Summary

**Municipalities For Ransom** - A look at the recent spate of government entities being struck by crippling ransomware and what can be done to better strengthen networks.

**SWAT Are You Thinking?** - SWATting may sometimes be intended as a practical joke, but it has serious consequences. See how authorities have handled recent cases.

**Staying Clean With Good Password Hygiene** - Why do we still use weak passwords? Our suggestions for strengthening your password posture and better protecting your sensitive information.

**H₂Oh No! The Current State of Phishing** - Phishing remains a threat to cybersecurity. We examine the current state of phishing and how you and your organization can combat the threat.

**Did My Dog Just Dox Me?** - Posting pictures of your pets on social media is a good way to share your furry family members with the world, but could you also be sharing more information than you intended?

**Power Trip: Critical Infrastructure’s SCADA Problem** - What is SCADA? We take a look at the computer systems that make the whole world run and the threats that could impact them.

About The Beacon

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

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

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

This addresses the DHS Standing Information Need HSEC-SIN-1 and FDLE SIN-1
Cybersecurity Awareness Month 2019

October is National Cybersecurity Awareness Month and even though we should all be focusing on cybersecurity every day, it’s a great time to do a check up on our cyber hygiene. This year’s theme is Own IT. Secure IT. Protect IT. It’s an initiative to promote personal accountability and proactive behavior, digital privacy, security best practices, common cyber threats, and cybersecurity careers. Let’s look at how you can play a part in securing your digital information:

- **Stay safe on social media:** Be careful what you share and only add people you know as friends.
- **Update privacy settings:** Make sure you aren’t sharing with a larger audience than you intend to.
- **Keep tabs on your apps:** Delete old or unused apps and review app permissions.

- **Shake up your passwords:** Commit to making longer, more complex, more secure passwords.
- **Use multifactor authentication:** Enable this setting where you can to add another layer of security to your accounts.
- **Safe online shopping:** Only shop on sites with HTTPS protection and use a credit card for purchases to protect from fraud.
- **Spot a Phish:** Learn the indicators of a fake email and don’t fall for this common cyber social engineering tactic.

- **If you connect, you must protect:** keep your device operating and security software updated.
- **Stay protected while connected:** Password protect your home Wi-Fi, and if you must use public Wi-Fi, use a VPN service.
- **If you collect it, protect it:** If your organization collects customer data, secure that information.

The changing season gives us a great opportunity to see what outdated security habits we can change. For more information on cybersecurity, tips on how to get involved in securing cyberspace, and cybersecurity resources, visit the National Cyber Security Alliance at https://staysafeonline.org/.

**BONUS!**
Hidden somewhere in this issue of the Beacon is a Halloween Cyber Ghost! See if you can find it!
Cyber Threats

Municipalities For Ransom

Although cybersecurity is constantly evolving with the increase of global technological infrastructure, cybercriminals are working just as quickly to evade these measures with ransomware attacks against vulnerable systems. Ransomware is a tool used by cybercriminals that infects computers and networks, restricting users' access to their files or destroying critical information unless a ransom is paid. In the past, ransomware primarily affected individuals, however, recent reporting suggests there has been a dramatic increase of attacks within state and government networks, specifically targeting schools, libraries, and small local governments. In the first half of 2019, there were more than 70 ransomware attacks reported in the United States. Of those 70, at least 50 targeted city governments and of those cities, at least 25 had between 15,000 and 50,000 residents. This increase in attacks is most likely the result of the wealth of data contained on these networks and a limited budget for cybersecurity staff for some city governments. Traditionally, ransomware occurs after a user clicks on a link in an infected email; however, recently there has been a trend in “drive by” ransomware which occurs when a user visits an infected site, clicks on a compromised ad on a legitimate webpage, or by exploiting 0-day vulnerabilities in applications. Infection can also occur through social media distribution and instant messaging apps.

With a growing list of ways to compromise systems, training and antivirus software is very important. Always be sure to keep software and hardware up to date on security patches and implement cybersecurity awareness training to teach users how to spot social engineering schemes. The best protection against ransomware is to keep good backups of your files, separated from your network, that can be accessed if the worst happens. A network disabled by ransomware may result in school closures, loss of access to government websites, and the compromising of potentially sensitive information.
When demanding money, cybercriminals usually require the ransom be paid in cryptocurrency, such as Bitcoin, because of the difficulty in identifying the identity of the cybercriminal. At times, the loss of public services, in both time and revenue, far outweighs the cost of rebuilding or recovering a network. This leads some entities to opt for paying the ransom. Recently, 22 cities in Texas were impacted by a coordinated ransomware attack, but have refused to pay the ransom and intend to rebuild their networks.\(^5\) A private cybersecurity firm estimates the amount paid to ransomware attacks in 2019 will be close to $11.5 billion globally.\(^6\)

Because cybercriminal actors are often located overseas, it can be difficult to catch those responsible for ransomware attacks.\(^7\) For this reason, it is important for cities to insure proper protection from the dangers of ransomware through security measures. As ransomware and other cybercrimes continue to increase, maintaining proper cybersecurity posture will continue to be an important factor in local governments, where one weak link can result in many different and expensive consequences.

---

Swatting is not a new phenomenon. Between 2002 and 2006, a group of five serial swatters targeted people using online telephone party chat lines, impacting over 100 victims and costing emergency responders $250,000. The victims were chosen at random and the perpetrators were mainly motivated by bragging rights. In more recent years, swatting has become more targeted. Various celebrities, including Justin Bieber, Kim Kardashian, and Tom Cruise, were swatted in 2013. Beginning around 2014, several content creators on the online video game streaming service, “Twitch”, were swatted while livestreaming, which broadcasted swatting confrontations to global audiences.

Though always dangerous, it turned lethal in December 2017 when a well-known swatter in online gaming communities was asked to swat someone because of a feud between gamers. The swatter was provided with the home address of an intended victim in Wichita, Kansas. According to law enforcement, the victim was not actually involved in the online dispute. The swatter called Wichita police, pretending to be the victim, and claimed that he killed his father and was holding the rest of his family hostage. Law enforcement arrived at the residence, where the victim was shot and killed. Afterwards, the swatter was arrested and sentenced to 20 years in prison for making a false report resulting in death in addition to false reports from other swatting calls. This tragic
incident hasn’t deterred further swattings in the gaming community. In 2018 and 2019, several activists were swatted, including at least one in Florida. Some of these activists suspected that their swatings were politically motivated.

Preventing swatting attempts is difficult. The time-sensitive nature of most threats made during swatting calls gives first responders little time to verify if such threats are accurate. Technologies like ID-spoofing can make threatening calls even more convincing. However, some cities have created mitigation strategies that can lessen the potential impact of swatting attempts. Seattle Police Department’s “Rave Facility” platform, based on the national SMART 911 registry, allows Seattle residents to designate themselves as potential swatting targets. If a critical incident is called in at a registered address, responding officers will be notified and the registering individual will be contacted, lessening the chances for hostile confrontation between police and victims. Law enforcement agencies are also looking to deter these hoax crimes with stiff penalties, including heavy fines and possible incarceration if a perpetrator is found guilty. Recent cases illustrate that law enforcement views swatting as more than a practical joke. With the increase in swatting cases, law enforcement agencies may continue looking to find additional solutions to prevent potential tragedy.

2 Ibid.
5 https://mashable.com/2017/12/29/swatting-death-andrew-finch/#t0Kja3zhEsqr
8 https://www.yahoo.com/lifestyle/fortnite-champ-swatted-while-streaming-015435042.html
9 https://www.wired.com/story/how-to-stop-swatting-before-it-happens-seattle/
10 https://www.seattle.gov/police/need-help/swatting

Staying Clean With Good Password Hygiene

Life is full of things to remember, and passwords are no exception. It is estimated that Americans have roughly 200 accounts that require some sort of password, and the number of passwords that each person has to maintain will likely increase in the coming years. A major problem associated with having so many passwords is that people end up using weak ones in an effort to remember them all. Some examples of weak passwords used by millions of users are “123456,” “qwerty,” and “Password,” these passwords may be easy for you to remember, but they are also extremely easy for bad actors to crack. Many people tend to be creatures of habit and may use the same password for years and across multiple accounts. Additionally, some people believe that the information their passwords are protecting is not valuable, so they are more lax with security posture.

Weak passwords open you and your place of employment to vulnerabilities that could put sensitive information at risk. It is estimated that one out of five American consumers has experienced online account compromise from having a weak password and that approximately 81% of confirmed data breaches were caused by weak passwords. Poor password hygiene can
also make you more vulnerable to theft of personal identifying information, identity theft, compromise of financial accounts, or other personal accounts being negatively impacted. For example, if your social media password and username are compromised, a hacker could impersonate you and damage your reputation. If you reused that social media password at your place of employment or on another site, a bad actor may be able to gain access to those other accounts. Some reporting indicates that as of January 2019, a dataset of nearly 2.2 billion stolen emails and passwords has resurfaced online; the lists contain a massive amount of data that could be negatively used by criminals. Although the information contained in the dataset was not the result of a new breach, it could pose a threat if you haven’t changed your password recently. Overall, a weak password is the easiest gateway for cyber attackers to exploit you and/or your organization.

Unfortunately, many systems and organizations still have lax password complexity stipulations, which don’t do much to encourage users to upgrade their password creation habits. Many still allow for common, and/or simple passwords and some will allow very short passwords with no complexity. It falls to users to make sure that their passwords are complex and secure. Practicing good password hygiene is a necessity in the digital age and gives you an opportunity to take your security into your own hands.

In order to help prevent compromise of your passwords, here are a handful of tips:

» Use passwords that are at least 15 characters long
» Craft passwords that contain a mix of numbers, symbols, upper case and lower case letters
» Ensure you use a different password for each account
» Regularly change your passwords to something unique each and every time
» Never reuse passwords
» If offered, use multifactor authentication
» Do not share your passwords with anyone

H₂ Oh No! The Current State of Phishing

Phishing attacks have been around for a long time, and each year, more and more individuals become victims of a phishing attack. One in every 100 emails that are sent is an attempt to deliver malware, spear-phish, or commit fraud. Although there is more discussion and awareness...

3 https://www.forbes.com/sites/kateoflahertyuk/2018/12/14/these-are-the-top-20-worst-passwords-of-2018/#50ddfd82a4541
5 https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
6 https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
8 http://secureflorida.org/staying_safe/strong_passwords/
concerning phishing, these attack rates continue to increase annually. According to a global survey conducted by a private cybersecurity firm, 83% of respondents said they had experienced phishing attacks in 2018, an increase from 76% in 2017.2

Until 2019, most attacks targeted financial information looking for credit card numbers or banking information. Now, instead of impersonating banks, many of these attacks impersonate Software-as-a-Service providers, like Office 365 or Dropbox. SaaS is a service model that allows users to purchase a use agreement for specific software, usually through an ongoing subscription, that is delivered and maintained through an internet connection. Reports of accounts whose SaaS credentials have been compromised have increased by 70% since 2017 and 280% since 2016.3 Customers of the largest tech companies are often attractive targets and phishing emails that spoof official correspondence from these companies have been observed attempting to solicit information.4

Emails are not the only way you can receive phishing attacks. Communication applications, such as Skype and Facebook Messenger, have been used as yet another way for cybercriminals to attack. Malicious links and messages from impersonated accounts are sent with the same intentions as through email, and many non-email platforms do not have the same built-in security measures as an email that scan links and detect malware. Users may be less aware of the potential vulnerabilities of these applications and are more likely to click on these files and links.5

Fortunately, awareness and information about phishing attacks is all over the internet. Government agencies, cyber blogs, and news agencies provide information about phishing attacks, trends, and tips on how to spot them. There are even online quizzes you can take to see if you can easily spot a phishing email.6 Surprisingly, “cyber-savvy” millennials, who play a significant role in today’s global workforce, are reported to be less cautious of cybersecurity fundamentals. In a global survey, baby boomers (ages 54+) had a greater fundamental understanding of phishing and ransomware terminology than the other age groups.7 This might be due to millennials being more comfortable with technology and letting their guard down while older generations tend to be more discerning when they encounter something unfamiliar on the internet.

As vulnerable demographics are becoming more educated on phishing attacks, cybercriminals continue to enhance their delivery
methods. HTTPS, a secure version of HTTP (the protocol used to send information over the internet), was a way to detect if a website we were about to click on was safe. Any website, especially those that require login credentials, should be using HTTPS. However, according to a survey, 50% of phishing sites now use HTTPS, an estimated 900% increase since 2016. This means that using HTTPS as a way to gauge whether a site is reputable may not be so useful anymore.

We should always pay attention to what we are receiving and from whom we’re receiving it. Users can activate multifactor authentication to add an extra layer of security to their accounts, and strong passwords are always recommended. Phishing isn’t likely to go away any time soon, and as bad actors continue to update their tactics, it falls to everyday users to remain vigilant and be careful with what they click.

Did My Dog Just Dox Me?

Doxing, the publishing of private or identifying information about someone with possible malicious intent, can be a difficult attack to defend against. Nowadays, with how easy it is to share information about ourselves online, we sometimes paint a target for bad actors to aim at. The more you post about yourself, the more information you may be providing to someone who may mean to do you harm. While there is a growing awareness of the potential dangers associated with sharing personal information online, information still gets through the cracks. You’d be surprised what information can be gleaned in apparently innocuous posts, including a picture of your pet. You wouldn’t think a bad actor could learn much about you from a picture of your pet beyond, maybe, a preference for a specific type of animal friend. However, most pets wear collars and, on their collars, tags with some of your contact information. This information can be vital in the event your pet is separated from you; if someone with good intentions finds them, the tag

---

6 https://phishingquiz.withgoogle.com/
8 https://www.cloudflare.com/learning/ssl/what-is-https/
provides contact information that may help your pet get home safely. However, if you post a picture of your pet, you may unintentionally share your name, phone number, and/or address with the world.

Even just one of those pieces of information can be misused if it falls into the hands of a bad actor, and this information can be used to gather further pieces to build a surprisingly robust profile of a person.

On its own, a phone number could lead to something as relatively minor as an increase in robocalls or prank calls to your number. In more severe cases, it could play a part in a SIM card swapping attack (a type of scam in which a threat actor uses social engineering to convince a mobile carrier to port a phone number to the actor’s phone). In combination with other pieces of information that may have been posted online or collected elsewhere, a bad actor may have everything they need to steal your identity entirely or locate where you live and places you frequent.

Other clues can be gleaned from small details in the pictures you share online. Tagging the dog park you go to every week or leaving personal items in the background of your pet pictures can give viewers clues as to your habits, location, or personal information. Likewise, posting photos that display valuable or expensive things you own (your pets included) could motivate someone to figure out where you live and come try to steal things from you.

Being aware of what you post in your photos and your privacy settings could be your best defense against getting doxed. The next time you want to post a picture of that memorable moment you managed to snap of your pet, take a minute and block out anything you can see on their tags. You don’t have to stop sharing pictures of your furry friends, but taking the extra time to make sure you’re not accidentally oversharing can help keep you that much safer.

1 https://www.lexico.com/en/definition/dox
3 Ibid.
Clean water, electricity, communications, mass transit, and manufacturing are some of the many industries industrialized nations depend upon for continued operations. Millions of people use these services every day without much thought about the technology necessary to operate them. A key component of continued operations for many of these industries is Supervisory Control and Data Acquisition (SCADA) technology. SCADA systems are industrial control systems that allow for automated supervision, control, and analysis of industrial processes. With the right security measures in place, these systems help industrial operations run efficiently, providing clean water and reliable energy for millions of people. However, SCADA systems that lack the proper security measures could be exploited in cyber-attacks with potentially severe consequences.\(^1\)

SCADA systems gather real-time data from field controllers, such as programmable logic controllers (PLCs) or remote terminal units (RTUs), which oversee industrial functions. The data is then presented to human operators using a graphical user interface, which shows information in a way that is easier to understand and analyze. Users can then adjust controls using the same software. SCADA systems also store data in order to track and analyze industrial processes over time.\(^2\)

Critical infrastructure networks are increasingly targeted by cyber actors seeking to disrupt vital services. Because so many critical infrastructure components depend on SCADA networks, the compromise of these systems could cause disruptions in the availability of necessary resources.

- In June 2010, Stuxnet malware infected the industrial control systems (ICS) and SCADA systems of the Natanz nuclear facility in Iran. Stuxnet’s main purpose was to damage centrifuges used in the uranium enrichment process in order to delay Iran’s nuclear program. The malware operated by first exploiting zero-day vulnerabilities within the nuclear facilities networks to gain access to computers connected to PLCs involved in
the uranium enrichment process. Once the PLCs were infected, the malware altered the PLC programming, causing over 1,000 centrifuges to operate over capacity, which damaged the equipment.3 4

- In December 2015, suspected Russian cyber-operatives remotely accessed three Ukrainian electricity control centers, gained control of the SCADA systems, and opened breakers at approximately 30 distribution substations. This attack resulted in over 200,000 customers losing electricity.5 The malware used in this attack, BlackEnergy, was specifically designed to target ICS and SCADA networks.6

Developing and implementing protective measures against critical infrastructure cyber threats is key to preventing disruptions to necessary services. Many infiltrations into SCADA networks begin with exploiting vulnerabilities within human-machine interfaces (HMIs) which are often installed on network-enabled locations. HMIs installed on air-gapped networks may be better isolated and less vulnerable to infiltration.7 Additionally, many SCADA and ICS systems utilize remote access; securing these connections by using multi-factor authentication, firewalls, or virtual private networks (VPNs) may also help prevent intrusion.8 Having a disaster recovery plan is essential in the aftermath of a SCADA attack. Cyber-attacks are not usually known for having human casualties, but SCADA and ICS control various processes that can either be harmful to humans (such as toxic chemical controls) or essential to human health (for example, powering life support). SCADA may not be the first thing that comes to mind when we talk about cybersecurity, but compromise of these systems can have far-reaching effects.

Editor's Note: In the July 2019 issue of The Beacon, we talked about Triton, another strain of SCADA/ICS malware that can have far-reaching impact. Triton affected the controls that kept chemical gas from being leaked, which could have resulted in human casualties.

1 https://www.forcepoint.com/cyber-edu/scada-security
2 https://www.youtube.com/watch?v=5voF5mloLo
4 https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/
6 https://blog.cdw.com/security/attacks-on-scada-systems-highlight-the-need-for-effective-cybersecurity
Cybersecurity officials warn state and local agencies (again) to fend off ransomware


- Multiple states have reported sophisticated ransomware attacks that have impacted government services.
- Some state and local government agencies may still be running Server Message Block (SMB) version 1, which has several vulnerabilities that Microsoft patched more than 2 years ago.

Analyst Note: Always keep up to date on manufacturer security and firmware patches. A lot of the malware infections seen after a patch is issued are due to lagging patch implementation.

Leapfrog Children’s Tablet Owners Should Remove Pet Chat Now


- Several vulnerabilities in an app on a children’s tablet would allow actors locate children, interact with them, or phish parents for sensitive information.
- The tablets do not use HTTPS encryption, putting sensitive data at risk of exposure.
- The app has been removed from the Leapfrog store but may be present on devices that are older than 3 years. The app will have to be manually uninstalled from most older tablets.

Analyst Note: Children's learning devices are still computers and can have vulnerabilities that can put children at risk. Stay up to date not only on what apps your kids are using, but security updates for those apps, as well as the physical devices the apps are installed on.
Virginia State Police recoup $300K stolen in BEC scam


- The Virginia State Police were able to recover just over half of $600,000 that was stolen from Spotsylvania County in a business email compromise.
- Threat actors sent a fake invoice two weeks prior requesting payment for a new turf field installed at a local high school. No arrests have been made.

Analyst Note: Business email compromise remains a threat, not only to businesses but government entities as well. Learning how to spot social engineering schemes remains the best way to avoid losses to these and other scams.

Block newly registered domains to reduce security threats in your organization


- More than 70% of newly registered domains are “malicious,” “suspicious,” or “not safe for work.”
- Blocking domains that are under 1 month old could be a measure that increases cybersecurity.

Analyst Note: Threat actors sometimes register new domains (a process that is simple and doesn’t take long) in order to facilitate malicious cyber campaigns. If an organization sees a lot of suspicious traffic to or from a newly created domain, blocking them as a rule could help improve their security posture.

Two charged with tech-support scamming the elderly for $10m


- Two crooks stole over $10 million from 7,500 victims. Most of the victims were elderly and located in the US and Canada.
- The threat actors tricked the victims into believing their computers were filled with malware so that the victims would pay for unneeded computer repair services.

Analyst Note: This is a classic tech support scam. Keep in mind that large tech support companies will never contact you directly about malware on your devices. If you receive one of these calls, hang up. If you're concerned about something being wrong with your computer, call the company directly on a number you’ve verified.
What is TLP?

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

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

www.SecureFlorida.org/The_Beacon

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

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

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

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

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