The Beacon

Florida Fusion Center #19-108 | Cyber and Critical Infrastructure Report | April 2019, Issue #19

Summary

An Apple a Day Keeps the Malware Away… Or Does It? - It's been said that Apple devices don't suffer from malware, but is that really true?

Can You Hear Me Now? 5G Voice Security - Faster mobile data is coming, but have security risks from previous generations been fixed?

A Chip On Your Shoulder: Humans Becoming IoT Devices - We may be approaching the day when man and computer merge. Explore the state of implantable tech and what that means for cybersecurity.

AIn't I the Brightest? - In what ways is AI both helping and hurting cybersecurity? We take a look.

In A Position to Solve Crimes: GPS and Law Enforcement - Several recent arrests have highlighted the unconventional ways that the Global Positioning System assists law enforcement.

Under Lock and Key: What is Cryptography? - Ever wondered what makes data secure? Learn about encryption standards and the algorithms that keep your data from prying eyes.

Data Protection in the U.S. - The European Union just enacted a sweeping personal data privacy bill that has had far-reaching impact. Could a similar bill be on the horizon here in the U.S.?

Protecting Kids Online: A Guide - Our advice for keeping your kids safe on the internet.

Contents

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

Editor's Corner

Where Are You Leaving Your Data?

You've improved your passwords, updated your privacy settings, and avoid using public Wi-Fi. Your home router password is 20 characters long. You can spot a phishing email from a mile away. But where are you leaving your data just laying around for someone to find?

Spring is a good time to think about cleaning up; not just the eaves and closets, but the places where you may have stored data in the past, too. We often don't think of some portion of our identifiable data being left on old devices, or the devices that we connect to. One recent study collected refurbished laptops and cellular phones (meaning gently-used devices that had been factory reset to be sold at discounted prices) and ran programs on them to scour for fragments of old files and documents that survived the reset and still contained personally identifiable information (PII).[1] The results were startling. Of the 85 devices tested, only two had been properly sanitized. Over 700 instances of PII were found across all of the devices.[2] Donating your old tech is a great way to give to those in need, but it is important to make sure you're properly disposing of your data, too. There are several software tools available to help you permanently delete data available on the internet.[3] If you decide that the risk is too high to chance your data falling into the wrong hands, the most effective means of data destruction are physical: take a hammer to the device, incineration (be careful with this one; look up how to do this safely), industrial shredding, electrolysis, or drilling at least three holes into the drive.[4] Why doesn't just deleting files work? When you delete a file, it isn't truly "deleted." Rather, the operating system flags the space where the file is located as available for being overwritten. If the space is never overwritten, the data is still lurking there somewhere.[5]

We've talked before in previous editions of the Beacon about who is responsible for deleting your data from Bluetooth-enabled infotainment and GPS systems in rental cars,[6] and the truth is no one has that official duty. That leaves it up to the consumer to protect their data and delete the information before returning a vehicle, but the best thing to do would be not to use that type of connection in the first place (an auxiliary cord connection is better). It's smart to remember to delete your device profiles before trading in a used car for a new one, as well. We can extend this line of thinking to every Bluetooth connection we encounter. Many electronics stores may have Bluetooth-enabled devices available for testing before purchase, but it is advisable to avoid doing this on unfamiliar devices.

Additionally, online profiles and email accounts that we abandon can hold a wealth of information. Remember to log in and delete what you don't use anymore. Just as we may spend some time in the coming weeks tidying up our house, it's a good idea to take stock of what old devices we may have and what we might be currently connected to.

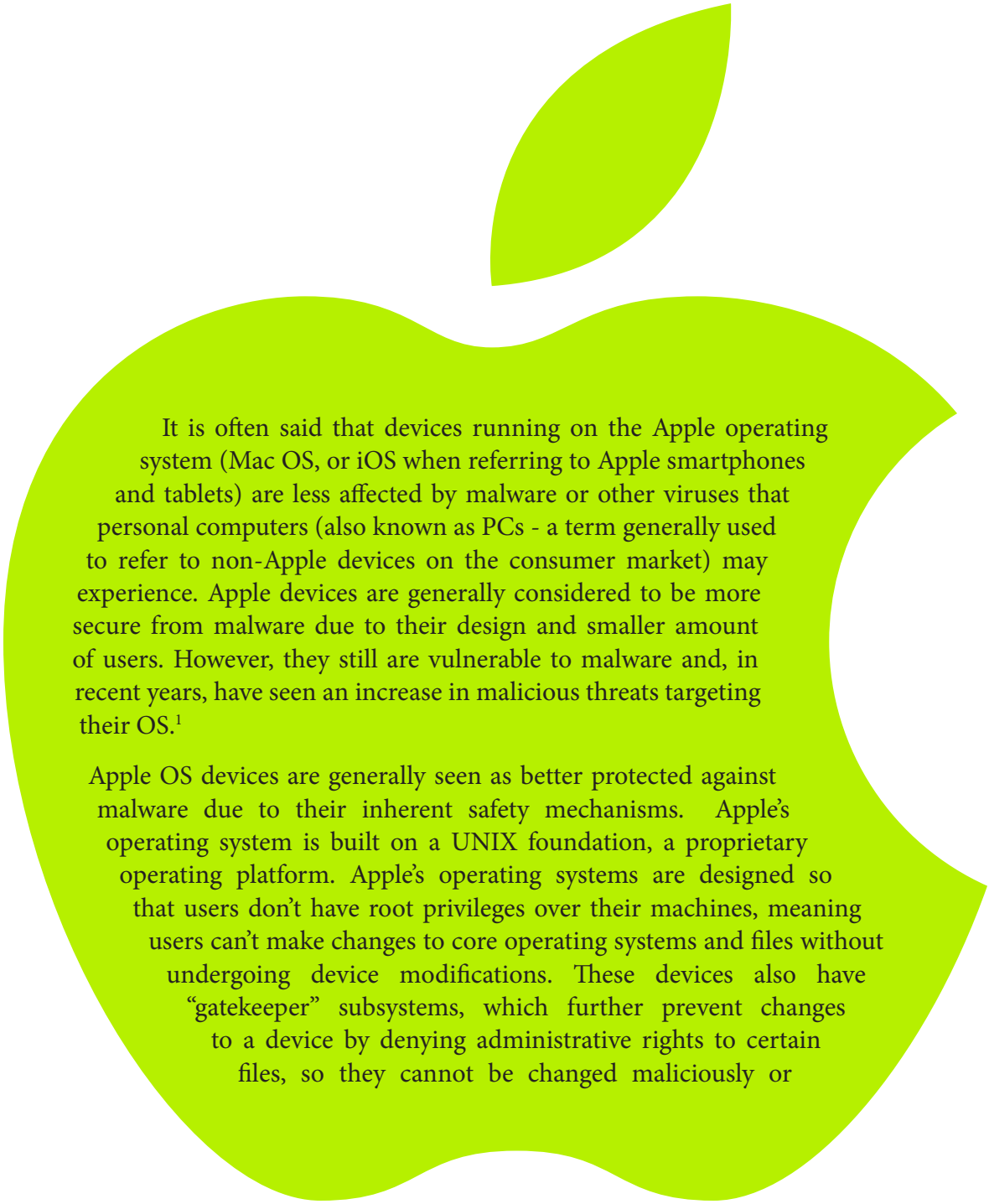
[1] https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/
[2] Ibid.
[3] https://www.lifewire.com/how-to-wipe-a-hard-drive-2624527
[4] https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/
[5] https://gizmodo.com/its-scary-how-much-personal-data-people-leave-on-used-l-1833383903
[6] http://secureflorida.org/vendorimages/secureflorida2007/2018%20Quarter%202%20Beacon.pdf

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

Cyber Threats

An Apple a Day Keeps the Malware Away… Or Does It?



It is often said that devices running on the Apple operating system (Mac OS, or iOS when referring to Apple smartphones and tablets) are less affected by malware or other viruses that personal computers (also known as PCs - a term generally used to refer to non-Apple devices on the consumer market) may experience. Apple devices are generally considered to be more secure from malware due to their design and smaller amount of users. However, they still are vulnerable to malware and, in recent years, have seen an increase in malicious threats targeting their OS.[1]

Apple OS devices are generally seen as better protected against malware due to their inherent safety mechanisms. Apple's operating system is built on a UNIX foundation, a proprietary operating platform. Apple's operating systems are designed so that users don't have root privileges over their machines, meaning users can't make changes to core operating systems and files without undergoing device modifications. These devices also have "gatekeeper" subsystems, which further prevent changes to a device by denying administrative rights to certain files, so they cannot be changed maliciously or

unintentionally.[2] In other words, Apple makes it very difficult for users to download, install, and run malware, but it is not entirely impossible.

PCs are utilized by more users worldwide than Macs. In 2017, there were an estimated 400 million active users of Windows 10 alone (not including other versions of Windows) and an estimated 100 million Mac users, making Windows 10 four times more prevalent than all Mac OS devices.[3] Criminals have more incentive to design and deploy malware that will interact with the most devices. Designing viruses to infiltrate non-Apple operating system devices would allow them to potentially infect a greater number of machines.[4] This may help to explain why we don't see the same numbers of malware targeting iOS users.

A recent report by an independent security institute found that the Apple operating systems experienced three times more attacks in 2017, as compared to 2016. In 2016, 3033 malware samples were identified, compared to 819 in 2015.[5] Other threats to the Apple operating systems include spyware, keyloggers, backdoors, adware, and potentially unwanted programs.[6] OSX.Coldroot, a recently discovered remote access tool (RAT) malware that affects Apple devices, creates a backdoor on the system and grants the intruder root access while also installing a keylogger. Fortunately, OSX.Coldroot contains multiple bugs in its programming, and fails on most iOS versions after 10.11, which is a good reason to keep software updated.[7] Another Mac malware, OSX.CreativeUpdate, was discovered as part of a supply chain compromise involving a third party Apple application store. Links on the store were replaced with malware files that, when downloaded and installed, used the host machine to mine cryptocurrency.[8] By the end of 2017, a private antivirus firm counted 270 percent more unique threats on the Mac platform than in 2016.[9]

Because Apple OS devices are vulnerable to malware, it's best for users to integrate security measures into their devices to ensure operational integrity and protect against malicious infiltration. Antivirus protection software can be used to prevent computer viruses. Experts also recommend keeping computer software up to date to prevent malware from exploiting bugs in older code.[10]

[1] https://www.computerworld.com/article/3262225/warning-as-mac-malware-exploits-climb-270.html
[2] https://www.digitaltrends.com/computing/can-macs-get-viruses/
[3] https://www.theverge.com/2017/4/4/15176766/apple-microsoft-windows-10-vs-mac-users-figures-stats
[4] https://www.securemac.com/malware/viruses-on-mac-what-you-need-to-know
[5] https://blog.malwarebytes.com/101/2018/03/the-state-of-mac-malware/
[6] https://www.malwarebytes.com/mac-antivirus/
[7] https://blog.malwarebytes.com/101/2018/03/the-state-of-mac-malware/
[8] Ibid.
[9] Ibid.
[10] https://www.macworld.co.uk/feature/mac-software/can-macs-get-viruses-3454926/

Cyber Highlights

Can You Hear Me Now? 5G Voice Call Security

Mobile data networks are the means by which mobile devices make calls, send text messages, and connect to the internet. Your phone will usually connect to a mobile carrier's network by default when your phone is on. Currently, fourth generation (4G) mobile data connection is the dominant protocol for cellular communications. Researchers have recently conducted a comprehensive security analysis on fifth generation (5G) mobile communication, but it has not yet been implemented widely for consumer use. The results of the report indicated that overall data protection is better than previous standards of 3G and 4G. The 5th mobile communication generation provides users with significantly more security in a number of areas, including more varied authentication methods and improving encrypted key management. But known flaws in the signaling protocols used in previous data network connection generations have been carried over into 5G as well. This poses threats in which traffic can potentially be spoofed or intercepted.[1]

When looking at the big picture, it's important to note how many users may be potentially affected by cellular communications vulnerabilities. Two-thirds of the world's population, roughly 5 billion people, use smart phones or other mobile devices every day. The massive number of users makes exploiting vulnerabilities potentially lucrative for criminals. Exploitation of a trusted mobile data network would allow bad actors to steal information in a manner that may be hard to detect.[2]

The Evolved Packet Core (EPC) architecture used by 4G and 5G wireless networks is a framework for providing converged voice and data on a Long-Term Evolution (LTE) network.[3] The EPC can be exploited by intercepting and collecting mobile data, as well as launching denial-of-service (DoS) attacks.[4] Research suggests that attackers looking to exploit these types of vulnerabilities do not need considerably hard-to-obtain tools or even considerable skills. Before 4G LTE, intercepting voice calls required specialized equipment and in-depth knowledge of the specific protocols used in voice transmissions. 4G switched to an all-IP network, meaning that threat actors could utilize conventional hacking tools, which are largely automated and do not require a deep understanding of

[1] https://www.csoonline.com/article/3267693/security/dont-rush-to-deploy-5g-if-you-want-iot-security-agency-warns.html
[2] https://www.ethz.ch/en/news-and-events/eth-news/news/2018/10/security-gaps-in-the-5g-standard.html
[3] https://searchnetworking.techtarget.com/definition/Evolved-Packet-Core-EPC
[4] https://www.darkreading.com/perimeter/new-4g-5g-network-flaw-worrisome-/d/d-id/1330062

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

the nature of the attack.[5]

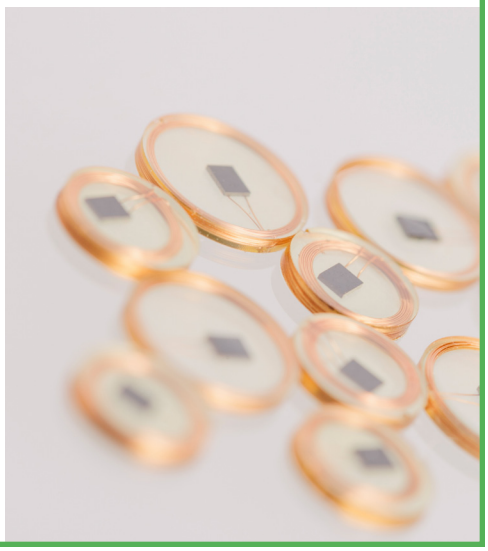
The EPC nodes have been previously exposed on the internet, which can pose great vulnerability to being hacked, and can be used by hackers trying to gain access to the infrastructure to launch other attacks. Security researchers assert that groups with an interest in these types of attacks are most likely nation-state actors and cybercriminals seeking to commit bank fraud or other types of crimes.[6]

The potential attack scenarios can be divided into three categories: interception of data, which can include text messages and unencrypted email; collection of data, which can include the location of the device; and disruption of services, such as the previously mentioned DoS attacks. Enterprises should be aware that when something is sent over 5G, it has the potential to be intercepted, and, as such, should take care to send communications only through encrypted means.[7]

Overall, 5G networks have vulnerabilities that pose risks to its users that may be exploited. In order to try and mitigate these risks, it is important to take necessary precautions. Enterprises are advised to use applications and services that have the latest versions of transport layer security (TLS), or HTTPS, which can assist in ensuring that data sent and received cannot be easily decrypted when connected to a website. For individual users, it is recommended to rely on encrypted communication apps, rather than regular SMS/MMS texting, for any data that might be sensitive.[8] Though exploitation of mobile networks has not been a widespread issue up until this point, it is wise to be aware of issues going forward. Good security posture can mitigate any damage should these vulnerabilities be targeted.

[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

A Chip on Your Shoulder: Humans Becoming IoT Devices

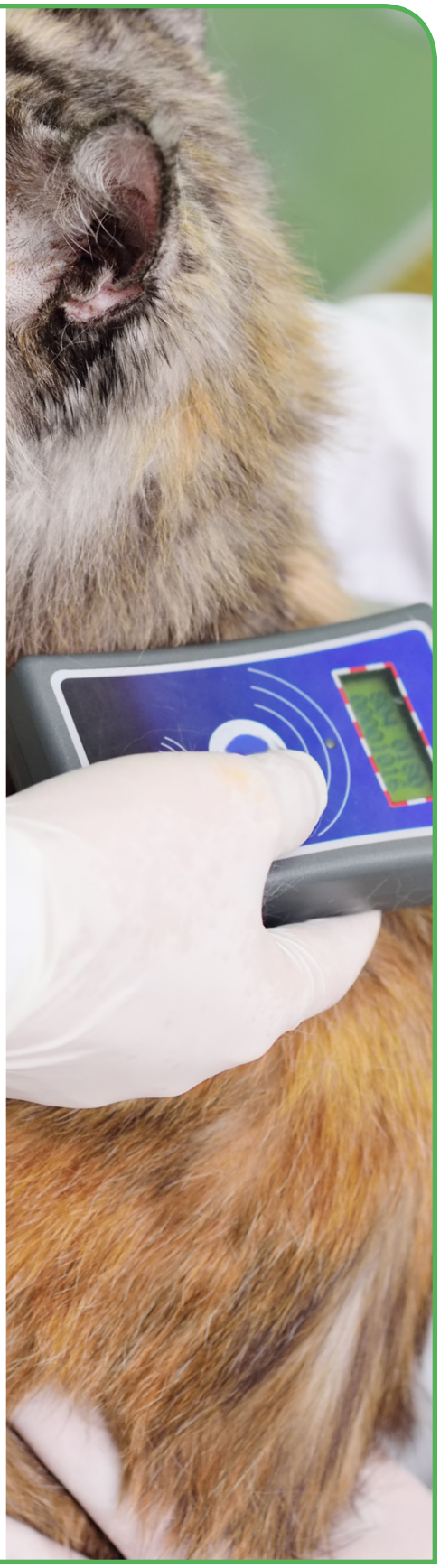


Science fiction movies have long depicted a future full of tech right at our fingertips, and sometimes in our fingertips. Some of these fantastical ideas are not so far off, though. Recently, implantable chips have made headlines as a novel idea that could serve a multitude of uses. You could wave your hand in front of a reader and pay for your groceries instead of carrying a wallet full of credit cards; your chip could carry your identifying information so that you won't need to worry about losing your identification card or passport; or a chip could relay real-time updates about your health to a doctor. You would become a human part of the Internet of Things; not a robot or cyborg, but a human component of a digitally interconnected world. As with any advancement in technology, there are several security concerns that arise with

technology that is being implanted directly into a human body.

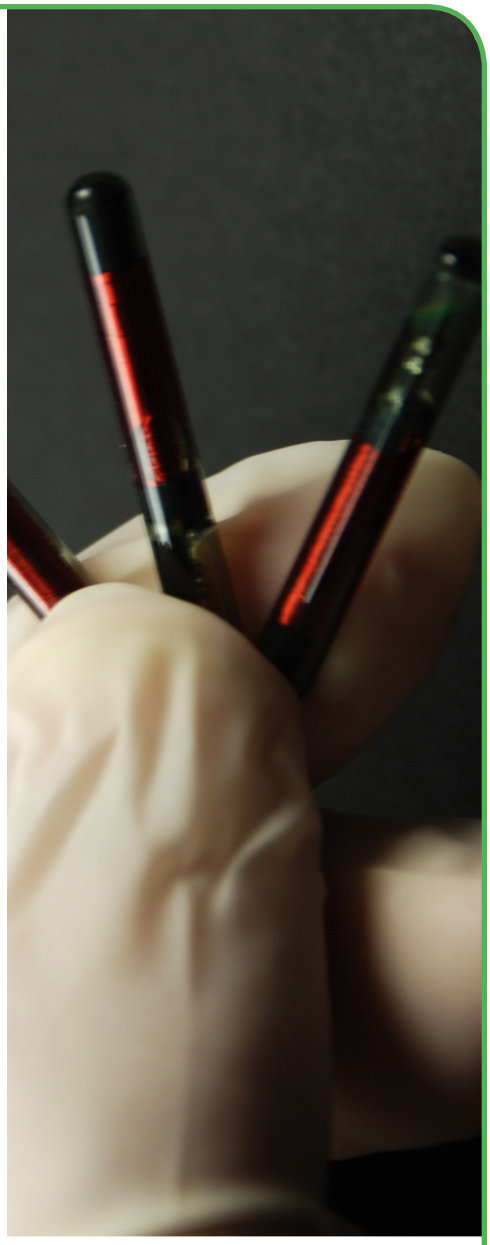
But first, where does this technology stand today? The most common implantable tech is usually a radio-frequency identification (RFID) chip, usually inserted just under the skin in a fleshy area (like the area between your thumb and forefinger). The chip is general contained in a non-reactive capsule (meaning it won't irritate or damage the surrounding tissue) with a small antenna for receiving and transmitting signal. They generally don't have a power source built in (like a battery), and only activate when a reader is close by.[1] This is the same technology used to microchip pets, and the chips can only hold limited information. Because of this, their use is pretty limited, but they can do things like store ticket information, identification, or payment information.[2] Some companies even use them in place of personnel badging, allowing users to access their offices, gyms, and homes by swiping their hand in front of readers.[3] The risk of exploitation with these devices is low as the information on them can only be picked up by a reader in extremely close proximity. They can't be tracked, like a GPS, and can't really do anything other than transmit data because of the lack of a power source. A battery can't feasibly be installed with the chips because they would either be too large or would eventually run out of charge.[4] It wouldn't be impossible to use them for nefarious purposes, but the effort for such little return makes it a low value target. A hacker might have more luck tracking or infiltrating a cell phone, which some users might keep so close that it is practically an implant itself. And yet, there is already talk of making physical cell phones a thing of the past, as well. Companies are developing concepts for cell phone implants to allow you to make calls in your head or even see a phone screen light up on the skin of your arm.[5] These may become more attractive targets as technology progresses to allow smaller, more powerful computers to be implanted within us.

An area where human IoT technology is making strides is in healthcare. These devices aren't as seamless as implanted chips, but they also have more complex functions. Modern medicine has meshed with technology to give us enhanced capabilities in diagnosis and treatment, so having medical devices implanted seems like an obvious next step. Brain implant devices (electrodes attached to a small, battery-powered chip) help with all sorts of neural ailments, including depression, seizures,



and schizophrenia. Digital pacemakers, tasked with regulating heartbeats, can be accessed by doctors to check for abnormalities or download a history of cardiac activity. Such devices, and other similar implanted health-measuring gadgets, have obvious benefits but the security concerns should give anyone pause. While there have been no verified cases of these devices being hacked, several security holes have caused panic in both patients and manufacturers, causing recalls and urgent notices to update firmware.[6] The consequences could be dire: a bad actor could, in theory, cause a pacemaker's battery to drain prematurely or cause irregular shocks to the heart. A way around these frightening possibilities is to use devices that can't be accessed remotely, but adjusting these devices often means repeated surgeries that come with their own risks.[7]

We're still a long way off from that glorious interconnected future where we don't have to carry a wallet anymore, but we are making strides to get there. Like all advancements in technology, for every two steps forward we must also take a step back to consider the security holes we may be passing on to the next generation of devices. Where a hacked IoT device (such as a camera or thermostat) may be an annoying experience, hacking a part of your body can have more pressing consequences.

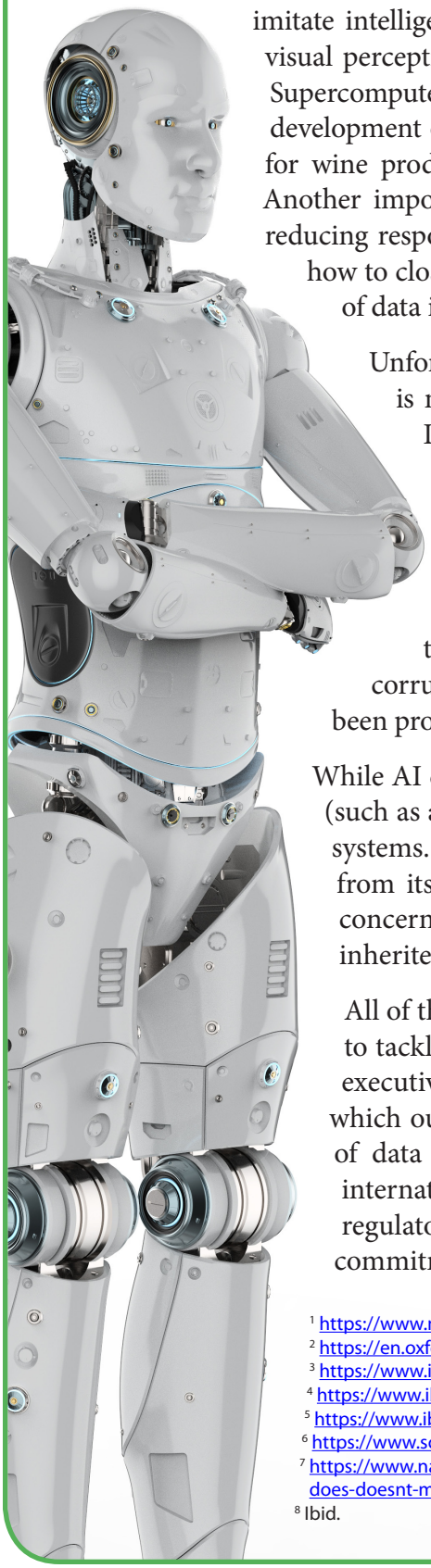


[1] https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/
[2] Ibid.
[3] https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-micro-chips-under-their-skin
[4] https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/
[5] https://www.cnet.com/news/the-mobile-phone-of-the-future-will-be-implanted-in-your-head/
[6] https://www.nextgenexecsearch.com/iot-medical-devices-transforming-healthcare/
[7] https://www.reuters.com/article/us-health-heart-pacemaker-cyber/pacemakers-defibrillators-are-potentially-hackable-idUSKCN1G42TB

AIn't I the Brightest?

Technology has advanced leaps and bounds in recent decades, with perhaps the most exciting of these advancements taking place in the developing field of artificial intelligence. While artificial intelligence (AI) today has yet to reach the same level of sophistication as that portrayed in science fiction literature, films, and television shows, every day developers move one step closer to making science fiction a reality.

Artificial intelligence is defined as the intelligence exhibited by machines or software that can be used to perform tasks which normally require human input, or the capability of a machine to



imitate intelligent human behavior.[1] These tasks cover a variety of fields including visual perception, speech recognition, decision making, and language translation.[2] Supercomputers with AI have been used for everything from assisting in the development of irrigation systems that resulted in increased quality of grapes used for wine production,[3] to improving customer service in the banking industry.[4] Another important application of AI is deployment for cybersecurity, drastically reducing response times for security analysts when counteracting threats, learning how to close holes in security nets for companies in the process.[5] As the amount of data increases, reliance on AI to help protect it will also increase.

Unfortunately, bad actors are always trying to get past protections, and it is no different with AI. In what has been dubbed Adversarial Machine Learning (AML), adversaries try to manipulate AI data and algorithms to trick it into letting in malware.[6] Bad actors can deluge a system with false negatives (malware designed to look benign), causing security analysts to potentially ignore alerts. Another way to thwart AI protections is to use poisoning attacks, which uses false data to taint the AI training data set. Once the data set has been changed, the AI can no longer detect malicious threats effectively as it uses corrupted data to "learn." Threat actors may also use their own AI that has been programmed to trawl the internet looking for vulnerabilities to exploit.

While AI can undoubtedly help connect the dots in a number of different ways (such as analyzing and sorting data), there is a growing concern for bias in AI systems. By definition, AI is in a state of constant learning, picking up nuances from its human developers and applying them to the tasks set for it. This concern has led to studies which have found that some AI systems contained inherited racial or socioeconomic bias.[7]

All of these concerns and more are high on lawmakers' priority lists of issues to tackle with legislation. On February 13, 2019, President Trump signed an executive order establishing the American Artificial Intelligence Initiative, which outlines five key areas of focus: research and development, availability of data and resources, ethical standards and governance, education, and international collaboration that also protects American interests.[8] This regulatory move is a mark of the potential of AI and identifies a national commitment to improvements in years to come.

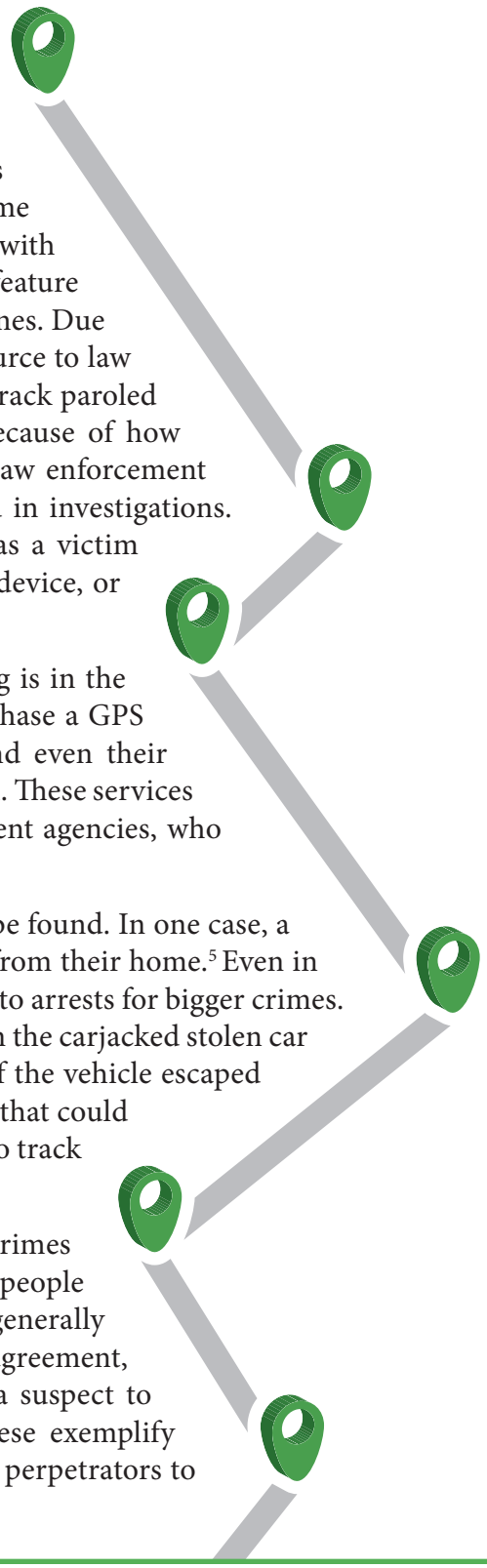
[1] https://www.merriam-webster.com/dictionary/artificial%20intelligence
[2] https://en.oxforddictionaries.com/definition/artificial_intelligence
[3] https://www.ibm.com/watson/stories/ejgallo/
[4] https://www.ibm.com/watson/stories/bradesco/
[5] https://www.ibm.com/security/artificial-intelligence
[6] https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/
[7] https://www.nationalgeographic.com/science/2019/02/what-trump-american-artificial-intelligence-initiative-ai-does-doesnt-mean/
[8] Ibid.

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

In A Position to Solve Crimes: GPS and Law Enforcement

The Global Positioning System, or GPS, is a utility owned by the United States government.[1] The system consists of 27 orbiting satellites that can communicate with devices (called a receiver). The receiver makes contact with 4 or more of the satellites and uses the distance of these satellites to calculate the receiver's location.[2] GPS provides real-time location and movement information for anyone or anything with an active GPS device. GPS services have become a common feature of many internet-enabled devices, including cars and cell phones. Due to its prevalence, this technology can provide a valuable resource to law enforcement that can also be used to manage a police force, track paroled inmates, gather evidence, and locate criminals.[3] Perhaps because of how integrated GPS functionality has become in many devices, law enforcement is now more able to use location data to solve crimes or aid in investigations. Solving some crimes may be aided by something as small as a victim or perpetrator leaving their location setting turned on their device, or using an app that tracks such data.



The most well-known example of GPS-enabled crime-solving is in the form of GPS devices for asset recovery. Consumers can purchase a GPS locator for their vehicle, heavy construction equipment, and even their laptop that can be activated in the case that it is reported stolen. These services usually have a direct terminal to participating law enforcement agencies, who can then track the exact location of the stolen item.[4]

Some devices don't even need a third-party GPS program to be found. In one case, a victim's smart watch was tracked via GPS, after it was stolen from their home.[5] Even in much larger cases, tracking stolen items and vehicles can lead to arrests for bigger crimes. For instance, the Boston Marathon bombers were caught when the carjacked stolen car they used as a getaway vehicle was tracked after the owner of the vehicle escaped and called the police.[6] The vehicle had a GPS location service that could be activated in the event that it is stolen, allowing authorities to track its movements.[7]

GPS data has revealed critical information in other types of crimes as well. As mentioned before, GPS data can be used to track people already convicted of crimes. Though ankle GPS monitors are generally used to track probationers and parolees as part of a release agreement, the coordinates from such devices have been used to link a suspect to crimes committed while under observation.[8] Cases like these exemplify the other uses of GPS data to either help solve crimes or link perpetrators to crimes during trial.

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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

It is important to know that the private GPS activity from citizens' vehicles and devices is not being actively monitored by the government and may well be protected by the Fourth Amendment, federal law, or state law depending on the circumstances.

[1] https://www.gps.gov/systems/gps/
[2] https://electronics.howstuffworks.com/gadgets/travel/gps.htm
[3] https://www.brickhousesecurity.com/gps-trackers/how-police-use-gps/
[4] https://www.lojack.com/for-law-enforcement/
[5] https://www.cultofmac.com/609756/apple-watchs-gps-helps-track-down-burglars/
[6] https://www.npr.org/sections/thetwo-way/2013/04/26/179296836/driver-hijacked-by-tsarnaev-brothers-helped-police-trace-them
[7] https://www.dailymail.co.uk/news/article-2991365/Boston-bombing-jury-photos-slain-police-officer.html
[8] https://www.sun-sentinel.com/local/palm-beach/fl-pn-convicted-rapist-probation-violation-sentence-20180618-story.html

Under Lock and Key: What is Cryptography?

With modern technological advancements, the internet has become a double-edged sword. We are able to use the internet for a multitude of things, from getting and storing information, to communicating with others, to making and spending money. However, a lot of sensitive information is also added to the internet every time we use it, and this sensitive information is not always protected from prying eyes. With the science behind cryptography, the sensitive information that is transmitted through the internet can be encrypted and protected.

What is Cryptography?

Cryptography is a key component of protecting information and communication between two parties.[1] Cryptography uses encryptions to encode the information that is being sent, so only the authorized parties can access it. Some types of encryption use what is called a "key," which is usually a random string of bits (a basic unit of information in computing) generated to scramble and unscramble data. It ensures confidentiality, integrity, non-repudiation, and authentication.[2] There are three main encryption methods used to secure information:

- Single-key, or Symmetric-key, encryption uses one key to encrypt and decrypt information, hence the name. This encryption type is primarily useful for protecting stored sensitive information but not transmitting it.[3] The most widely used single-key encryption is the Advanced Encryption Standards (AES), which is a block cipher (a method that encrypts

entire blocks of text, rather than one bit at a time) that is implemented in software and hardware.[4]

- Public-Key, or Asymmetric-Key, encryption uses two different keys to encrypt and decrypt information. The first key is a public key that is used to encrypt the information, and the second key is a private key that is used to decrypt the information.[5] This type of encryption is a bit more complicated, but it allows information to be sent between two parties more securely. There are several systems that implement public-key encryption, but one of the most successfully used on the internet is the Rivest-Shamir-Adleman (RSA). This encryption method is based on the presumed difficulty of factoring large integers (meaning it would be too hard to guess a set of generated large numbers that are used as keys). Secure Socket Layer (SSL - the secure connection that shows up as a padlock next to the address bar when you visit a website) uses a mix of asymmetric and symmetric key encryption to secure your browsing.[6]
- Hash functions are used to change a message into an unreadable string of text. Hash functions are commonly used to protect large files and software when transmitting them to a second party. Hashing also ensures that data hasn't been tampered with as any minute change would also alter the hash. Many websites and databases also store passwords as a hash value.[7] The most used hash functions are MD5 and SHA-1 (Secure Hash Algorithm 1).[8] Below you can see the word 'password' in both MD5 and SHA-1 hash.

  MD5: 5f4dcc3b5aa765d61d8327deb882cf99

  SHA-1: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

Why is cryptography important to cybersecurity?

Cybersecurity depends on cryptographic encryption methods to protect computer systems and the data that the systems store, retrieve, and send. Without cryptography this sensitive data would be available to everyone and anyone to take and misuse. Cyberattacks continue to occur with greater frequency, and threats come from all types of adversaries. As technology evolves towards concepts like quantum computing, hackers are able to anticipate the repeating processes of encryption algorithms and access secure information more easily.[9]

Quantum computing utilizes the laws of quantum mechanics to solve complex problems at a faster rate than classic computers.[10] This type of computing will allow scientists to discover new areas of science, technology, engineering, and mathematics. However, like the internet, quantum

computing has the ability to be a double-edged sword. Hackers can use quantum computers to decrypt encrypted data at faster rates and pose a serious security risk to all the sensitive information that is found on our computer systems.

Taking into account the issues quantum computers may pose, an infrastructure security software company developed a new encryption that, in theory, will prevent hackers from predicting the repeating processes of current static encryption types. The company's Anti-Statistical Block Encryption (ASBE) uses randomization in its encryption process to eliminate the static behavior that is seen in the other types of encryption. ASBE also incorporates factors that use temporary and "always unique" to its authentication process. This new incorporated factor is also random like ASBE.[11] It is possible that we will see more of ASBE or similar methods in the future as an option for encryption.

The standards of encryption will continue to evolve to meet privacy needs. It's always good to make sure you're encrypting any sensitive data and to make sure that your connection is secure when you're browsing online. Most major companies and banking institutions use encryption when storing passwords, making transactions, and protecting other critical data. If you are curious as to how your interactions are protected, you can contact the institution to inquire.

[1] https://searchsecurity.techtarget.com/definition/cryptography
[2] https://www.garykessler.net/library/crypto.html#intro
[3] https://www.btcwires.com/glossary/cryptography/
[4] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[5] https://www.btcwires.com/glossary/cryptography/
[6] https://www.digicert.com/ssl-cryptography.htm
[7] https://lifehacker.com/how-your-passwords-are-stored-on-the-internet-and-when-5919918
[8] https://www.btcwires.com/glossary/cryptography/
[9] http://www.govtech.com/security/Is-Cybersecurity-Encryption-Ready-to-Break.html
[10] https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/
[11] http://www.govtech.com/security/Is-Cybersecurity-Encryption-Ready-to-Break.html

Data Protection in the U.S.

On May 25, 2018, the European Union enacted regulation regarding data privacy called the General Data Protection Regulation, or GDPR. The GDPR affects businesses of all sizes and will regulate how a company gathers, stores and looks after personal data. Companies that aren't headquartered in European countries but do business with European consumers are subject to the law. That means that even American companies that operate in Europe must abide by the GDPR. This is a concept known as data sovereignty. The GDPR requires personal data to be encrypted and the owner of the data (in this case, the person that the data refers to) may inquire what information the company stores and may request the data be erased. Additionally, a company that suffers a data breach will need to report this information within 72 hours of discovering the breach.[1] You may have noticed some of the effects of GDPR when visiting websites, which now prompt you to accept a privacy agreement concerning the information they keep. The U.S. currently does not have a federal-level data privacy law but several states have passed their own similar regulations. California, Illinois, and Vermont

have some sort of law that impacts data privacy, and most states have some law concerning data breaches. The result is a patchwork of different, and sometimes conflicting, laws that make it difficult to have a cohesive response plan for both the state and private entities.

Several large tech companies have requested that the federal government enact a law to supersede state laws, with the Federal Trade Commission as the regulating federal agency.[2] This would standardize both response to incidents and regulate how and for what purpose data can be collected. Currently, U.S. consumers do not benefit from any provisions of the GDPR even though U.S. companies are obligated to comply.[3] This does not mean that U.S. consumers haven't benefitted from the GDPR in other ways. Facebook has made its privacy settings more prominent and easier to navigate for all users and Google, though it hasn't substantially changed its collection practices, has made its privacy policy easier to understand.[4] It should be noted that at this time, tech companies have submitted recommendations but no formal legislation has been introduced or approved. The potential impact of this federal law will likely have some positive and negative effects. The possible positive benefits might include:

- Consumers that have had their personal data compromised will be notified within a certain amount of time upon the company finding the breach.[5]
- Consumers may opt out of having their personal identifiers on file with a specific company.[6]
- Consumers may request to know the specific personal data a company has on file, which requires the businesses to be transparent. They will also have the "right to be forgotten," meaning they can request that the data be deleted.[7]
- Businesses are required to have a privacy policy and it must be written in plain English, which will make them easier to understand.[8]
- Having one data privacy law will standardize practice across the country, instead of multiple different laws across states.[9]

A federal data privacy law may have good intentions but may also have unintended consequences. Many of the companies who have submitted suggestions have also been clear on the pitfalls they wish to avoid. Some of the concerns these suggestions try to address are that the requirements for data access be reasonable and that data deletion not conflict with the operation of business or lead to the breaking of other laws. Additionally, there is some concern that a U.S. law that differs too greatly from laws enacted elsewhere (like GDPR) would create overlapping, inconsistent, or conflicting rules.[10]

There is no "one size fit all" law or regulation when it comes to data security, but with a federal law there will at least be some standardization of practice. Lawmakers will have to weigh whether the potential protections to data privacy outweigh the impacts to businesses.

[1] www.techradar.com/news/what-is-gdpr-everything-you-need-to-know
[2] www.npr.org/2018/10/08/654893289/why-the-tech-industry-wants-federal-control-over-data-privacy-laws
[3] https://threatpost.com/what-will-gdprs-impact-be-on-u-s-consumer-privacy/132137/
[4] https://www.inc.com/associated-press/google-twitter-facebook-gdpr-privacy-policy-effects.html
[5] www.techradar.com/news/what-is-gdpr-everything-you-need-to-know
[6] Ibid.
[7] www.cnet.com/news/us-privacy-law-is-on-the-horizon-heres-how-tech-companies-want-to-shape-it/
[8] www.techradar.com/news/what-is-gdpr-everything-you-need-to-know
[9] www.cnet.com/news/us-privacy-law-is-on-the-horizon-heres-how-tech-companies-want-to-shape-it/
[10] http://fortune.com/2019/02/21/technology-companies-federal-data-privacy-law/

Protecting Kids Online: A Guide

Keeping kids safe on the internet is an ongoing challenge for parents. It has been reported that one in five children who use the use internet have been sexually solicited; that 25% of children have seen unwanted pornography; and that nearly 60% of teens have received an email or instant message from a stranger, of which nearly half replied.[1]

There are also a host of other concerns associated with your children having open access to the internet. Cyberbullying, which is the systematic infliction of psychological distress through the use of technology, is one of the most prevalent and persistent online threat to children today.[2] It's also difficult to know who you are really talking to online, which makes it difficult for children, especially, to make judgements about the safety of their interactions.[3] Children can also easily access inappropriate sites with a few clicks of the mouse.

In April 2000, the U.S. federal government enacted the Children's Online Privacy Act (COPPA), which helps to protect the personal data of children younger than the age of 13 when they are online. The act requires websites to explain their privacy policies and prohibits requiring more personal information than necessary from a child, such as date of birth, social security number, or home address. The law was put in place to protect children's sensitive information and prevent it from falling into the wrong hands.[4] Many websites, in an effort to forgo dealing with the special rules concerning children, prohibit people under the age of 13 from signing up for services or creating accounts (both things that would require the collection of personal data). Parents can find a site's child privacy policy in the privacy statement located in either a dedicated privacy page or the "About" page for the site.

Below are some tips to help protect your children when they are on the internet:

- Create rules for internet use in the home.
- Keep an open, honest, and trusting relationship with your child so that they can approach you with any concerns or experiences.

- Regularly check the internet history of internet-capable devices to see which sites your child has visited.
- Know all of your child's email accounts, screen names, and which social networking sites they are a part of.
- Discuss the dangers of the internet with your child, and keep an open line of communication with them so they can comfortably report their experiences.
- Install filtering/monitoring software to block certain websites.
- Install antivirus or tracking software on your child's cell phone. Smart phones are computers, and the same issues that can affect a desktop can also strike a phone.
- Monitor the types of video games that your children play. Remember that any game that allows for multiple players will also allow for communication between players.

For additional information on how to effectively implement these tips, please visit the Florida Department of Law Enforcement's Secure Florida webpage at http://www.secureflorida.org/.

Aside from these tips to ensure your child's safety, it is also important to identify warning signs that may indicate your child is involved in unsafe internet practices. Spending long hours online, attempting to obscure the content on the screen, becoming emotional or depressed after spending time online, and withdrawing from family or friends are all indications that something might be wrong.[5]

Monitoring children's online activity is no easy task given the speed at whitch technology changes, but one key thing to remember is that you are the parent and you set the rules regarding your child's internet usage.

[1] https://www.sentrypc.com/home/statistics.html
[2] http://www.secureflorida.org/social_networking/cyberbullying/
[3] https://childdevelopmentinfo.com/family-living/kids-media-safety/children-teens-web-internet-safety/#.XGLeBFxKiUk
[4] https://kidshealth.org/en/parents/net-safety.html
[5] https://www.childrens.com/health-wellness/internet-safety-for-kids-and-teens

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.

A DNS hijacking wave is targeting companies at an almost unprecedented scale

https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale/

- Attackers manipulate the Domain Name System records that allow computers to find a company's computers on the internet. They replace the IP address for a legitimate site with a malicious address that allows them to harvest credentials or launch malware attacks.
- DNS records were changed after login credentials were compromised for the administration panel of the target's DNS provider.

Analyst Note: While all of your passwords should be lengthy, complex, and strong, some passwords are more important than others. The DNS controls how people looking for your site are routed to it, so the password to such sensitive data should be created with high security in mind.

Robocall scams surge to 85 billion globally

https://www.zdnet.com/article/robocall-scams-surge-to-85-billion-globally/

- Spam calls grew 325% from 2017, with an estimated 12 billion calls per month globally.
- UK, Spain, Italy, France, and Argentina were the countries with the most calls. In the U.S., the most impacted regions were area codes in Texas, Orlando, Atlanta, and Birmingham.
- Bank account scams were the most common scam, followed by extortion and kidnapping, and credit card scams.

Analyst Note: With these calls on the rise, it's more important than ever to be able to spot scams and social engineering. If you ever doubt the authenticity of the call, hang up and call the entity (bank, IRS, law enforcement) that is possibly being spoofed.

Nest Hack Leaves Homeowner Sleepless in Chicago

https://www.darkreading.com/attacks-breaches/nest-hack-leaves-homeowner-sleepless-in-chicago/d/d-id/1333779

- A family's home automation devices were breached by unknown threat actors. The perpetrators spoke through the microphones in the devices directly to the family members and set the thermostat temperature really high.
- The breach occurred due to duplicated passwords stolen from other online sites. The owner was not aware that two factor authentication was available for the devices.

Analyst Note: Home automation devices make life easier and centralize control over features in one place, but they are subject to the same rules as computers. Unique passwords are best, and it's always a good idea to enact multifactor authentication wherever you can.

Hundreds of Thousands of Medtronic Defibrillators Could Be Vulnerable to Hacking Due to Flaw

https://gizmodo.com/hundreds-of-thousands-of-medtronic-defibrillators-could-1833481773

- Some devices contain a flaw that could be exploited by someone with knowledge of the devices in close proximity to a patient who has one. The vulnerability would allow an attacker to intercept and impact the functionality of certain models of defibrillators and monitoring devices.
- No incidents have been reported and a fix is in progress.

Analyst Note: With advancing technology, the quality of healthcare is also improving. The security around these devices is also paramount. Should you have one of these impacted devices, contact your doctor or the manufacturer for further instructions.

Google and Facebook scammed out of $123M by man posing as hardware vendor

https://www.tripwire.com/state-of-security/featured/google-and-facebook-scammed-out-of-123-million-by-man-posing-as-hardware-vendor/

- A Lithuanian man plead guilty after wiring over $100 million to his personal bank account after posing as a computer hardware vendor that supplied equipment to data centers. He registered his company name identically to a well-known vendor. The man faces up to 30 years in prison.
- The scam is considered a Business Email Compromise (BEC), as the man impersonated invoices from a legitimate company doing business with the targets.

Analyst Note: Social engineering campaigns can deceive even large companies with tight security. Always verify to whom you are sending a payment and that goods and services have actually been rendered for invoices.

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):

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

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.

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

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

THE BEACON

Editing by: Ashley Grover
Designed by: Maria Olivella

April 2019

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

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