The Beacon

Florida Fusion Center | Cyber and Critical Infrastructure Report | Mar 2014 Issue #2

Summary

The Secure Florida Beacon Intro — This is the second issue of *The "New" Secure Florida Beacon*. To which we say, "Hello world." We wanted to take an opportunity to introduce ourselves and say that we would like to get to know our readers. Help us out if you can by completing our survey.

Windows XP Support Ends April 8 — April 8 marks the day that Microsoft will end regular security updates for the nearly 13-year-old Windows XP operating system. This could spell trouble for the near 30% of computers that still use Windows XP.

Microsoft Tech Support Scam Activity in Florida — Florida Fusion Center cyber analysts recently received phone calls from citizens reporting solicitation from fraudulent Microsoft tech support personnel. This type of activity is not new, however recent citizen calls suggest a possible uptick in this activity in Florida.

The Internet of Things Can Create a Security Concern — Back in the day, computers connected to the Internet. Now whole hosts of devices connect to the Internet. This connectivity offers more selling points for new devices, but also poses a greater security threat for network administrators to consider.

The Physical side of Cyber Security, Focus: Energy Sector — The distribution of the power infrastructure across a vast geographic area creates a challenging landscape for grid operators, who must secure their assets against all plausible scenarios. The interconnected nature of the power grid means a physical security breach in one location could result in a disruption in others, ultimately affecting both physical and cyber assets system wide.

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. Secure Florida's mission is to protect the citizens and economy of Florida by safeguarding our information systems, reducing our vulnerability to cyber attacks, and increasing our responsiveness to any threat.

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/s/SFBeacon2

Contact SecureFlorida.org at:
(850) 410-7400
Admin@SecureFlorida.org

Editor's Corner

Intro and Survey Request

You are now reading the second issue of *The Secure Florida Beacon*. It may be obvious, by virtue of its content, what this publication hopes to achieve. However, we would like to take an opportunity to introduce ourselves.

The newly developed *Secure Florida Beacon* is an effort to inform Florida's citizens, businesses, and other organizations of the changing nature of the information security landscape.

The Secure Florida Beacon is new and we want to address the needs of our audience as best we can. As such, we need to know more about you. If you would, please take a moment to complete our survey. It will help us better plan the content of future issues.

Each *Secure Florida Beacon* will include a link to a survey that we always encourage our readers to use.

http://www.surveymonkey.com/s/SFBeacon2

In addition, we encourage our readers to contact us with questions or observations. You can always: **Let Us Know**.

Windows XP Support Ends April 8, 2014

Way back in December 2001, Microsoft released Windows XP. Since that time, XP has found its way onto computer systems all over the world. In fact, XP was considered such a reliable operating system that - at 12 years old, and followed by two other (three, if you count Vista [But, who counts Vista?]) Microsoft operating systems - Windows XP still maintains 30% market share.[1] Yes, as of this February, 30 out of 100 computers are still running XP. Microsoft, to their credit, is not mincing words: "Support for Windows XP will end on April 8, 2014. There will be no more security updates or technical support for the Windows XP operating system."[2]

Granted, computers running Windows XP will still work, but after April 8, Microsoft will not be patching the holes found by the hacker community. Depending on your situation, this can be a REALLY big deal. Easpecially alarming is the number of old XP machines performing business and mission critical functions.

Microsoft gave the information technology world plenty of warning, such that most large companies made security arrangements or have upgraded their systems. However, a chance remains that many home users and small businesses depend on older systems that have functioned very well for years. These computers, particularly in small business environments, may rarely see any direct human interaction. Others may be point-of-sale terminals—where operating system interactions are only assessable to administrators. The computer works just fine if it ain't broke, why fix it? How many of these XP computers are hiding in the dark recesses of your network?

Check to see if you have machine running Windows XP at home, work, or somewhere on your network. The numbers suggest there are a lot out there.

1 http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

2 http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

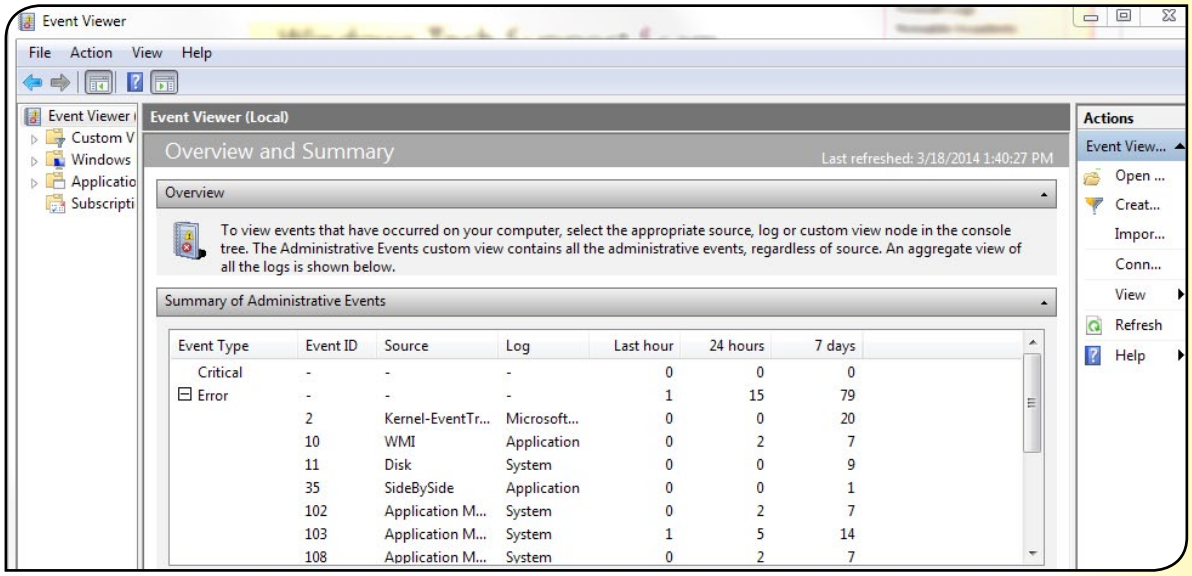
Citizen Issues

Florida Fusion Center cyber analysts regularly receive citizen concerns and complaints. These calls vary greatly, but here we present developing trends.

Windows Tech Support Scam

The Windows Tech Support scam has been around for a long time; however, the volume of recent reports we received suggests a possible uptick in the number of citizens receiving this solicitation in Florida. It should be noted that baseline levels of this activity are not known.

The scam works like this: a citizen receives a phone call typically from a man with an Indian accent. The caller claims to be from Windows Technical Support and is calling to alert the citizen that their computer is running slowly due to a virus or an outdated piece of software. The citizen is then given step-by-step instructions on how to access the Microsoft Event Viewer. Event Viewer is primarily a tool for system administrators to determine why a computer is not functioning properly. It logs all Microsoft error reports as well as warnings and important messages. The citizen is naturally alarmed when they see all of the "errors" listed there. The catch is this—even computers that are operating properly will have a long list of events logged here.



The caller then directs the citizen to type some "instructions" into the computer which result in the caller gaining remote control of the machine.[1] Once the caller is able to take control of the citizen's computer, they have access to personal information and all the files on that computer.

This scam is a classic example of **social engineering**.

1 **Several citizens reported being directed to download software from www.ammyy.com, a website that features remote desktop software. Ammyy is in no way affiliated with the scammers, and they have a prominent warning on their website to warn people against giving unknown people access to their computer.**

Contents

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

LET US KNOW:
(850) 410-7400
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

The Bitcoin Framework

Once known only to the users of the darker corners of the Internet, Bitcoin has seen a huge surge in publicity, acceptance, and in mainstream consciousness. Chances are you have heard of it, but do you have a firm grasp on what Bitcoin is? You should. Read on for the What, When, Who, Where, How, and Why of Bitcoin basics.

What is Bitcoin?

Is it money for geeks? Maybe.

Bitcoin is an open-source Internet-based peer-to-peer infrastructure for generating and transferring virtual currency. It includes the currency itself (bitcoins), the framework, and the system for creating, storing, and processing Bitcoin payments. In simple terms – it is digital money and the means to use it.

Specifically, a bitcoin is a virtual "crypto currency" used for Internet-based financial transactions. Mainstream media articles tend to show pictures of actual coins stamped with "Bitcoin" markings, serving to mislead casual observers. Although some physical coins have been created as a novelty, real bitcoins are 100% virtual and unlike minted coins, bitcoins have no real intrinsic value and are not legal tender. Unlike traditional financial institutions, the Bitcoin infrastructure is a decentralized, peer-to-peer network with no central point of control. Further, all transactions are recorded in a publicly available ledger known as the "Bitchain." This infrastructure makes Bitcoin ideal for anonymous transactions, difficult to tamper with, and unconducive to government regulation.

When did Bitcoin come into Existence?

Bitcoin has been around since 2009. The system is based on a conceptual paper published in 2008 by an anonymous author (or possibly group) using the pseudonym Satoshi Nakamoto. The Bitcoin community adopted the open-source software and works together to make and implement changes to the system's infrastructure. No single person or entity controls the system, making government regulation of the framework difficult.

Who creates bitcoins?

While it is not publicly known who originally created the Bitcoin framework, bitcoins are generated through a process known as "bitcoin mining" that can be undertaken by anyone. Bitcoin mining is the process of decrypting a very complex encryption algorithm. The process is so difficult that it is highly unlikely any one computer will successfully "crack" the encryption to unlock a Bitcoin block.

Miners generally join large pools—spreading the effort—in hopes that someone in the pool will be fortunate enough to crack the code. If so, everyone in the pool shares the resulting bitcoins. Currently, 25 bitcoins are awarded when the encryption algorithm is cracked. However, that number is designed to halve every 4 years until the year 2020, when it is predicted that all possible bitcoins will have been awarded.

Secure FLORIDA.org

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

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

Where are bitcoins located?

Bitcoin users maintain their holdings in a virtual Bitcoin "wallet." The wallet is little more than a program running on a personal computer or mobile phone used to make transactions on the Bitcoin network. Upon creating a new Bitcoin wallet, the new user becomes part of the Bitcoin framework. If a user's computer is lost or stolen, or the wallet's passphrase is forgotten, the associated bitcoins are not replaced; they simply become inactive on the network.

How does one acquire bitcoins?

There are four ways to obtain bitcoins.

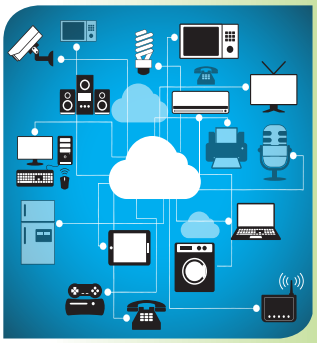
1. **Direct person-to-person transactions**, where bitcoins are transferred from one user directly to another, typically in exchange for goods or services. This could entail very small transaction fees or, in some cases, no fees, which is one of the primary benefits realized by the system.
2. **Purchase of bitcoins from a Bitcoin exchange**, an entity that holds bitcoins and "sells" them for different types of currencies like the US Dollar. This exchange method is generally favored by individuals purchasing bitcoins in bulk, on speculation that the market value will go up. The largest exchange, Mt. Gox, has been widely covered in the news after being "hacked" in February, causing the exchange to become insolvent and ultimately forcing the exchange into bankruptcy.
3. **Paying cash in a person-to-person exchange** to a local Bitcoin seller. Sellers are found using Internet forums and online classified sites like Craigslist. This type of hand-to-hand exchange is considered the most anonymous and is favored by individuals looking to maintain the highest level of privacy.
4. **Running your own Bitcoin mining software** or possibly joining a mining pool, in hopes you will be lucky enough to solve a Bitcoin encryption algorithm and be awarded bitcoins directly from the system.

Why do people use bitcoins?

Simply, because of the Bitcoin promise—secure cheap transactions with no central control. Ostensibly, the primary advantage of using bitcoin is their cheap transaction cost. Fees associated with Bitcoin use are substantially less than with a credit card or other traditional type of financial transaction. Additionally, the transactions are touted as secure due to the incredibly complex encryption that is used to create the bitcoins, which in turn protects Bitcoin from tampering, duplication, or theft. And, of course, users are drawn to the security provided by the anonymity of transactions.

It is certainly worth noting that these notions have been challenged in recent months as large scale theft of bitcoins have been disclosed by major Bitcoin exchanges, resulting in the loss of millions of dollars and significantly destabilizing an already volatile market. As popular as the virtual currency has become in recent months, its viability as a legitimate currency is currently in serious flux. Stay tuned.

The Internet of Things



The Internet of Things is the term given to non-traditional devices that are able to connect to the Internet, such as refrigerators, televisions, thermostats, cars, baby monitors, cameras, and security systems. The ability to access these devices over the Internet is both a selling point and a security concern.

The security concern is valid. As with a laptop, if a smart television with a forward-facing video camera and microphone became compromised, a malicious actor could remotely activate those components.

In January 2014, Proofpoint Inc., a security-as-a-service provider, reported they uncovered a possible "Internet of Things based cyberattack involving conventional household 'smart' appliances."[1] The report indicated that between December 2013 and January 2014 more than 750,000 phishing and spam emails originated from everyday consumer gadgets, such as compromised home-networking routers, connected multi-media centers, televisions, and at least one refrigerator.

1 www.proofpoint.com/about-us/press-release/01162014.php

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7400
Admin@SecureFlorida.org

According to the report, devices other than the conventional PC or mobile device, sent more than 25 percent of the emails.

We should point out that several security experts have criticized the accuracy of this report. Their concern focused on lack of evidence to prove that the malicious emails were in fact sent from the television or refrigerator rather than from a PC within the same network. The report did, however, show the capability of malicious actors to take advantage of vulnerabilities associated with most non-traditional Internet connected devices.

The number of non-traditional devices connected to the Internet is estimated to grow significantly in the next several years. In 2012, there were roughly 2.5 billion non-computer connected objects globally; by 2020, that number is likely to reach 12 billion.

The concept of the Internet of Things is not new. The combination of quick implementation of advanced technology and high demand for unconventional devices to be Internet connected creates numerous security concerns. It is important to address these concerns while the technology develops rather than as an after-thought.

In an effort to address this issue Cisco announced in February 2014, an *Internet of Things Security Grand Challenge*. Cisco challenged security experts worldwide to submit solutions to security challenges created by the emergence of the Internet of Things. Cisco will announce the winning solutions at the 2014 Internet of Things World Forum held on November 20, 2014 in London.

Considering Two-Factor Authentication

In the last issue of *The Secure Florida Beacon*, we briefly mentioned "two-factor authentication." We would like to expand that discussion in this issue.

With each major data breach (think "Target"), more passwords are identified, cracked, and published for use by the hacker community. In addition, the technology to process and ultimately crack passwords is getting faster and more efficient. The result is that users have to create different passwords that ultimately are longer and more complex. Passwords are becoming nearly impossible for people to manage but simpler for computers to crack.

Two-factor authentication is a process whereby access to a website, or other account, requires two separate forms of identification: usually a password and one other form.

Two-factor authentication generally requires that you supply two out of three authentication factors: a knowledge factor, a possession factor, and an inherence factor. In other words:

- Something only the user *knows* (such as a password or PIN)
- Something only the user *has* (such as a swipe card or portable authenticator)
- Something only the user *is* (like a fingerprint or retinal scan)

An example of two-factor authentication that we are all familiar with is the automated teller machine (ATM). Each ATM requires a card (possession factor) and a PIN (knowledge factor). If you lose the card, your account is still safe because the person who finds it will not know your PIN.

The use of two-factor authentication is gaining in popularity as many major web sites offer the feature as an option.

Currently Offering 2FA Option

Amazon	Last Pass
Apple	LinkedIn
Dropbox	PayPal
Evernote	Steam
Facebook	Twitter
Google/Gmail	Yahoo! Mail

Most systems use your cell phone either to generate an authentication number, or to receive one in the form of a text message. Others make use of a separate, physical authenticator carried on a key chain or plugged into a USB port.

The Beacon staff urges you to consider using two-factor authentication wherever you can. Its use can significantly reduce account breaches, online

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

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

fraud, and identity theft, because a password alone would not be enough to give a thief access to a user's account.

An additional note: users need to recognize that the security of the *possession factor* (phone, authenticator) is critical to the overall account security, as recovery of the password is sometimes remarkably simple.

Password Recovery

Everyone needs to be concerned about account security, but we can classify users into two categories. The vast majority of us are in the first group – those who have no access to trade secrets, state secrets, or confidential financial information. For the most part, thieves don't want our accounts specifically; they want *any* account they can get. Two-factor authentication works very well for us because hackers won't spend the extra effort to get around it.

However, it is the second, smaller group that thieves might target specifically. Some accounts are worth spending extra time and effort to crack – system administrators, CEOs, and business accountants, to name a few. For those users, the effectiveness of two-factor authentication might depend on the security of the password recovery options, or, "*What do I do if I don't have my possession factor?*"

Many account tools depend on answers to "secret questions" to verify your identity. Because the pool of questions is frequently limited, the answers are simple to discover. Your mother's maiden name? Your first car? The street where you grew up? Consider the security risks of depending on such questions to verify your identity.

To make this element as secure as possible, write your own question if you can. Chances are slim that anyone can find out what your Great-Aunt Sally gave you for your tenth birthday. On the other hand, *you can just lie*. Who will argue when you claim that you first car was a **1938 Rolls Royce Wraith**? Or that your mother's maiden name is **K@7yt$!xx**?

Password Safety

In spite of the considerable security increase offered by two-factor authentication, don't use it as an excuse for having a weak password: security depends on *both* factors. Remember the rules for having a strong password:

- Make it at least 15 characters.
- Use uppercase letters, lowercase letters, numbers, and special characters.
- Keep it private and hidden.

Password Management

Most of us have way more passwords than we can remember. If it makes sense for you to use a password management program, you might want to start your search for a good one here:

http://password-management-software-review.toptenreviews.com/

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

BUSINESSAFE

Critical Infrastructure

Contents

The Physical side of Cyber Security

Focus: Energy Sector

The energy sector, specifically the electricity subsector, is one of our nation's most critical lifelines. Yet, the electrical subsector shares numerous interdependencies with the communications, transportation, and information technology sectors. This interdependent nature means that a threat to one becomes a threat to all.

Recent media reports have highlighted several high-profile energy sector incidents throughout the US. The most notable one occurred at the Metcalf electric substation just south of Silicon Valley in California. In April 2013, two individuals cut fiber optic lines at two underground communication vaults near the Metcalf substation, causing the supervisory control and data acquisition (SCADA) communications to fail at multiple substations. The saboteurs, armed with assault rifles, fired on a number of transformers from outside the substation fence line. They successfully caused a substantial cooling oil leak, leading to failure of those transformers.[1]

Metcalf Substation

In a separate set of incidents, an individual in Arkansas was responsible for wreaking havoc on electrical power lines and energy facilities between August and October 2013. The suspect pulled down power lines and set fire to a control building.[2]

Then in February 2014, officials in Georgia arrested three members of an anti-government group for plotting an attack against federal facilities, power grids, transfer stations, and water treatment facilities. According to prosecutors, the group's goal was to trigger martial law. [3]

These instances highlight the real threats faced by owners and operators of energy assets. The June 2013 edition of the CIP Report [4] documented threats to the power grid varying

1 http://www.cnn.com/2014/02/07/us/california-sniper-attack-power-substation/

2 http://www.justice.gov/usao/are/news/2013/November/JWoodring_indict_JTTF_110613.html

3 http://www.huffingtonpost.com/2014/02/21/georgia-militia-facebook_n_4834322.html?utm_hp_ref=politics

4 http://cip.gmu.edu/wp-content/uploads/2013/06/June-2013_Energy.pdf

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

LET US KNOW:
(850) 410-7400
Admin@SecureFlorida.org

among state-sponsored attacks, domestic violent radical organizations, single-person strikes, and other coordinated attacks. Disruption from these attacks could result in cascading effects further affecting communications, transportation, food, water, and banking and finance.

Government and industry officials have reacted to these and other incidents with an increased focus on security planning and training at energy sector facilities. In the Metcalf substation incident in California, Pacific Gas and Electric (PG&E) discovered that local authorities were not fully aware of the criticality of the site. In the aftermath, PG&E made concerted efforts to educate law enforcement and provide information on such critical facilities to emergency responders.

Additionally, the Metcalf incident highlights the need to ensure that security planning includes all sections of an organization such as operations, security, and information technology. Likewise, companies must ensure cooperation with external organizations in their security planning. At Metcalf, officials from both communications and power companies worked feverishly to identify and fix the disruptions. However, it eventually became clear that because the organizations worked independently they were not effectively communicating with one another or with responders.

Although physical security breaches also present threats to an organization's cyber infrastructure, mitigation strategies remain the same. Stakeholders need to protect the assets "within the fence line" from theft, cyber sabotage and network intrusion, all of which can be equally damaging scenarios. What is important is that all stakeholders recognize the vulnerability and know what measures to take to mitigate a threat when it occurs.

Florida faces the additional challenge of being the only state with relatively limited grid connectivity along its northern border. Realizing this, industry officials in Florida are taking proactive steps to mitigate vulnerabilities at their energy facilities by sharing industry lessons learned with federal, state, and local response agencies.

View our BusinesSafe FACT SHEETS to learn how to protect your business from potential security breaches.

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

LET US KNOW:
(850) 410-7400
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

Google Fiber Chooses Nine Metro Areas for Possible Expansion

http://arstechnica.com/business/2014/02/google-fiber-chooses-nine-metro-areas-for-possible-expansion/

Summary:

Google Fiber is ready to expand, as Google has identified nine metro areas scattered around the country as possible sites of deployment, the company said.

"We've invited 34 cities in nine metro areas across the US to work with us to explore what it would take to build a new fiber-optic network in their community," Google said in an announcement today. "Many of these cities asked for Google Fiber in 2010 and have since continued to try to bring better Internet access to their residents."

Analyst Note: According to www.netindex.com the US broadband speed ranks 33rd in the world with an average download speed of 21.81 Mbps. By comparison, Hong Kong, ranked number 1, has an average download speed of 73.07 Mbps. Google's efforts may have the effect of pushing other Internet service providers to increase their speed offerings. Comcast currently offers a 105 Mbps cable connection in many markets. We believe that the increase in available bandwidth will serve to broaden the cyber security attack landscape. As speeds increase, prices will likely drop for slower connections, allowing more connectivity. While the percentage of bad actors remains relatively constant, their numbers will likely increase.

2013 An Epic Year for Data Breaches with Over 800 Million Records Lost

http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

Summary:

If it felt as though last year saw more and bigger data breaches than usual, well, that's because it did. 2013 was a bumper year for data loss, dominated by a handful of truly enormous breaches, according to a summary report from threat intelligence consultancy firm Risk Based Security (RBS).

Analyst Note: 2013 saw an increase in the number of data breaches while at the same time the scale of breach grew tremendously. The recent Target breach highlighted the risk in a very real way.

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

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org

Windows XP Cutoff Poses Breach Risk for Retailers

http://www.computerworld.com/s/article/9246011/Windows_XP_cutoff_poses_breach_risk_for_retailers

Summary:

Retailers running Windows XP-based point of sale terminals will soon face an increased risk of hacker attacks, Symantec says.

Analyst Note: Many point of sale terminals run Windows XP. As of Febuary the operating system maintains nearly a 30% market share as of February. The presence of Windows XP hidden in plain sight, as it were, offers a tremendous opportunity for hackers when Microsoft ends XP support on April 8. The coming month will likely see an uptick in XP-focused malware and holds the potential for future high profile data breaches, particularly in the retail sector.

What Justin Bieber's Twitter Hack Teaches Us About Social Media Security

http://www.forbes.com/sites/jameslyne/2014/03/12/what-justin-biebers-twitter-hack-teaches-us-about-social-security/

Summary:

Justin Bieber's Twitter account was hijacked briefly this month and, now that the dust has settled, it seems like a good opportunity to review how these attacks happen and what all of us should learn about Twitter security.

Analyst Note: This article includes "Simple Twitter Security Advice – 7 Tips," which contains further discussion on two-factor authentication and the importance of good password-recovery questions.

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

www.surveymonkey.com/s/SFBeacon2

The Secure Florida.org Beacon

Editor Kevin Wiggins

Design Chris Kenworthy

Secure Florida.org

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

Let Us Know:
(850) 410-7400
Admin@SecureFlorida.org