The Beacon

Florida Fusion Center #15-100 | Cyber and Critical Infrastructure Report | July 2015 Issue #7

Summary

All About Hacking — It's always in the news, but what does "hacking" really mean? This issue explores many of the topics related to this buzzword.

Medical Records: the Latest Data Breach Contraband — Medical data theft is the most lucrative category for identity theft. We discuss why that is and the steps you can take to protect your information.

Securing the Internet of Things — These days, so many things can connect to the Internet. Learn some of the ways to maximize the security of smart thermostats, baby monitors, and everything in between.

Hacking Happens — Not all hackers are created equal. We define the major categories and motivations of hackers to explain why you may be a target.

Florida Department of Education Cyber Attacks— In 2015, Florida's Department of Education's standardized testing weathered technical difficulties and a cyber attack. This article covers an issue that will be on the rise as schools shift to paperless testing.

Hacker Tools: ION Cannon — A tool to test website security, the ION cannon is also a weapon used by hackers for denial of service attacks. This provides an overview of how it works.

Contents

About *The Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness.

Secure Florida is an Internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC). The FIPC was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure protection analysts. FIPC analysts work to protect Florida's infrastructure through FDLE's Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

If you see a topic where you would like more detailed reporting, or have seen something you think we need to know about, Let Us Know.

We welcome your feedback.
www.surveymonkey.com/r/TheSFBeacon7

Contact SecureFlorida.org at:
(850) 410-7645
Admin@SecureFlorida.org

Editor's Corner

All About Hacking

Whether it's a large corporation, the government, or your local gas station, it seems that almost every day the media is reporting about this hack or that data breach. Pop culture puts the issue at the forefront as well, portraying normal citizens' personal information as at the mercy of crafty, masked individuals behind a set of computer screens. Unfortunately, data theft is a trend that probably will not be going away anytime soon. Since so many things about our lives are somehow connected to the Internet, odds are we all have been a victim of a hack (and if you haven't, you probably will be in the future).

Because hacking is at the forefront of cybersecurity concerns, we at the FIPC often field questions on the topic. Therefore, we have decided to dedicate this issue to hacking, attacking the topic from a variety of angles. Within this publication, you will find a wealth of information about the motivations, tools, and targets in the world of hacking. There is a variety of reasons that individuals would want to steal your information. Sometimes it can be personal; there is a spectrum in the hacking community, and different people fall in different categories based on their particular motivations.

We also discuss steps you can take to protect yourself, and your data. Today, so many details of our lives reside on the Internet—health records, financial information, employment applications, social media data, and more are all online, under varying levels of security. This can make it difficult to track and control the dissemination of that information, especially because this information can be breached both accidentally and through the actions of criminals. Proactive steps to assess what information is out there, and why someone would want to steal it, is a great way to minimize issues down the road if you experience data theft.

There is no guaranteed solution to prevent someone from getting your information. In 2014, nearly half of adults in the U.S. last year reported that they have been the victim of a hack. However, we hope that this issue addresses concerns and clarifies some misconceptions and myths behind who and why someone would steal your information.

Secure FLORIDA.org

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Cyber Highlights

Cyber Highlights represent issues cyber analysts have seen active in Florida. The following articles are intended to serve as overviews of issues we feel the citizens of Florida would benefit from knowing.

Contents

Medical Records: the Latest Data Breach Contraband

No one who follows the news would be surprised to learn that data breaches are on the rise in the U.S., both in frequency and in numbers of victims. Last year alone Staples, P.F. Chang's, Michael's, Sony, and even the State of New York were all victims, and it seemed that every week there was another announcement. However, it might shock you to learn that the fastest growing sector for the theft of such data is the healthcare industry.

The U.S. Department of Health and Human Services (HHS) is required by law to post a list of breaches of unsecured protected health information. So far this year, HHS lists 122 breaches—nearly one a day—affecting from 500 individuals to nearly 80 million (Anthem, Inc.).[1] What's noteworthy is that the top eight were all the result of hacking. And the top six were from hacking of data servers.

Why are medical records so attractive to thieves?

First of all, medical records often are not protected by robust security measures. "Hospitals have low security, so it's relatively easy for these hackers to get a large amount of personal data for medical fraud," stated Dave Kennedy, an expert on healthcare security and CEO of TrustedSEC.

In addition, medical records contain a wealth of saleable personal information: names, birth dates, policy numbers, diagnosis codes, and billing information. Using this information, not only can a thief file false insurance claims, they can also purchase equipment and prescriptions for resale on the black market. Stolen health credentials can go for $10 each, about 10 to 20 times the value of a U.S. credit card number.

How is medical record theft different from other types of identity theft?

When most of us hear "identity theft," we think of stolen credit cards. In recent years, financial institutions have made credit card theft nearly painless for consumers, but not so with the theft of medical records. There are several key differences, among them:[2]

1 U. S. Department of Health & Human Services. Breach Portal. 17 Jun 2015 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

2 Ponemon Institute, LLC. Fifth Annual Study on Medical Identity Theft. February 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

- Medical identity theft is costly to consumers. More than half the people in one Ponemon study had to pay an average of $13,500 simply to resolve the crime.
- Medical identity theft is complicated and time-consuming to resolve. Unlike credit card theft, often victims of health record theft are not told for months after the crime, by which time resolution is more difficult. HIPAA regulations, while providing privacy, also contribute to the complexity.
- Medical identity theft can have a negative impact on reputation. Victims often feel that the release of sensitive health information has led to the loss of career opportunities or even, in a small number of cases, current jobs.

How do I protect my medical records?

Unfortunately, there is no surefire way to protect your medical records from theft. Your only recourse is vigilance. The Federal Trade Commission offers some tips:[3]

- Be cautious of any "free" health services or products that need your health plan ID number.
- Never provide any health information over the phone unless you initiated the call and are sure of whom you are talking to.
- Keep all medical-related receipts and compare them to your bills.
- Correct any mistakes in your medical records. You have the legal right to review your records; contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and location where a thief may have used your information.
- You can also ask for the names of anyone who asked your medical provider for copies of your records (disclosures). By law, you can receive a free copy from each of your providers every 12 months.

3 Federal Trade Commission. Medical Identity Theft. August 2012. http://www.consumer.ftc.gov/articles/0171-medical-identity-theft

Securing the Internet of Things

The "Internet of Things" (IoT) refers to devices with Internet connectivity that allow the sending and receiving of data. IoT includes smartphones to baby monitors to house lights that can be turned on and off remotely. Even a toaster that can be controlled from miles away. The number of "things" connected to the Internet is already greater than the world population; by 2020, experts estimate there will be about 50 billion of these devices worldwide.[4]

Benefits

Although there are still no flying cars, the IoT reflects a massive shift in our daily routines. There are many benefits: Internet-connected thermostats can result in consumer savings and improved energy conservation; 'smart' medical devices can monitor, collect, and aggregate vitals to better treat patients; Internet connectivity in cars provides better road safety and convenience to drivers. The list of benefits is nearly endless, because the IoT is intended to make our lives easier and more efficient.

4 Cisco. How Many Internet Connections are in the World? Right. Now. 23 June 2013. http://blogs.cisco.com/news/cisco-connections-counter?_ga=1.47530535.1688981833.1434990076

SecureFLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org

Risks

While the benefits are numerous, we may not regard our "smart" toaster's security with the same level of scrutiny as we would a regular computer.[5] The biggest concern is the lack of security settings that sit on these devices. In addition, manufacturers may not provide automatic updates to fix security vulnerabilities, which could put your devices at risk if the software goes unpatched. And applications that work within smart devices may not properly implement encryption, which could compromise the security of information you transmit.[6] Depending on the type of app, this could include financial data or other personally identifiable information.

A search engine called Shodan finds Internet-connected devices:[7] everything from heating control systems, water treatment plants, traffic lights, video-conferencing devices, baby monitors, and countless other devices that have an IP address. If a device is not secured with a password, it is easy for someone to find, remotely connect to, and control it *(Editor's note: In Florida, it is a felony to intentionally access a network or network device you do not have explicit permission to access).*

Unsecured smart devices carry a spectrum of risks. Individuals might be able to access your thermostat and change the temperature a few degrees. This may not seem like a *huge* deal to you but it might be to a hospital. Or imagine if they gained control of your video-capable baby monitor to spy on you and your family. Hackers could locate and tamper with settings on an array of devices in a small geographical area as a diversionary tactic in order to accomplish something more serious.[8]

A separate risk is the degree to which you want companies to track your personal information. Smart TVs aggregate your viewing preferences, which is convenient when browsing for new movies. Other IoT devices retain much more personal information, however. For example, fitness trackers not only keep a record of the number of daily steps you take and let you brag about it on social media, but also may retain a wealth of other health information you may not wish to disclose.

So what can we do to protect ourselves, while still taking advantage of all the efficiencies the IoT offers?

- Keep a current list of the devices you own. Just because it doesn't have a keyboard or a screen, doesn't mean it can't be used as an attack vector.
- Evaluate the security settings on any device you purchase. Many devices can be used remotely. If you don't need that functionality, be sure to disable it. If you can protect the device with a password, be sure to select a strong one–don't use default factory passwords or easily guessed ones such as "password."
- Regularly check manufacturer websites for your smart devices to find out if there are software updates. If the manufacturer discovers a security vulnerability, they will often provide a patch for you to download.

5 Symantec. The Internet of Things: New Threats Emerge in a Connected World. 20 Jan 2014. http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world

6 Federal Trade Commission. Internet of Things: Privacy & Security in a Connected World. FTC.gov. January 2015

7 http://www.shodanhq.com/

8 PCMag. Can We Secure the Internet of Things? 23 Apr 2015 http://www.pcmag.com/article2/0,2817,2482620,00.asp

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Hacking Happens

Hacking happens. The news of late indicates as such, so we may as well admit it to ourselves. If it has not been hacked, it will be. So, what is there to say about the matter? Awareness. We all know about hacking, but there are nuances of the craft that are not as well known. Here, we would like to supply some information about the Who, What, and Why of the hacker world.

Who hacks?

Different groups hack for different reasons; as such, attribution of an incident is important to understanding why it happened. Popular culture dictates that a hacker is a teenager wearing a hoodie, hunched over a sticker-covered laptop. While sometimes true, it is more likely you would never recognize a hacker if you saw one. We have categorized the types of hacker as we have come to understand them.

Nation-State Sponsored Hackers

These hackers are employed by a military, government agency, or government contractor. They may work for any country willing to pay them. They are usually well paid, well trained, and well organized. Their job is to break into computer systems; they work in a highly secretive realm in the name of national security. They want your country's information more than they want yours, so they operate quietly with hopes of never being discovered. The longer they can maintain a backdoor into a computer system the better. *Primary motivation: Information*

Criminal Enterprise Hackers

Criminal organizations in many parts of the world have discovered that physically stealing money from a victim proves labor intensive and dangerous. The Internet, however, allows thieves to do their work with little physical risk. If they were to steal your wallet, they would likely get very little money and then still have to outrun you. But if they can use the Internet, they can literally have the world between them and you. This category of hacker also operates as quietly as possible: they get the data, sell it, and cash in quickly. *Primary motivation: Money*

Hacktivist

The noisiest of the hacker community is the hacktivist. They have a cause they are advocating for, and they use hacking techniques to disrupt, disclose, or generally cause a mess to publicize this cause. They may initially quietly gain access to a system, but then the gloves come off. Hacktivists might steal sensitive information in an effort to embarrass a person or organization. They might also attack a website to make it stop working or even destroy hardware to cause financial damage. *Primary motivation: Attention*

Script Kiddie

These are folks with the interest and time to hack things, but with no real monetary or ideological reason. They simply wish to hack. As such, their results vary. They could be good at what they do. Or, maybe even more troubling, their inexperience with a tool might inadvertently cause greater damage than they intended because they miscalculate the consequences of their actions. In May 2015, an Idaho high school student caused a denial of service attack against the school during state mandated computer-based tests. This student now faces a felony record and apparently did not assess the potential severity of the incident. *Primary motivation: Bragging rights*

Whatever goal a hacker has, one result remains the same. They cause problems--costly and often annoying problems. We can't stop hacking, but understanding why we are targets helps us better protect ourselves and respond to breaches.

SecureFLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org

Department of Education Cyber Attacks

Over the last several months, FDLE investigated two cyber incidents directed at the Florida Department of Education's (DOE) computerized testing program.

The first incident was observed on Monday, March 2, 2015, when Florida's 8th, 9th, and 10th grade students began taking the computer-based writing component of the English language arts Florida Standards Assessment. At the start of the two-week testing window, districts experienced a number of technical difficulties, including delays due to administrator log-in issues and students who were logged out of the test prior to completion.[1] DOE officials said testing provider American Institutes for Research's (AIR) computer servers began experiencing sporadic denial of service attacks as early as March 3, 2015 which prevented student access to tests over the course of several days.

Following DOE Commissioner Pam Stewart's directive to find the cause, AIR determined that a software update had caused the log-in and log-out issues. AIR has successfully retrieved many student responses, however they confirmed that the denial of service issues were the result of a cyber attack. FDLE has been working in conjunction with DOE and FBI counterparts to identify the responsible parties. Despite these issues, in the first week of the two week testing window, more than 60 percent of students who had registered to take the test were able to complete the computer-based component.

A second incident was brought to the attention of FDLE on Wednesday, May 13, 2015, when Florida DOE officials advised schools districts to suspend state end-of-course exams in civics, U.S. history, and biology. According to DOE spokesperson Cheryl Etters, "it was an attempt by an outside party to somehow shut down the system." The system was back up within about two hours.[2]

Computer-based testing is a great way to minimize paper consumption and increase the speed of processing thousands of students' scores. However, there are still vulnerabilities which, if exploited, can cause major issues such as those experienced by Florida this year.

1 Florida Department of Education. FDLE Investigating Cyber-Attacks Against FSA Testing System. March 2015. Web. <http://fldoe.org/newsroom/latest-news/2010319-fdle-investigating-cyber-attacks-against-fsa-testing-system-.stml>.

2 Solochek, Jeffrey. Tampa Bay Times. 18 May 2015. Web. <http://www.tampabay.com/blogs/gradebook/florida-eoc-testing-delays-caused-by-outside-cyber-attack-again-officials/2230128>.

Hacker Tools: ION Cannon

Many tools used by bad guys to hack and cause problems for websites are the same ones that the good guys use to make sure those same sites are protected. One such tool is the ION Cannon, which comes in two flavors: Low and High. ION Cannons are used by penetration testers to test the resiliency of websites against Denial-of-Service (DoS) attacks. They are also used by hackers and hacktivists to bring down targeted websites using the same DoS attacks.

With a DoS attack, an individual connected to the Internet will try to flood a server hosting a website with fake TCP/UDP or HTTP requests. When multiple individuals participate simultaneously, it is called a Distributed Denial of Service (DDoS) attack. Best case, the attack will cause the site to become temporarily less responsive; worst case, the site will be overwhelmed and go offline--sometimes for days, depending on the length of the attack. While some hackers initiate this type of attack with their own "home grown" coded tools, others use freely available tools such as the Low Orbit ION Cannon (LOIC) or the High Orbit ION Cannon (HOIC).

When the LOIC first came on the scene it was the weapon of choice of the hacktivist collective Anonymous. While not the only tool used, Anonymous requested that others download it and join them in the attacks because it was easy to use and free to download. The LOIC is TCP/UDP focused in its attacks. It's simple: enter the URL of the target, choose an attack method, and hit "IMMA CHARGIN MAH LAZER." That's it.

The HOIC is similar to the LOIC, but instead of being TCP/UDP focused, it floods the site with HTTP requests to bring it down. Whereas the LOIC can only target one site at a time, the HOIC can flood multiple websites at once. The real difference that HOIC has over LOIC is its use of what it calls "Booster Scripts" which allow HOIC users to implement some anti-DDoS randomization countermeasures, making it appear that the attack is coming from a number of different users, as well as increasing the magnitude of the attack.

As with many of the tools used by hackers and hacktivist groups, the same tools are used by the people who work to protect the networks and servers that store and process the data entities hold near and dear. Tools like the LOIC and HOIC will continue to evolve, allowing the good guys to see how vulnerable they really are.

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

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.**

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

Contents

The USAF found and flattened an ISIL base because of selfies

http://www.engadget.com/2015/06/03/the-usaf-found-and-flattened-an-isil-base-because-of-selfies/

- The U.S. military regularly monitors ISIL-controlled media accounts for intelligence.
- A selfie taken outside a headquarters building was posted on one of these accounts.
- U.S. military intelligence units were able to use that photo to determine the coordinate locations of the building.

Analyst Note: In the past, we have emphasized how much information can be wrapped up in your social media posts. This is an extreme example that shows how easy it is for someone to pinpoint personal data about you based on what seems to be a harmless photograph.

Police can access phone location data without a warrant, US court rules

https://nakedsecurity.sophos.com/2015/05/07/police-can-access-phone-location-data-without-a-warrant-us-court-rules/

- In May, a federal appeals court reversed a decision that required law enforcement to obtain a warrant when seeking cell phone records from U.S. wireless carriers.
- The court ruled a compelling governmental interest in obtaining the records, and because they are property of the wireless carrier, do not fall under a citizen's right to privacy.
- Privacy advocates are expected to appeal to the U.S. Supreme Court.

Analyst Note: As the amount of information tracking everyone's movements accumulates, we can expect to see this sort of issue become a larger factor in legal cases. The good news is that the wealth of data can both convict the guilty as well as exonerate the innocent.

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Why Yes, That Creepy Icon *Is* Your Free Copy of Windows 10

http://gizmodo.com/why-yes-that-creepy-icon-is-your-free-copy-of-window-1708121347

- This summer, Microsoft is rolling out its new operating system, Windows 10
- Current users of Microsoft operating systems can reserve a free copy to automatically download to your computer when it gets released (probably July 2015)

Analyst Note: If you currently use Microsoft, you may have noticed a new Windows icon in your notification tray. This free upgrade is totally legitimate. The nice thing is that if you decide you don't like the new operating system, you can revert back to your current version.

The Dark Web As You Know It Is A Myth

http://www.wired.com/2015/06/dark-web-know-myth/

- The "dark web" is sites within the normal Internet not indexed by normal search engines. Access to these sites requires specialized software and encryption.
- Usually thought of as a marketplace for illegal activities, many of the things bought, sold or discussed can also be found on the 'normal' Internet as well.
- The dark web is actually a collection of sites of good, bad, and weird; it is quite a bit smaller than the normal web.

Analyst Note: This article discusses some of the misconceptions about what exactly the dark web is. Although illegal activity does take place on the dark web, it is not as illicit as it is often described. Much of the time, users of the dark web simply use it to take advantage of the privacy and censor-free environment.

Worker fired for disabling GPS app that tracked her 24 hours a day

http://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/

- All smartphones are equipped with GPS technology, which can be disabled at the user's discretion.
- Third party apps can also be downloaded to smartphones that allow others to track movements of the phone remotely (which was the case here).

Analyst Note: This article is a good reminder that as smartphone users, we may be giving away more information about our location than we realize. Even with personal devices, it is important to assess how much we need to broadcast locational data.

Help us improve *The Secure Florida Beacon*. Please take a moment to complete our survey.

www.surveymonkey.com/r/TheSFBeacon7

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org

Secure Florida's Best Practices for Office Information Security

1. Be suspicious of email links and attachments.

Emails designed to trick you into clicking links and downloading files come to inboxes daily. It is a practice called phishing and it's surprisingly effective. The easiest way for someone to get unauthorized access to your network is for you to give it to them. Never click on email links and never download attached files unless they are from trusted sources.

2. Use strong passwords and keep them private.

Your password is one part of the information security process that you control. Remember that you are protecting your accounts not only from someone trying to guess your password, but also from someone who steals password files to crack them. A strong password can take so much time to crack that it's not practical to keep trying.

3. Back up your files regularly.

That spinning plate on your hard drive is an accident waiting to happen, and Florida is the lightning capital of the country. Hard drive crashes, electrical surges, and operator errors lead to many lost files. So do stolen laptops. Make sure you have backups of your important files.

4. Be careful when using public WiFi.

When you connect to Public WiFi, or an "open network," anything you transmit can be seen by others. This includes usernames, passwords, account numbers, and confidential work information. Using a "secure" connection (such as HTTPS, SSL, or VPN) helps lessen the risk.

5. Use password protected screen savers.

It can take only a few minutes for a stranger—or even a coworker—to take advantage of a computer left idle.

6. Download only from approved sources.

As with email attachments, never download files from untrusted sources. Be especially suspicious of free software; it often has malicious software bundled with it.

7. Don't give out information to unverified individuals.

Social engineers try to fool you into giving out confidential information. Sometimes the information they ask for seems harmless, so their request doesn't raise any red flags. Before giving out any office-related information, be sure the person making the request is authorized to receive it.

8. Know and follow your organization's information security policies.

Your organization has its own security rules on matters such as using USB drives and personal devices on your work computer. Follow them carefully.

Information Resources

The Florida Infrastructure Protection Center (FIPC) was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure analysts who work to protect Florida's infrastructure through research, intelligence, and training.

The Dispatch

The *FIPC Dispatch* is compiled twice weekly by cyber intelligence analysts in the Florida Fusion Center. The content is intended as an informative compilation of current and open-source cyber news for the law enforcement, cyber intelligence, and information security communities.
To join the Dispatch mailing list, write to **FIPC@fdle.state.fl.us**

Secure Florida is an Internet safety and awareness outreach effort of the FIPC. Designed for the vast majority of computer users, Secure Florida covers all areas of computer, network, and communication security. The website **www.SecureFlorida.org** features articles and links on topics such as identity theft, social networking, strong passwords, email safety, and keeping kids safe online.
To sign up for alerts and other notices, visit **www.secureflorida.org/members/signup/**

The Beacon

The *Beacon* is published quarterly by Secure Florida to highlight cyber and critical infrastructure security information and awareness. With original articles, the *Beacon* seeks to provide privacy and security information to all Internet users.
To read issues of *The Beacon*, visit **www.secureflorida.org/news/the_beacon/**
To sign up for *The Beacon*, visit **www.secureflorida.org/members/signup/**

The CSAFE effort provides Internet safety presentations for organizations, clubs, schools, and businesses anywhere in Florida. For more information visit **www.secureflorida.org/c_safe**

Class Topics Include

- Best Practices for Internet Security
- Family Online Safety
- Combating Cyberbullying
- Online Safety for Seniors
- Identity Theft
- Mobile Communications
- Email Safety
- Internet Laws & Regulations