Summary

Like a Bad Penny - The Windows tech support scam is back

Ransomware Update - An update on advances in ransomware

PIN and Chip Basics - A look at the rising technology of chip cards and how it can affect you

Wearable Technology - We discuss how to safely use your wearable smart tech

Be Smart with SmartPay - Learn about SmartPay and how to use it safely

Malware as a Service - Learn how criminals have turned hacking into a business

Chemical Awareness - What you need to know about how proximity to chemical plants can affect you and your business

A Culture of Security - This article covers steps you can take to make security second nature

Basic File Formatting for Images - Everyone should know these basic file format tips

Contents

Summary 1

Editor’s Corner 2

Cyber Highlights 3

Like a Bad Penny
Ransomware Update
PIN and Chip Basics
Wearable Technology
Be Smart with SmartPay
Malware as a Service

Critical Infrastructure 12

Chemical Awareness

Guest Insight 14

A Culture of Security

Design 101 15

Basic File Formatting for Images

Dispatch Highlights 17

About The Secure Florida Beacon

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

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

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

Aware and Prepared: Tax Fraud

With Tax Day quickly approaching, we’d like to remind our readers about the scams and fraud that occur around this time of year. Criminals usually exploit citizens in two primary ways: either they pose as the IRS to extort money, or they steal citizens’ identities and use that information to fraudulently steal the victims’ tax refunds.

Tax-related identity theft occurs when someone steals your Social Security number (SSN) and files a fraudulent return. Often, taxpayers don’t even realize this theft has occurred until they try to file their taxes, only to be told by the IRS that a return has already been filed under their SSN. Sometimes, the IRS catches it and may send you a letter that they found a suspicious return under your SSN. Sometimes, the IRS catches it and may send you a letter that they found a suspicious return under your SSN. This call had all the hallmarks of a classic scam – the message was intentionally vague so you might think it really pertains to you; it also began by saying it was the “final notice,” a scare tactic to trick the taxpayer into quickly forking over money. It was also from a Washington, D.C. area code, to trick you into thinking it might really be from a government agency.

As a reminder, the IRS will never call with demands to make immediate payments to them. The IRS will also never request payment information over the phone, or threaten you with arrest for failure to provide them with that information. If you think you may have been the victim of a tax-related scam, you can file a complaint with the Federal Trade Commission at identitytheft.gov.

If you think your SSN has been compromised due to tax-related identity theft, the IRS recommends taking these steps:

- Respond immediately to any IRS notice (editor’s note: that will never be an email or threatening phone call!); call the number provided or go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return rejects because of a duplicate filing under your SSN or you are instructed to do so by the IRS.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.


Cyber Highlights

Like a Bad Penny: Windows Tech Support Scam is Back

Back in Issue #2 (March 2014), we told you about an apparent surge in Windows Tech Support scams. Over the past two months, there has been another surge, but with additional and alarming variations.

Briefly, the original scam worked like this: a user receives a phone call typically from a man with a foreign accent, claiming to be from Windows Technical Support, who is calling to alert the user that their computer has a problem. The caller offers to fix the problem and gives the user a series of instructions resulting in the caller now having remote access to the computer. (Sometimes the user is aware of this access, sometimes not.)

The variations we are seeing now frequently involve:

- Stealing banking credentials; one victim even reported having $5,000 taken out of his account while he was still on the phone with the scammer.
- Locking up the computer and demanding payment to unlock it.
- Requiring payment for the “service” provided, often calling every couple of months thereafter for additional service. One victim paid more than $3,500 for such calls, believing it was necessary.

This results in the scammer having not only your credit card information, but access to your computer and all of the personal and financial information there as well.

A number of the complaints have been about calls from the 239 area code (southwest Florida).

Things to Remember

- Microsoft (or Windows) will NEVER contact you—either by phone or through your computer or tablet—to tell you about problems with your computer. They simply don’t do that. EVER.
- Never call a number because a pop-up on your computer tells you there’s a problem.
- Never allow a stranger access to your computer, unless you initiated the call.
- Ditto with your credit card information.
- Always maintain current antivirus software and security updates.
Ransomware Update: Locky

Query any search engine for “online security threats of 2016” and, along with data breaches and nation-state espionage, you will find ransomware. Affecting individuals, businesses, and governments alike, ransomware has become one of our most serious threats…and worst fears.

Whether CryptoLocker, CryptoWall, or TeslaCrypt, most ransomware today is “cryptoviral,” in that it encrypts your files until you pay money to get them decrypted. Until that time, the files are lost to you, unless you have a good backup procedure. You can sometimes remove the ransomware itself, but your files will still be encrypted.

One new ransomware version has been especially prolific recently and shows signs of only increasing in significance—Locky. Although CryptoWall still dominates the market, security firm Fortinet research shows that Locky comprises about 16% of recent ransomware infections, and has far surpassed TeslaCrypt.1

Locky

- Locky emerged in February 2016; all affected files have a .locky extension appended to them.
- It targets more than 150 file types, including .gif, .jpg, .mp3, .pdf, .txt, and MS Office files.
- The ransom demands seem to vary from about .5 bitcoin to 1.0 bitcoin (roughly $215–$430).2
- Locky spreads using MS Office email attachments with embedded macros; social engineering entices users to enable Office macros to view the file.
- More than half of all infections are in the U.S.

Avoidance: Never enable macros in files from untrusted sources.

As always, keep regular backup files, apply your security patches, and be wary of email from untrusted sources.

2 https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

PIN and Chip Basics

How have chip cards changed security of credit cards?

CHIPS VS MAGNETIC STRIPS

- Contain chips that encrypt information into codes that change every transaction
- Costly and much harder to maliciously duplicate
- Inserted into a terminal at the beginning of a transaction and removed at the end
- Transaction times are slightly longer to allow the chip to create its codes
- Have magnetic strips that contain static data
- Inexpensive and easy to maliciously duplicate
- Swiped once at the end of a transaction
- Transactions are faster since the card only transmits the static information the magnetic strip contains

What does it mean for me?

Even though the U.S. has been slow to adopt this technology, mostly because of how expensive it will be to get new terminals and issue new cards, the bottom line is these new cards are more secure. Chip cards are so much harder and more expensive to clone than the magnetic strip cards we use now because the chip serves so many purposes during a transaction. The higher cost of production and longer transaction times are the price we pay for increased security. If you consider that a few extra seconds and spending a bit more in upfront costs would mean a drastic increase in the security of your money, it sure seems like an easy decision to adopt this technology.

Slowly but surely, the U.S. is starting to see that. Major card companies are now holding merchants responsible if fraudulent transactions happen on their watches when they could’ve been using chip cards but chose not to. Because of the lingering liability, many banks and credit card companies are making the switch, although most will still allow for magnetic strip usage. Eventually the magnetic strip will become as obsolete as the CD player, replaced by the MP3 player that is the chip card, but we’re not quite at that stage yet. There are still many places that don’t accept chip cards because they don’t have the appropriate terminals, so you shouldn’t go cutting up your magnetic strip cards just yet.
Internet could easily get your data. Especially if used in conjunction with other information such as date of birth, this source could be a gold mine for criminals.

Accurate and real-time location-based tracking from wearables is also useful for criminals or stalkers who could easily exploit this information. Social media or activity tracking data posted online indicating you are on vacation easily allows a criminal to break into your home, safe with the knowledge you won’t be there. Other malicious actors may use this information to embarrass or extort you – many wearables track every bodily function, including sleeping, toilet use, mood, and all kinds of physical activity. Would you be comfortable sharing all of that information with anyone? Probably not…but as more of this kind of data is transmitted from devices onto the Internet, it is more at risk of being exposed and exploited.

Data brokers and marketers are also extremely interested in the data collected with wearables, and they could get it legally. How? It comes down to the privacy policy of the fitness apps and wearables you use. While many have security and privacy policies designed to protect the user’s data, plenty of apps don’t have privacy policies at all. This is a classic case of “let the buyer beware,” because it is up to you to know and understand what data you may be releasing to the wide open Internet.

If you have a wearable or are looking to purchase one, there are still some ways to protect yourself:

- Give the device a name that isn’t your actual name.
- Assign your device, and any online accounts associated with it, strong passwords that are unique for each account.
- Adjust all privacy settings so that you’re not accidentally broadcasting too much information publicly.
- Read the privacy policy so you know what information is or is not being protected.

Be Smart With SmartPay

You may have seen the placards or devices at the checkout line advertising the ability to pay using Apple Pay, Samsung Pay, or Android Pay. These apps allow you to use your smartphone to store credit/debit card information to make an easier, more secure way to pay your bill. But what makes this method better than swiping a card or using a chip? We break down each of the types of SmartPay technology, and what you need to know about their security.

Android Pay

Android Pay spawned from Google’s original peer-to-peer payment service, Google Wallet. Many of the features of Android Pay streamlines features of Google Wallet, making it easier and simpler for the consumer to use.

So how does it work? Android Pay uses Near Field Communication (NFC) technology to allow your phone to communicate with the payment terminal. This is the same type of technology used for scanning barcodes. When it launched in 2015, 70% of Androids could use Android Pay.1 However, some older models may not be equipped with NFC technology, so be sure to verify yours is compatible with the app.

When you store a credit/debit card in Android Pay, it doesn’t actually store your card’s information. Instead, it validates the information you provide with the bank, and then creates a virtual credit card, which acts as a token for your real account information. This virtual card number changes every transaction, and is what is shared with the merchant at the time of the transaction. This prevents criminals from stealing and re-using your card’s information.

If your phone is ever lost or stolen, you can use Android’s device manager to wipe the phone remotely, so that a thief can’t use Apple Pay to fraudulently make purchases on your dime.

Apple Pay

Like Android Pay, Apple Pay uses NFC to communicate with point-of-sale systems. Apple Pay also replaces your actual credit/debit card information with a security code that is provided during the transaction in order to prevent fraud. This number is unique for each purchase to ensure security.

However, depending on which Apple device you use, there are other security measures in place as well. If you are using an iPhone (version 6 or later), Apple Pay employs two-factor authentication. When you hold your phone up to the reader, you will be prompted to provide your fingerprint on your iPhone screen to authenticate the purchase. If you use an Apple Watch, you enter a passcode (which stays active so long as you are wearing the watch) to verify the use of Apple Pay.

Like Android Pay, if you ever lose your Apple device, you can use the cloud backup service also allows you to remotely wipe your phone if it is lost or stolen.

Apple Pay is currently limited to more recent versions of iPhones and iPads, so be sure to verify your device is compatible.

Android Pay

<table>
<thead>
<tr>
<th>What devices support it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android phones with NFC and HCE support running KitKat OS (4.4) or higher</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does it support multi-factor authentication?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What payment methods are supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit &amp; debit cards, loyalty cards, gift cards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does it support purchases in other apps?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Android Pay(^1)</th>
<th>Apple Pay(^1)</th>
<th>Samsung Pay(^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android phones with NFC and HCE support running KitKat OS (4.4) or higher</td>
<td>Apple iPhone 6, 6S, 6 Plus, 65 and 65 Plus, Apple Watch, iPad Air 2, iPad Pro and iPad Mini 3 and 4</td>
<td>Samsung Galaxy S7, S7 Edge, S6 Edge, S6, S6 Edge+ Galaxy Note 5, S6, S6 Edge and Galaxy Note 5</td>
</tr>
<tr>
<td>No</td>
<td>Touch ID (fingerprint)</td>
<td>Touch ID (fingerprint) or PIN</td>
</tr>
<tr>
<td>Credit &amp; debit cards, loyalty cards, gift cards</td>
<td>Credit &amp; debit cards, loyalty cards</td>
<td>Credit &amp; debit cards</td>
</tr>
</tbody>
</table>

Apple Pay is currently limited to more recent versions of iPhones and iPads, so be sure to verify your device is compatible.

1 http://www.the verge.com/2015/12/28/9618687/google introduces android pay replace wallet app

Samsung Pay

Currently, Samsung Pay is more limited than Android Pay or Apple Pay, because right now it only works with higher-end Samsung devices (the Galaxy S7, S7 Edge, S6 Edge+, S6, S6 Edge and Galaxy Note 5). You must also have a Visa or MasterCard issued by Bank of America, Chase, Citibank, US Bank or Wells Fargo.

Samsung Pay is quite similar to the other two versions of smart pay. It uses NFC technology, but it also uses something called “Magnetic Secure Transmission” which allows you to use your phone as a payment method on standard credit card machines.2 This means that if a point-of-sale terminal has a standard magnetic strip card reader, you can swipe your phone as if it were a normal credit card, using Samsung Pay.

Like Apple Pay, Samsung Pay uses a secure element to store your card’s tokens on a chip embedded in the phone. It creates a 16-digit token to represent your credit/debit card, but also transmits a one-time code created by the phone’s encryption key. When you set up Samsung Pay, you are required to provide either a fingerprint or PIN. Purchases cannot be made without this authentication, which protects you from unauthorized purchases. Samsung’s “Find My Mobile” service also allows you to remotely wipe your phone if it is lost or stolen.

All three payment methods have many security features in place to protect the security of your money. The chart below compares some of the features of each smart pay technology, as well as the devices that support each application. No matter what type of payment method you decide to use, it is important to always keep an eye on your accounts to catch any fraudulent activity that does occur.

Android Pay

<table>
<thead>
<tr>
<th>What devices support it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android phones with NFC and HCE support running KitKat OS (4.4) or higher</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does it support multi-factor authentication?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What payment methods are supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit &amp; debit cards, loyalty cards, gift cards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does it support purchases in other apps?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

1 http://time.com/4068133/apple-samsung-android/  
2 https://www.android.com/pay/  
3 http://www.apple.com/apple-pay/  
4 http://www.samsung.com/us/samsung-pay/
Malware as a Service

Back in the day, we used to warn you about script kiddies: novice computer hackers who did not have the skills to create their own malicious software, so they downloaded it from obliging hacker sites. The goal of these hackers was often to harass, test network security, or prove their own skills. Or they may have simply wanted to brag to their hacker buddies. However, pretty much gone are the days of hacking to brag; hackers now want something more lucrative, usually money. The once haphazard assortment of computer criminals has evolved over the years into organized groups with promising business models. One such venture is Malware-as-a-Service (MaaS).

MaaS is a vast criminal underground market that allows hackers to gain access to build-it-yourself malware kits and hosted management services necessary for deploying malware across the Internet. The services often also supply 24/7 customer support, even hotlines for technical assistance. A variety of attacks are available, including phishing, spearphishing, and ransomware, at reasonable prices. A DDoS (distributed denial of service) attack, for example, can be contracted on the Dark Web at under $40 per hour.¹

These malware kits can be obtained for little cost by anyone, regardless of their knowledge or experience. Fees are generally paid in bitcoins—which themselves baffle attempts to identify their origin. And the ease of use, combined with the reasonable price, has made the venture extremely lucrative. One security firm has estimated that MaaS can yield a breathtaking 1,425% return on investment in just the first 30 days alone.


Note:
The Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address and elude law enforcement. However, they need special software and setup to use. These sites are not searchable by tools like Google and Bing. The Dark Web is frequently (though not exclusively) used for criminal purposes.

As with any market, rising demand and competition drive prices down. And as prices continue to fall and the number of malware services increases, the risk of becoming a victim is growing increasingly more severe. Not only do we have to be watchful of the numerous organized crime groups, but the minimum amount of professional knowledge required to enter the cybercrime arena opens the door to any number of "lone wolves" as well.

And the kits are not the only product. The Russian MaaS market particularly also provides users access to computer botnets, which are essentially networks of infected "zombie" computers that are infected with malware and can be ordered to perform any number of tasks. The cost can range from $35 to $270 for 1,000 zombies, depending on the country.²


One example:

In February 2016, Kaspersky Labs published their findings on the remote access trojan Adwind. This malware is distributed through a single MaaS platform, and between 2013 and 2016, has been seen in at least 443,000 private users, and commercial and noncommercial organizations around the world. Among its uses are the ability to:

- collect keystrokes
- steal cached passwords and grab data from web forms
- record video from a webcam and sound from a microphone
- transfer files
- steal VPN certificates

http://www.kaspersky.com/about/news/2016/Adwind

So what does all this mean to us as computer users?

It means that personal and enterprise security is more important than ever. The number of bad guys able to steal our money, our personal information, and our intellectual property has grown exponentially, and will only continue to do so. The most likely venues for malware today are phishing emails and social engineering. Computers users must become aware of the threats and how to combat them.

Prevent phishing:
http://www.phishing.org/scams/prevent-phishing/

Learn more about social engineering:
https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232
Critical Infrastructure

Chemical Awareness

Security directors of every critical infrastructure sector should be knowledgeable about the location and types of high-risk chemicals in proximity to their operations. Situational awareness of potential hazards associated with these chemicals is vital to comprehensive emergency response plans.

Background

The chemical sector is one of the sixteen sectors designated for critical infrastructure protection nationwide. Because of the likelihood of terrorist attacks against these chemicals, some companies in this sector are covered by the Federal Chemical Facility Anti-Terrorism Standards (CFATS) program which identifies and regulates high-risk chemicals at those facilities.1 Examples of failed threats directed toward high-risk chemicals at a facility include a plot by a domestic group to create an explosion at a ‘Texas natural gas’ processing facility causing the release of hydrogen sulfide gas and a plot in 1999 by two men to create explosions at a propane gas facility in California.2 Companies in other sectors that use or store large amounts of high-risk chemicals are also covered by CFATS. However, some facilities that have high-risk chemicals onsite are exempt from CFATS, including those regulated by the Maritime Transportation Safety Act, public water systems, water treatment facilities and facilities owned by the Departments of Defense and Energy.

Attack Incidents

A successful attack at a high-risk chemical facility occurred in June 2015. The targeted facility, located in France, was owned by a subsidiary of Air Products, Inc., a U.S. company with operations in 50 countries. A known driver for a delivery company gained access to the factory in his truck. Before he got there, the driver had lured his boss into the back of the truck, hit him over the head with a car jack, and strangled him. The driver decapitated his boss, and placed his head on the factory's fence in order to maximize publicity. He then rammed the truck into the gas cylinders, which triggered an explosion and injured two workers. When emergency response arrived, he was attempting to set off an additional explosion. The driver was detained, arrested, and charged as a terrorist.3

How to protect your facility

To develop situational awareness, the National Institute of Health U.S. National Library of Medicine has a publicly available online reference map of high-risk chemical locations.4 The map identifies companies that are regulated by the Environmental Protection Administration Toxic Release Inventory (TRI) program. Some of the chemicals in the TRI program are vulnerable to terrorist attack, while others (such as lead) are considered not vulnerable. Some companies are exempt from reporting, and some high-risk chemicals are not included.5

Another web-based tool is the Vulnerable Zone Indicator System managed by EPA. If you provide your facility location to the EPA, the EPA will provide an email if your location is in the zone of damage from a chemical accident at facilities that use certain hazardous substances.

These tools, as well as assistance from your Department of Homeland Security Regional Domestic Security Advisor,6 can aid security directors in developing situational awareness regarding the impact of high-risk chemicals to their organization.

1 https://www.dhs.gov/sites/default/files/publications/CFATS%20Update%20FS_May2014_508_0.pdf
2 https://www.fpiexec.org/readinglibrary/2001/Oct01/terror-attacks-listed-0kb-bomba-city-booming
3 http://www.cnn.com/1999/US/12/04/bomb.plot.02/index.html (c) PM US
4 http://toxmap.nlm.nih.gov/toxmap/flex/
5 http://www.csb.gov/west-fertilizer-explosion-and-fire/
6 http://www.dhs.gov/proactive-security-advisors
7 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4703955/
8 https://www.epa.gov/imp/forms/vulnerable-zone-indicator-system
Guest Insight

A Culture of Security

This article comes from the Florida Agency for State Technology (AST). AST was established in 2014 by the Florida Legislature to oversee the state’s essential technology projects and house Florida’s Chief Information Officer. AST is an inter-agency fusion liaison with the Florida Fusion Center.

One person can undo our entire security investment, and it may not even be intentional. Employees are an organization’s first line of defense against cyber-attack and data compromise. While focused on our organization’s mission, deadlines, and personnel matters, we must not ever forget about the sensitivity of data and information we work with daily.

Employees must not make bad choices about passwords, emails they send or websites they visit. Hackers will take advantage of any opportunity; they will employ techniques to trick unsuspecting employees into clicking on links in emails or divulging sensitive information on the phone. Employees must remain ever vigilant and aware of suspicious activity.

Vigilance does not end with the computers we use daily as cyber-attacks can have a physical element. A person taking photos or videos of areas and items that are typically not of interest to others (e.g., a doorway or parking lot) and “false” alarms could be the early stages of something dangerous.

Information security professionals work to protect information from many types of attack, but often the first line of defense rests with each employee of an organization.

Keep the following in mind:

- Always view links in emails with caution. Email is often the way computer hackers gain initial access into networks.
- Be alert to social engineering attempts. These attempts include phone calls where the caller asks probing questions with a sense of urgency to get you to divulge sensitive information on the phone.
- Take note of individuals photographing buildings the average person would not find interesting. For example, someone taking pictures of the Capitol, a monument, or fountains is not suspicious. However, someone taking pictures of parking lots, exit doors, utility equipment, or the outside of non-descript office buildings is suspicious.
- Your job may afford you knowledge of the location of infrastructure that is important to the State’s computing environment including the route of important communication cables, or critical utility facilities. Be alert and report suspicious activity around these locations.

Support the development of a culture of awareness in information security. When you see something, say something.

Design 101

Basic File Formatting for Images

As people who work with digital materials on a near day-to-day basis, it’s important that you understand images — because they aren’t simple, but they don’t have to be complicated. When it comes to digital images, it really isn’t enough to just say something like, “I need an image…” Images come in file formats and each one has its pros and cons.

Deciding which format fits your desired function will determine which format is right for your specific situation.

Most file formats differ in two main areas: compression and number of colors. Compression deals with how information is treated within the image. File formats have different algorithms that dictate how data in the image is treated. File types that are “lossy” use algorithms that sacrifice appearance for smaller file size while “lossless” file types retain more information, resulting in larger file sizes. Depending on how your image will be used, you may want the small file size or you may need the more accurate image.

The other difference in file formats is in the number of colors they will display. Some display only the bare minimum, black and white, and will therefore take up the least amount of digital space. Others can display up to 16 million colors (24-bit), reaching the limit of what the human eye can accurately distinguish. The image’s purpose should determine the number of colors that would be most efficient. The list of image file formats is extensive, but the following list contains the ones the everyday user would likely come into contact with:

JPEG (Joint Photographic Experts Group)

Pros: Loads quickly good for small and large file sizes, has a wide color-bit range
Cons: Lossy compression that compounds, doesn’t support transparency (see PNG)

Most images on the web are JPEGs. JPEG is a lossy format, but the resulting smaller file size make it the go-to format for the web since smaller files will load faster. For print, however, JPEGs are less than ideal since every time you save a JPEG, the image is re-compressed, eroding the image with each save.

TIFF (Tagged Image File Format)

Pros: Flexible, lossless compression, high quality
Cons: Not web-compatible, longer load times

TIFF is a highly flexible and lossless file format. TIFFs can be saved with a variety of compression algorithms and can display several color-bit amounts. Its major downside is that it cannot be displayed on the web, making it incompatible for online platforms but highly desirable for print.

Florida Infrastructure Protection Center (FIPC)

April 2016

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

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

Contact us:

Email: admin@secureflorida.org
Phone: (850) 410-7645
PNG (Portable Network Graphics)

**Pros:** Supports transparency, allows for most accurate viewing on the web, great for images with large areas of uniform color

**Cons:** Not always web-compatible, larger images take up very large amounts of space

PNG is another lossless file format, falling somewhere between JPEG and TIFF in terms of capabilities. It can display a variety of color-bit amounts and, its most notable trait, supports transparency. Transparency deals with pixels that are, simply put, invisible. As an example, the ball on the left is a JPEG, which does not support transparency, and the ball on the right is a PNG:

GIF (Graphics Interchange Format)

**Pros:** Supports animation, good for small images with fewer than 256 colors in uniform areas, also supports transparency

**Cons:** Very old format that hasn't been updated in a long time, not very good for anything other than small, simple images or animations

GIF is a somewhat outdated format, overshadowed by its replacement the PNG, but is still appropriate for small web graphics and animated graphics. It primarily displays a lower range of color despite its lossless compression, but can be effective for images with a limited color range.

For comparison's sake, here's the same image saved in each file format:

Got ransomware? What are your options?

https://nakedsecurity.sophos.com/2016/03/03/got-ransomware-what-are-your-options/

- If you find you or your organization have become victims of ransomware, there are a variety of ways to recover.
- Once you have resolved the ransomware, it is important to take proactive steps to back up data and protect systems from future infection.

Analyst note: Although this article lays out a variety of options to deal with ransomware, the best cure is engaging in good security practices to prevent infection in the first place.

Know your enemy: The most popular hacking methods

https://www.helpnetsecurity.com/2016/02/12/know-your-enemy-the-most-popular-hacking-methods/

- A survey conducted by security company Balabit surveyed experts on the greatest cyber threats to their organizations.
- Social engineering remains the highest threat to cyber security, followed by compromised accounts and web-based attacks.

Analyst note: By recognizing and understanding the greatest threats to you and your organization, you can be proactive in mitigating and responding to events, or even avoiding them altogether.
Trend Micro flaw could have allowed attacker to steal all your passwords


- Security researchers have discovered a flaw in an antivirus product that could allow hackers to steal passwords.
- This type of vulnerability has also been detected in multiple security companies’ antivirus software over the past several months.

Analyst note: Malicious actors are always on the lookout for new and better ways to compromise your systems. Always make sure your software is up to date to avoid making yourself vulnerable.

Xfinity’s security system flaws open houses to thieves

http://www.wired.com/2016/01/xfinitys-security-system-flaws-open-homes-to-thieves/

- Hackers have discovered ways to manipulate real-time text security systems into sending false information via a jamming system.
- This jamming prevents the home system from communicating if there has been a physical break-in, which may allow criminals to exploit this known vulnerability.

Analyst note: As technology continues to permeate more parts of our lives, it is important for consumers to remain aware that all types of smart devices can still be exploited for malicious purposes.

First known hacker-caused power outage signals troubling escalation


- A new strain of BlackEnergy malware led to the first known hacker-caused power outage, leaving thousands of homes in Ukraine without electricity.
- The group allegedly responsible, known as The Sandworm Team, has a history of targeting other governmental agencies.

Analyst note: This attack signals a potential increase by malicious actors in targeting critical infrastructure systems like electrical grids, and emphasizes the need to have good security controls in place.

Secure Florida’s Best Practices for Office Security

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

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

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

4 Be careful when using public Wi-Fi.
   When you connect to public Wi-Fi, or an “open network,” anything you transmit can be seen by others. This includes usernames, passwords, account numbers, and confidential work information. Using a “secure” connection (such as HTTPS, SSL, or VPN) helps lessen the risk.

5 Use password protected screen savers.
   It can only take a few minutes for someone to take advantage of a computer left idle.

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

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

8 Know and follow your organization’s information security policies.
   Your organization has its own security rules on matters such as using USB drives and personal devices on your work computer. Follow them carefully.
SecureFlorida is an Internet safety and awareness outreach effort of the FIPC. Designed for the majority of computer users, Secure Florida covers all areas of computer, network, and communication security.

To sign up for alerts and other notices, visit www.secureflorida.org/members/signup/

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

The Beacon is published quarterly by Secure Florida to highlight cyber and critical infrastructure security information and awareness. The Beacon seeks to provide privacy and security information to all Internet users.

To read issues of The Beacon, visit www.secureflorida.org/news/the_beacon/

To sign up for The Beacon, visit www.secureflorida.org/members/signup/

The FIPC Dispatch is compiled twice weekly by cyber intelligence analysts in the Florida Fusion Center. The content is intended as an informative compilation of current open-source cyber news for law enforcement, cyber intelligence, and information security communities.

To join The Dispatch mailing list, write to FIPC@fdle.state.fl.us

The SAFE 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