Summary

As If Ransomware Needed an Upgrade... - Ransomware groups are upgrading their tactics to deploy more effective attacks. We take a look at some of the most recent changes.

Coronavirus Cons - Cybercriminals are taking advantage of the COVID-19 pandemic to exploit people. Find out how you can protect yourself.

COVID-19 and the Tech Supply Chain - COVID-19 has tested the tech supply chain. We examine the impacts.

Learning Curve: Adopting to Fully-Online Learning - A look at some of the challenges of adapting to a new learning environment.

Teleworking Does Not Mean Forgetting About Cybersecurity - Teleworking can present a number of cybersecurity challenges. We’ve provided some tips for staying secure at home.

People Don’t Lie on the Internet... Do They? - Misinformation and disinformation can sometimes be tough to spot. Find out how to separate fact from fiction.

Time for a Check Up: Evaluating Cyber Threats and How they Impact the Healthcare Industry - We discuss some of the threats facing this sector and provide strategies for shoring defenses.

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
Prevent the Spread

Over the past few months, we’ve all done our part to help in preventing the spread of the COVID-19 virus through a variety of efforts including practicing social distancing, frequently washing hands, and cleaning and disinfecting surfaces. Although these measures help in protecting us from viral infections, they don’t do much to protect our computers – and cyber criminals don’t seem to be taking any sick days! Analysts at Secure Florida want to ensure that you also do your part in preventing the spread of malware by boosting your computer’s immune system with a few easy steps.

**Use firewalls and antivirus software**

Firewalls help protect your computer by blocking unauthorized users and information from coming into contact with your network. Antivirus software backs up your firewall by fighting any malware that manages to get into your network.

**Stay up-to-date on patches**

As vulnerabilities are found in your software or operating system, patches will be issued to address them. Failing to install these patches in a timely manner can leave your device open to cyber criminals who try to exploit these vulnerabilities.

**Think before you click**

Cyber criminals hope that you’ll absentmindedly click on links and open attachments. Links may take you to a website where hackers can harvest your personal information and malicious email attachments, even those that at first appear to be legitimate, often contain malware. Hover your cursor over links to double-check their destination, and have your anti-virus scan attachments before opening them to check for malware.

**Practice good password hygiene**

Avoid reusing passwords. Use a strong password with a combination of letters, numbers, and special characters to prevent hackers from cracking it and gaining access to your accounts or devices.

**Be wary when using public Wi-Fi**

Public Wi-Fi, especially those that don’t require authentication, may not have optimal security measures in place to protect your browsing data. Information transmitted over these networks, including usernames, passwords, and emails, may be visible to others. Using a virtual private network (VPN) can help by encrypting your internet connection.

It is important to remember that, in both our response to COVID-19 and cyber-attacks, preparedness is key! Taking the proper precautions early can help in preventing challenges later. The steps mentioned above will help you protect others by first protecting yourself and your devices.
Cyber Threats

As If Ransomware Needed an Upgrade...

For years, cyber criminals have generally followed the same basic attack methodology when deploying ransomware. They would infect a victim’s systems with ransomware, encrypt their files, and demand a ransom payment in order for the organizations to gain access to the encrypted files. This methodology has been fairly successful in eliciting funds from organizations. In fact, 2019 was one of the worst years for ransomware attacks. There was a reported increase in attacks on state and local government agencies, and global damages from ransomware attacks were estimated to be approximately $11.5 billion.¹

By the end of 2019, some ransomware groups had altered their usual methodology to increase the effectiveness of their ransomware attacks. In December 2019, the City of Pensacola experienced a Maze ransomware attack which disrupted many city operations including phone service, email, and online bill payment. In the attack, information on the city’s computer networks was exfiltrated before the networks were encrypted. The Maze ransomware group then threatened to release the data if the city refused to pay the ransom. A few weeks after the attack, and after the city refused to pay the ransom, the Maze group posted 2GB of the exfiltrated data on a publicly accessible website.²

Although data theft and ransomware are commonplace in the cyber world as separate acts, this incident was one of the first ransomware attacks in which significant amounts of data stolen from a victim was published publicly to encourage ransom payment. A similar incident occurred in May 2019, when a ransomware operator posted screenshots of data stolen from a Baltimore City server. It’s likely that ransomware attackers increasingly encountered victims who had adequate file backups and could therefore choose to not pay ransoms to obtain decryption keys. In these instances, the ransomers were left without payment. This method increases the leverage that ransomers have by threatening the information security and reputation of organizations. Even organizations that may have their files backed up may want to avoid the public exposure of employee or customer information. The Pensacola incident serves as a grim indicator of what could become the new norm in ransomware attacks. Since the incident, many other ransomware groups have agreed to adopt the same data exfiltration methods to increase their leverage and encourage targeted organizations to pay up.³
Cyber criminals are determined and will continue to adapt their ransomware tactics to increase their chances for a payout. Organizations and government agencies can protect themselves by continuing to follow cybersecurity standards including maintaining up to date antivirus and software patches, keeping file backups stored securely and separate from your network, and continuing to train employees on recognizing social engineering schemes.

2 https://arstechnica.com/information-technology/2019/12/pensacola-city-government-was-hit-by-maze-ransom3

Coronavirus Cons

Cyber criminals remain as opportunistic as ever and continue to look for new ways to exploit individuals for financial gain or to cause disruption. While the COVID-19 pandemic impacts the U.S., cyber criminals will likely continue to look for ways to use scams related to the pandemic to prey on others for financial gain.

People may be more likely to fall victim to malicious scams and tricks initiated by cyber criminals when distracted or under stress.1 Cyber criminals may attempt to take advantage of this by recycling old tricks and scams that were effective in the past. For example, phishing emails may be deployed claiming to be from legitimate health-related or governmental organizations with information related to COVID-19 that contain malicious attachments. Additionally, fraudulent websites and mass text messages claiming to be from legitimate sources may be used to cause panic or to solicit money.2

In March 2020, the U.S. Department of Health and Human Services experienced a cyberattack that was meant to cause disruption and disinformation during the COVID-19 pandemic. The distributed denial of service (DDOS) attack overloaded the department’s servers for several hours.3

In March 2020, a malicious site was discovered which claimed to be hosted by Johns Hopkins University and
which featured a live map of purported COVID-19 global cases. The site mimicked the layout and features of the legitimate Johns Hopkins COVID-19 map but contained malware designed to steal user’s information when visiting the site using the AZORult trojan.\textsuperscript{4,5}

Cybercriminals are likely to continue to seek opportunistic methods to deploy malware, exploit individuals, and cause disruption. They will likely continue to use previously successful social engineering tactics including phishing messages, fraudulent websites, and network disruption or intrusion attacks. A few tips to avoid these tactics include:

1. **Beware of requests for personal information or money**: Research organizations or charities seeking money in relation to COVID-19 to ensure they are legitimate.

2. **Verify email addresses or links**: Inspect links by hovering your mouse over URLs to reveal the link’s destination. Do not open attachments or click links from unverified sources.

3. **Be mindful of “urgent” phone calls or emails**: Social engineering messages often create a sense of urgency or demand to initiate a quick and irrational response from victims. Verify suspicious calls or emails before interacting with caller or senders.

4. **Report scams**: If you believe you’ve seen or been a victim of a scam, report it to law enforcement.\textsuperscript{6,7}

5. **Stay informed via trusted sources**: For the most up-to-date information on COVID-19, visit the Center for Disease Control and Prevention website and review guidance from your local county and state health departments.

\textsuperscript{4} AZORult is a trojan stealer that collects various data on infected computers and sends it to the C&C server, including browser history, login credentials, cookies, files from folders as specified by the command and control server.

\textsuperscript{5} \url{www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/}
\textsuperscript{7} \url{www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response}
\textsuperscript{4} \url{www.krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/}
\textsuperscript{5} \url{securelist.com/azorult-analysis-history/89922/}
\textsuperscript{6} \url{www.who.int/about/communications/cyber-security}
\textsuperscript{7} \url{us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html}
Cyber Highlights

COVID-19 and the Tech Supply Chain

COVID-19 has impacted many of the behind-the-scenes areas of everyday life that many of us take for granted - including the tech industry’s supply chain. COVID-19 began spreading globally from China - one of the top producers of technological items and the source of most of the tech industry’s labor in the world. China’s manufacturing sector was hit hard by factory closures leading to a 13.5% drop in the country’s industrial output for January and February 2020 – a record downfall. This continues to pose a challenge to both consumers and producers seeking ways to continue maintaining normalcy despite the virus. Many U.S. companies have faced challenges in manufacturing their products due to restrictions put on suppliers in cities further up the supply chain. Some companies have been forced to stop manufacturing altogether until conditions are safer. One company reported in late March that they were experiencing significant fluctuations in the flow of electronics from its producers in Asia. Some experts are expecting to see companies moving to a complete reorganization of supply chains during this time. These setbacks all add up to products not being debuted on time and a lot of revenue being lost as a result.

As many tech companies and their supply chain components adjust to an uncertain future, many have chosen to take this opportunity to assist in combatting the virus’ spread by contributing their resources. These efforts include producing N95 masks, manufacturing hands-free door openers and ventilators, and deploying robots to hospitals hit hard by the pandemic to transport equipment and supplies. These efforts can help in meeting the demand for necessary equipment and services but can also present cybersecurity challenges for manufacturers if proper cyber hygiene measures aren’t followed. As companies alter equipment to meet different requirements, the introduction of new processes, authentication measures, and third-party entities could present companies with new vulnerabilities. Malicious cyber actors will likely view these shifts in operations as opportune times to target companies as they adjust to new circumstances. In the tech supply chain, cyber actors are likely to target information technology and operational technology systems with unpatched vulnerabilities that
Learning Curve: Adapting to Fully-Online Learning

In some communities, the transition from traditional to distance learning environments has meant making some changes. Some have started providing students with paper handouts and assignments, while others have implemented video conferencing platforms such as Zoom and Vidyo to host live lectures and are using learning management systems such as Google Classroom and Canvas for assignments and exams. Despite the technical difficulties, uncertainties, and

In an effort to limit the spread of COVID-19, many schools across the country have closed and have transitioned from a traditional classroom environment to distance learning.

1 https://www.ft.com/content/318ae26c-6733-11ea-800d-da70c66e4d3
10 https://www.cisa.gov/insights
12 https://foreignpolicy.com/2020/03/04/blindsided-on-the-supply-side/
challenges, students are excited to get online, see their classmates and teachers, and most importantly they are eager to learn.3 4 For students who are increasing the amount of time spent online, it is important to implement strategies for safe and effective online learning.

Some communication platforms used by schools to hold online classes have raised a number of security concerns. Recently, Zoom, the video conferencing platform, faced safety and privacy concerns after several incidents in which hackers wrote offensive comments, or posted pornographic or racist images during Zoom meetings. Law enforcement agencies are encouraging schools to make their Zoom meetings private and set strong passwords for participants.5 As educational institutions adjust to using third-party entities for classes, parents may want to use this time as an opportunity to discuss the importance of using strong passwords, setting privacy controls for online accounts, and learning how to react to questionable or dangerous content online.

A public service announcement released by the FBI highlights the potential challenges some educational systems may face if students who may not be as well-versed in cybersecurity are thrust into a fully online learning environment.6 Maintaining an open line of communication with children can help parents educate them about online safety and remain aware of what programs and online platforms their children are using.7 8 Spending time browsing the internet with children can help parents have an idea of what their child does online and who they interact with. Additionally, parents can establish rules about online activity by setting times for internet use, designating apps and games that children are allowed to use, and installing parental control software to block unwanted content.9

The internet can be an invaluable resource for children - providing access to knowledge and entertainment, but it can also be dangerous for those who aren't knowledgeable about online threats. As school districts continue to be targets of cyberattacks, keeping students, educators, and school staff aware of cyberthreats is important in helping to reduce the risk.

---

2 https://appleinsider.com/articles/20/03/16/what-to-expect-from-remote-learning-management-systems-during-the-coronavirus-outbreak
3 https://www.tampabay.com/news/education/2020/03/30/day-one-for-online-learning-in-tampa-bay-eager-students-slow-computers/
4 https://denver.cbslocal.com/2020/03/30/coronavirus-colorado-teachers-students-online/
7 https://www.reformaustin.org/lifestyle/keep-your-kids-safe-online-while-you-work-from-home/

---

**Teleworking Does Not Mean Forgetting About Cybersecurity**

As teleworking has become a more common practice, it is imperative to remain vigilant when it comes to physical and digital cyber security. Criminal cyber actors may take advantage of opportunities when many are teleworking at the same time to create disruptions, steal sensitive information, and compromise organizations' databases and/or servers. It is necessary to stay diligent and help ensure your organizations data and networks are secure at all times no
matter where you are working from.

Employers that allow people to work remotely are encouraged to have policies and procedures in place for teleworking. Some recommendations for these policies include not storing company material on non-approved devices (e.g. personal USB flash drives), ensuring security software and virus protection software is up-to-date, and utilizing multifactor authentication, if possible.

Employees should follow their company’s guidelines and general cybersecurity best practices when working from home. This includes:

- Only using work devices for work activities and avoiding the use of unauthorized devices for work purposes.
- Only using trusted websites to research and gather information.
- Only opening attachments from recognized sources. Avoid clicking on pop-ups, unknown emails, or links.
- Being aware of social engineering scams where scammers pose legitimate companies to obtain personal information, and taking steps to verify unusual requests.
- Only using secure and password-protected Wi-Fi connections or hotspots.
- Being conscientious in choosing a location to work so as to avoid others from seeing potentially sensitive or confidential information.
- Ensuring that your system’s updates are done consistently on your machines, and locking your device when stepping away.
- Being alert to where you leave your work phones, computers, etc. and ensuring these devices are not stored in places where they could be easily manipulated or stolen.

In addition to these guidelines, emphasis on strong password hygiene is essential. It is recommended that you have strong passwords (15 or more words/characters) that are unique to each account and that they are regularly updated. Additionally, avoid saving passwords to your machine and instead enter them each time you need to login to different locations. This helps lessen the likelihood of hackers stealing your passwords and using them to access unwanted data. It may be helpful when applying telework best practices, to keep in mind that if an action would not be appropriate at work, do not try it at home. Be prepared and cautious when teleworking and make sure to ask questions if you think something doesn't seem right. Being diligent is a necessity in order to limit compromises.

4. [https://www.zdnet.com/article/working-from-home-cybersecurity-tips-for-remote-workers/](https://www.zdnet.com/article/working-from-home-cybersecurity-tips-for-remote-workers/)
5. [https://www.secureflorida.org/SF/Online-Safety/Passwords](https://www.secureflorida.org/SF/Online-Safety/Passwords)
6. [https://www.comparitech.com/blog/information-security/security-remote-working/](https://www.comparitech.com/blog/information-security/security-remote-working/)
People Don’t Lie on the Internet…Do They?

With the ever-increasing popularity of social media and online communication, sharing information and ideas with people around the world has become an attainable reality to anyone with internet access and a phone or computer. However, as information sharing becomes easier, so does spreading misinformation. As the COVID-19 pandemic continues, people will continue to seek out the latest information and guidance for responding to the ever-changing situation. Because information shared during this time of uncertainty has the potential to impact the health and safety of many individuals, it is vital that people receive and share the most accurate information possible.

Misinformation is false, misleading, or inaccurate information.¹ Some instances of viral online misinformation may start as good faith misinterpretations of accurate sources that spread through online communities. For example, some individuals continue to spread misinformation relating to the origin of COVID-19 and unproven cures for the virus.² Although this information is likely spread with good intentions, inaccurate information spread during a time of uncertainty and fear can put lives at risk.

Other instances, called disinformation, are started deliberately with the objective of deceiving people.³ There are many reasons malicious actors of various scopes and alignments may want to spread disinformation. In the context of the COVID-19 pandemic, many criminal actors or adversarial nation states may seek to spread disinformation to support criminal acts, such as scams for financial gain or create confusion. Some individuals have even been known to commit illegal or violent acts based on conspiracy theories fueled by inaccurate information posted online.⁴ Like misinformation, disinformation may then be shared by people under the assumption that is accurate or truthful, further disseminating the dishonest messaging.

Misinformation can spread easily online and may even become more popular than information from accurate sources.⁵⁻⁶ For example, it was reported that some U.S.-based websites that posted misinformation about COVID-19 received 142 times the social media engagement as the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO).⁷

Misinformation and disinformation spread in a variety of ways. Academic research suggests that people are more likely to share online misinformation if it supports pre-existing beliefs and less likely to share misinformation if it contradicts pre-existing beliefs. People may also be less likely to verify and more likely to share misinformation that provokes a strong emotional response, such as outrage, shock, or fear.⁸⁻⁹ Additionally, some people spreading disinformation may impersonate or falsely cite official sources to trick their audience into trusting them. For example, recent widespread misinformation posts on social media falsely claimed that
organizations like the CDC and WHO advocated consuming garlic, sesame oil, or bleach to cure or prevent COVID-19. This information was not only inaccurate but, in some instances, had the potential for serious consequences.

Recognizing disinformation and misinformation online requires the viewer to consider several questions when viewing information online.

First, is it written in a way to appeal to cognitive biases? Is it overly skewed towards a certain perspective or written in a way to generate strong emotions like outrage, fear, or reassurance? These factors alone do not confirm misinformation, but may indicate a need to evaluate the information further.

Second, where is the information coming from? Is the original poster providing any citation or source for their claim? Is the source reliable, and are there multiple sources backing up the claim?

Third, is the poster representing the information from those sources accurately? If they are paraphrasing or quoting information from a trusted source, does it accurately reflect the content of the source?

If the answer to any of these questions is no, you may be looking at misinformation. Adopting a cautious mindset, understanding warning signs, and helping others be more mindful about the kinds of content they see and share online will help protect one's circle from falling for and sharing misinformation.

5. [https://www.ideals.illinois.edu/bitstream/handle/2142/47257/308_ready.pdf?sequence=2&isAllowed=y](https://www.ideals.illinois.edu/bitstream/handle/2142/47257/308_ready.pdf?sequence=2&isAllowed=y)
9. [https://www.ideals.illinois.edu/bitstream/handle/2142/47257/308_ready.pdf?sequence=2&isAllowed=y](https://www.ideals.illinois.edu/bitstream/handle/2142/47257/308_ready.pdf?sequence=2&isAllowed=y)
Critical Infrastructure

Time for a Check Up: Evaluating Cyber Threats and How They Impact the Healthcare Industry

Understanding the current cyber threat environment in the healthcare industry may now be as vital as ever as the public health sector works to combat COVID-19. Cyber threats in the healthcare industry can impact any healthcare entity from major hospitals to mom-and-pop pharmacies. Patient health data is among the most coveted types of data by hackers and they are always looking for ways to obtain it. In fact, more patient records were breached in the first half of 2019 than in all of 2018.1

There are several types of cyber threats that commonly impact the health care industry. The most prevalent include malware, ransomware, and phishing attacks.2 These threats can lead to security breaches and the unauthorized access of files containing personally identifiable information including full names, Social Security numbers, or even personal health information. The data, once accessed, can be sold for identity theft or insurance-fraud purposes. It can also be encrypted and used to extort money from an affected health entity.3 Between 2018 and 2019, the healthcare sector saw a 71% increase in data breaches.4 5 Healthcare data including prescriptions, insurance documents, and medical records with PII can be sold by cyber criminals on the dark web for anywhere from $3 to $500 per listing depending on the data set.6

Security breaches can be very costly to healthcare organizations. Globally, healthcare organizations pay an average mitigation cost of $6.45 million per incident, which is 65% higher than the costs seen in other industries.7 Some reports suggest that smaller healthcare organizations impacted by cyberattacks may even be forced to go out of business. In 2018, about 57% of medical practices in the U.S. had 10 physicians or fewer and about 15% were run by lone practitioners. Smaller organizations like these, may lack robust cybersecurity tools and may not have a dedicated cybersecurity specialist to monitor and patch their systems.8 However, no healthcare business, regardless of size, can afford the possibility of a security breach. After a cyber-attack, costly post-breach response resources are needed to address the incident. Additional costs may include HIPAA fines and reputational damage.9
There are some strategies that healthcare organizations can use to improve their cybersecurity measures. This may include conducting one of the many forms of cybersecurity evaluations. A network assessment, for example, can be conducted to review your IT infrastructure and identify risks that might arise from insecure network configurations or outdated software across traditional or wireless networks. Another form of cybersecurity evaluation is an advisory assessment, which evaluates infrastructure security from a higher level. This is more of a holistic view of your complete security program to analyze strategy, best practices, and gaps to address. Regardless of type, a cybersecurity evaluation can ultimately help redirect IT resources and focus on weak spots that, if breached, could be detrimental.10

Once a cybersecurity evaluation is complete, actions should be taken to address identified risks. A survey of healthcare organizations released at the end of 2018, found 95% of respondents who conducted an evaluation were able to identify ways to further enhance their security posture. Some of the actions listed included adopting new or improved security measures; drafting, revising, and/or testing policies and procedures; and conducting new or additional training of personnel. Only 5% of respondents indicated no additional actions were deemed necessary.

For healthcare, as in all industries, it is important to have the right IT tools, resources, and trained staff following the same guidelines. Furthermore, regularly evaluating your network and cybersecurity posture can help to protect organizations and their customers from ever-evolving cyber threats. However, simply evaluating your network is not enough to protect your organization. Revising, adopting, and testing new and improved policies/procedures based off these evaluations is essential to increasing your organization’s cybersecurity posture.11

---

1 https://healthtechmagazine.net/article/2020/01/why-all-health-care-businesses-need-cybersecurity-assessment
2 https://www.upguard.com/blog/cyber-threat
5 Ibid.
6 https://www.zdnet.com/article/this-is-how-hackers-make-money-from-your-stolen-medical-data/
10 Ibid.
Ransomware attacks vs Kimchuk, Visser reveal supply chain threat to DOD


- Attackers reportedly gained access to company payroll information and purchase orders from a customer’s nuclear division.
- The group behind the attack began posting files from the attack online in an effort to extort the manufacturer into paying the ransom.

Analyst Note: Government and military networks often contain highly sensitive information that, if published online, could have severe consequences. Cyber attacks stemming from trusted third-party entities can quickly become vulnerabilities if their network security isn’t sound.

Verizon: Attacks on Mobile Devices Rise

https://www.darkreading.com/mobile/verizon-attacks-on-mobile-devices-rise/d/d-id/1337136

- Mobile devices continue to be attacked by cyber criminals, according to a report compiling information from surveys and interviews with over 1,000 business and cyber security professionals.
- Roughly 40% of respondents to the survey reported that they experienced a mobile security compromise in 2019.
- 43% of respondents stated that they sacrificed mobile device security for a number of reasons including expediency and convenience.

Analyst Note: Many focus their cybersecurity efforts on desktop and laptop devices instead. However, given the vast amount of personal information stored on mobile devices, mobile device security deserves the same level of attention.
Malware and HTTPS - a growing love affair

- Although many assume that when websites use HTTPS, the website is “safe” and free of malware, this isn't the case.
- According to a study, HTTPS is likely being used in roughly one fourth of malware-related traffic.

Analyst Note: As most legitimate websites migrate over the HTTPS, so have cybercriminals. We can’t assume that just because a website uses HTTPS, it’s safe. Using firewalls and antivirus software will help in protecting your device should you stumble across a malware site.

Why fixing security vulnerabilities in medical devices, IoT is so hard

- Some medical IoT devices contain software that can be vulnerable to a range of cyber threats including remote control takeover, denial of service attacks, and information leaks.
- Patches and updates for these devices may be overlooked as these devices age and as the parties responsible for maintaining them change.

Analyst Note: IoT devices can make our lives easier, but it’s important to remember that these devices often have vulnerabilities like other computerized devices. As such, it’s necessary to ensure these devices are updated and patched at regular intervals to reduce risk.

US Govt Warns of Ransomware Attacks on Pipeline Operations

- The hackers were able to gain access to the operational technology (OT) network after first hacking into the information technology (IT) network via a spearphishing email.
- The attack resulted in the facility ceasing operations for two days until replace equipment could be implemented.

Analyst Note: Cyber criminals continue to attempt to gain access to OT networks supporting critical infrastructure. These individuals often attempt to gain access initially through the IT networks of these entities using common social engineering tactics in order to pivot and access the OT network.
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.