tax season by having all of your documents in order, and prepare to file early so you can preempt anyone who might try to steal your return.

The IRS will issue an Identity Protection PIN (IP PIN) if you have been a victim of identity theft. However, if you filed a tax return in Florida, Georgia, or the District of Columbia last year, you are eligible for an IP PIN, even if you haven't had your identity stolen. An IP PIN helps to prevent fraudulent misuse of your Social Security Number for federal tax returns, and they send you a new one every year. Find out more information at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

[4] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#place
[3] https://identitytheft.gov/Steps
[4] https://www.cnbc.com/2017/09/18/your-next-worry-after-the-equifax-breach-fake-tax-returns.html

Design 101

Color Me Successful: Understanding Color (Part 1)

"This doesn't look anything like the picture on the screen! The colors are way off, ***why is that?***" That's a great question with an answer that won't make sense unless you understand a few basic concepts about color. To start with, we'll need to look at how color works before it even shows up on a computer screen. This article will focus on the two most well-known color models and how they work; this lays the groundwork for talking about how these models come into play in your every day workload for the next issue.

RGB Color Model

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

So we've got the RGB model, with keywords ***additive*** and ***light***, and the CMYK model, with keywords ***subtractive*** and ***pigmented***. The big question now is, "Why does any of that matter?" Before we answer that, think about this: what is your computer screen made of? Thousands of little lit-up squares called pixels. ***Colored light***. What are your hard-copy prints made of? Thousands of little ink dots. ***Colored pigments***. You interact with both these color models everyday and you didn't even know it.

With the RGB model at work on your computer screens and the CMYK model working in your prints, we're ready to discuss how to really make them work for *you* in the next issue, to ensure that your work is as accurate to real-world color as it can be. Look forward to the January 2018 edition for **Color me Successful: Understanding Color (Part 2)**!

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.

Facebook has your number – even if it's not your number

https://nakedsecurity.sophos.com/2017/07/20/facebook-has-got-your-number-even-if-its-not-your-number/

- Telephone numbers are used to aid password resets, and so someone could falsely add another user's telephone number in an effort to hijack the account.
- Another vulnerability that exists is if a user changes their telephone number, but fails to update their profile.

Analyst Note: Facebook regularly updates their default privacy settings, so make sure to keep an eye on yours. Set your profile to alert you for any unrecognized login attempts, and verify that phone numbers listed on your profile are the ones in use by you.

Disney sued for tracking kids on its mobile games

http://mashable.com/2017/08/04/disney-lawsuit-ad-tracking-kids-mobile-games/?utm_cid=hp-n-1#EsVufbQPpmqq

- The Federal Trade Commission (FTC) has very strict rules about the kinds of information internet companies can collect on users under 13 years old. These regulations, laid out in the Children's Online Privacy Protection Act (COPPA), cover not only what kind of data can be collected on these users, but how it must be stored and protected as well.
- Disney came under fire recently for allegedly using ad tracking software in some of their web-based games for kids, and is currently the subject of a lawsuit for violation of COPPA.

Analyst Note: It is important for parents to understand how internet privacy rules work. COPPA is the reason why most social media sites require users to be over 13, because then the sites are not required to comply with its stricter privacy regulations.

Hacker Helps Family Recover Minivan After Losing Key

https://www.bleepingcomputer.com/news/technology/hacker-helps-family-recover-minivan-after-losing-one-of-a-kind-car-key/

- A family lost the keys to their car, only to discover they had a "smart" key, unable to be replicated by either the dealership or a key duplicator.
- Ultimately, the family was saved by a hacker, who was able to reprogram the car to be compatible with three newly created keys.

Analyst Note: This kind of situation may become more commonplace as more sophisticated technology becomes integrated into all aspects of our lives. While some of these risks can be anticipated, there are likely to be some pitfalls as we increasingly rely on computers for things large and small.

Facial recognition tech leads to 4,000 New York arrests

https://arstechnica.com/tech-policy/2017/08/biometrics-leads-to-thousands-of-a-ny-arrests-for-fraud-identity-theft/

- New York implemented a facial recognition system for its driver's license system back in 2010, which now has a database of over 16 million photos.
- As a result of this system, law enforcement has identified more than 21,000 possible identities associated with civil and criminal cases.

Analyst Note: We talk a lot about the importance of biometrics in cybersecurity, and this is a great example of a success using biometrics. Improved facial recognition technology will revolutionize how we catch criminals in the future.

Why You Should Be Encrypting Your Devices

http://fieldguide.gizmodo.com/why-you-should-be-encrypting-your-devices-and-how-to-ea-1798698901

- Encryption of your mobile devices, while a complex technical process, is actually a very simple, and important, way to secure your data. It prevents others from hacking into the information on your device unless they have the password.
- Apple devices and newer Android devices have an encryption feature pre-built into their security settings, and full encryption of your device is as easy as enabling that function.

Analyst Note: Tech companies have been making it easier than ever for end users to incorporate encryption into their devices and browsing habits. It's important, however, to keep good cyber hygiene practices in other areas so as to not defeat the encryption features you have in place.

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 lightning 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 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

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