

Cloudy with a Chance of Malware



2014 National Cyber Security Awareness Month

Randell Smith, CISM, CISSP, PMP
Chief Information Security Officer

Information Technology Services

**Our Shared
Responsibility**

staysafeonline.org



National Cyber Security
Awareness Month

City of Phoenix



Agenda

A word cloud of cybersecurity terms including: Targeted Attacks, Zero-days, Bots, Mobile, Social Media, Linux, Emerging Attacks, Spam, Internet of Things, Windows, Vulnerabilities, Spearphishing, Discovered, Increased, Volume, Percentage, Decreased, Massive, and Target.

1. Introduction – Threat Landscape
 - Cyber Facts
2. Protecting yourself and your family against hackers and cybercriminals
3. Using social media safely
4. Recovering from having your personal information compromised
5. Questions & Answers



Cyber Facts - Malware





Cyber Facts - Phishing



MORE THAN 50%
of phishing emails in
2011 were targeted at
online banking users





Cyber Facts – Credit Card Fraud



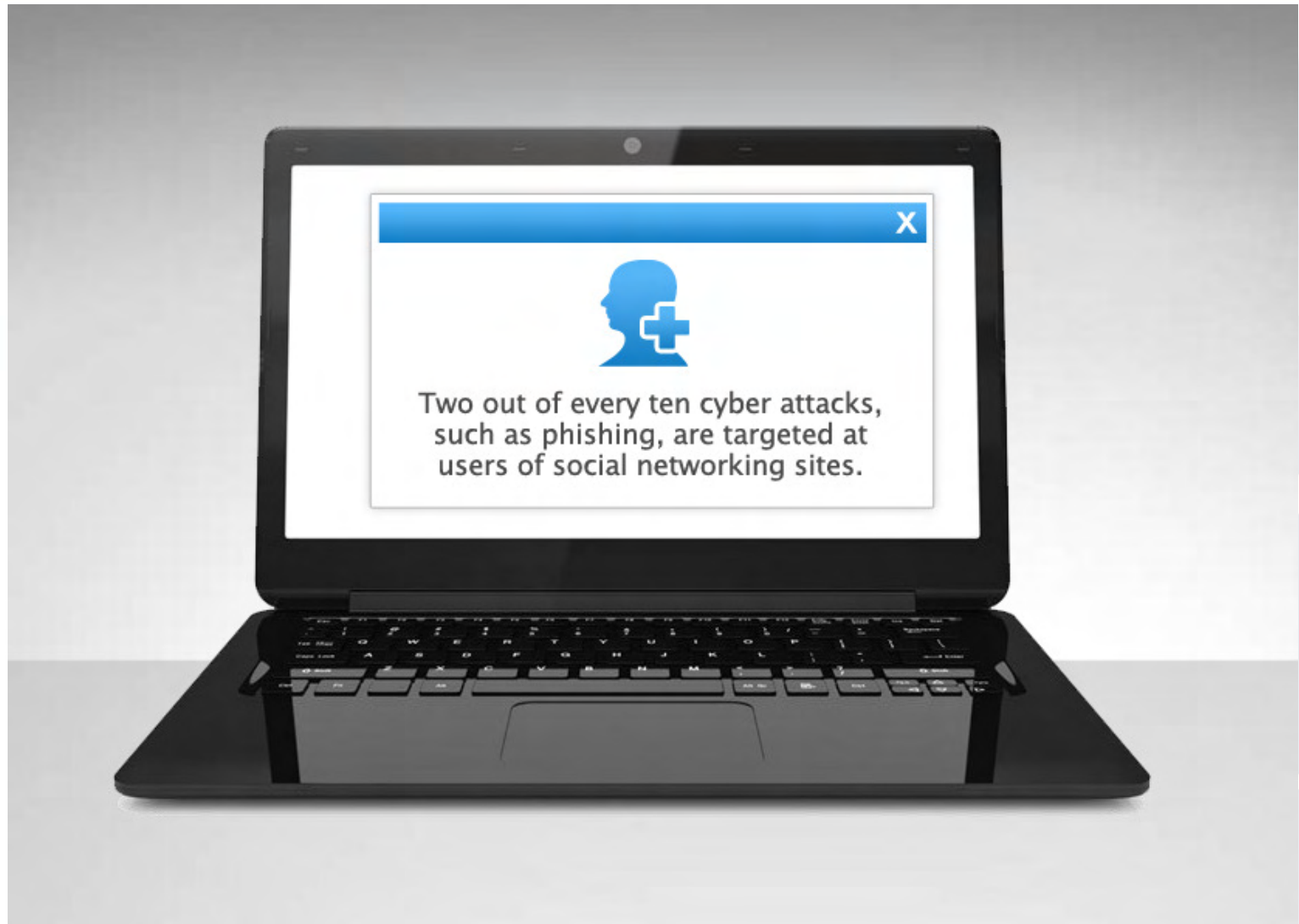
RECEIPT

CREDIT CARD
FRAUD COSTS
MERCHANTS
ABOUT
**\$20
BILION**
A YEAR





Cyber Facts – Social Media





Cyber Facts – ID Theft





Cyber Facts – Mobile Devices



Malicious programs and viruses are making their way onto mobile devices very quickly. Today, the Android platform is the most targeted by malware threats.





Cyber Facts – Online Gaming



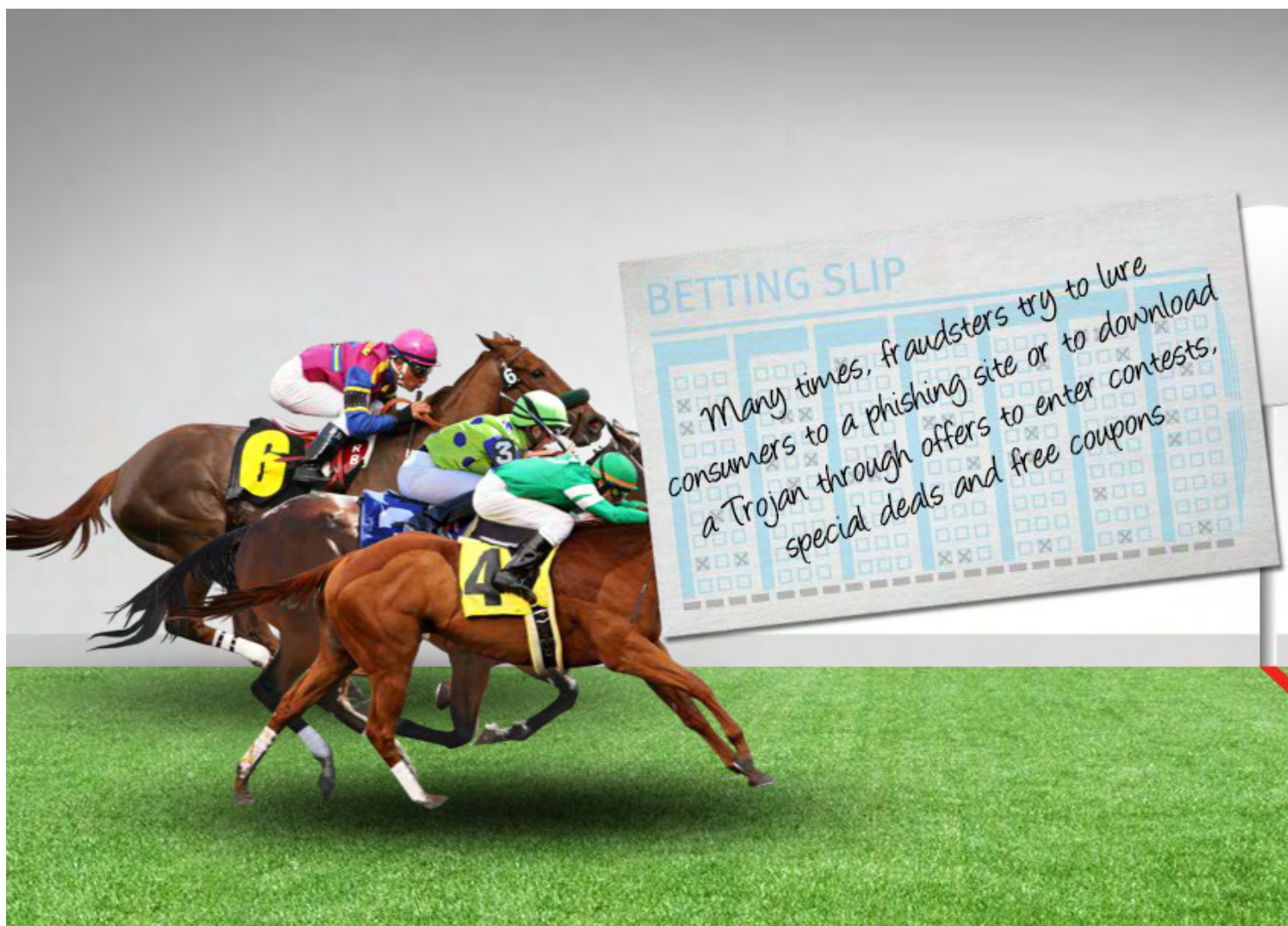
GAME OVER

Online gamers are often targeted by fraudsters through messages that offer sneak previews or free access to upcoming game releases





Cyber Facts – Free Stuff





Cyber Facts – Email





Scale and speed of cyber-attacks is escalating

- Federal government suffered a **680% increase in cyber security breaches** in the past six years. (Face the Facts USA)
- Cyber criminals **stole over \$100 million** from US banks in 2013. (Congressional Cybersecurity Caucus)
- **600,000 accounts are compromised** every day on **Facebook** (Floridatechonline.com)
- **43% of companies** had a **data breach** in the past year
- The National Nuclear Security Administration records **10 million attempted hacks a day**. (Defense News)
- The U.S. Navy receives **110,000 cyber attacks every hour**. (Floridatechonline.com)
- The estimated **annual cost of global cybercrime over \$100 billion**. (Go-gulf.com)



Online Threats



- **30,000** URLs (websites) are infected every day; 80% of those infected sites are legitimate.
- **85% percent** of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web.
- Drive-by downloads have become the top web threat.

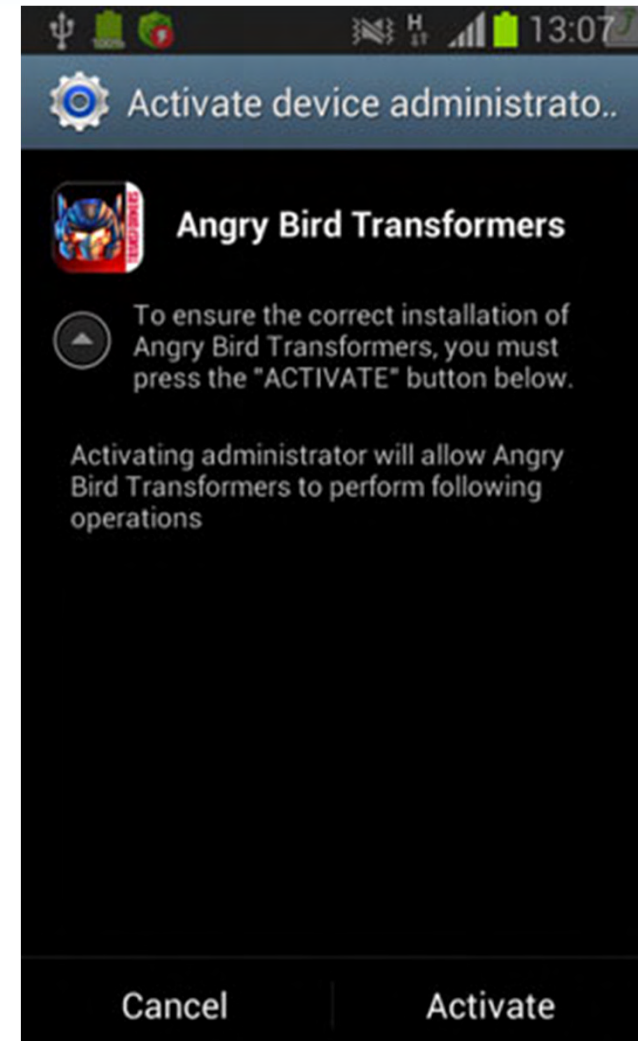
Update antivirus and operating system



Angry Birds Malware



1. New Android malware Trojan **formats the device's SD card** and **deletes all content** on it.
2. Malware hides all notifications about new incoming SMS.
3. An SMS message saying is **sent to every contact in the device's address book** and every valid phone number from which an SMS is received.
4. Messages are **sent repeatedly to all these numbers every five seconds**, so the mobile account associated with the compromised device can be depleted in minutes or even seconds.





Smishing Attacks



- **‘smishing’** (term used to describe SMS phishing) is a more promising tool for cyber criminals than phishing (email) because **users have fewer defensive technology tools.**
- Text messaging—most common non-voice use of a mobile phone.
- 73 percent of adults text daily (41.5 messages/day).
- Ages 18 and 24 average 110 messages/day. Mobile phones aren’t equipped to help users avoid malicious text messages.



Data Breaches >30,000+ accounts

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



Oct 15
Undisclosed



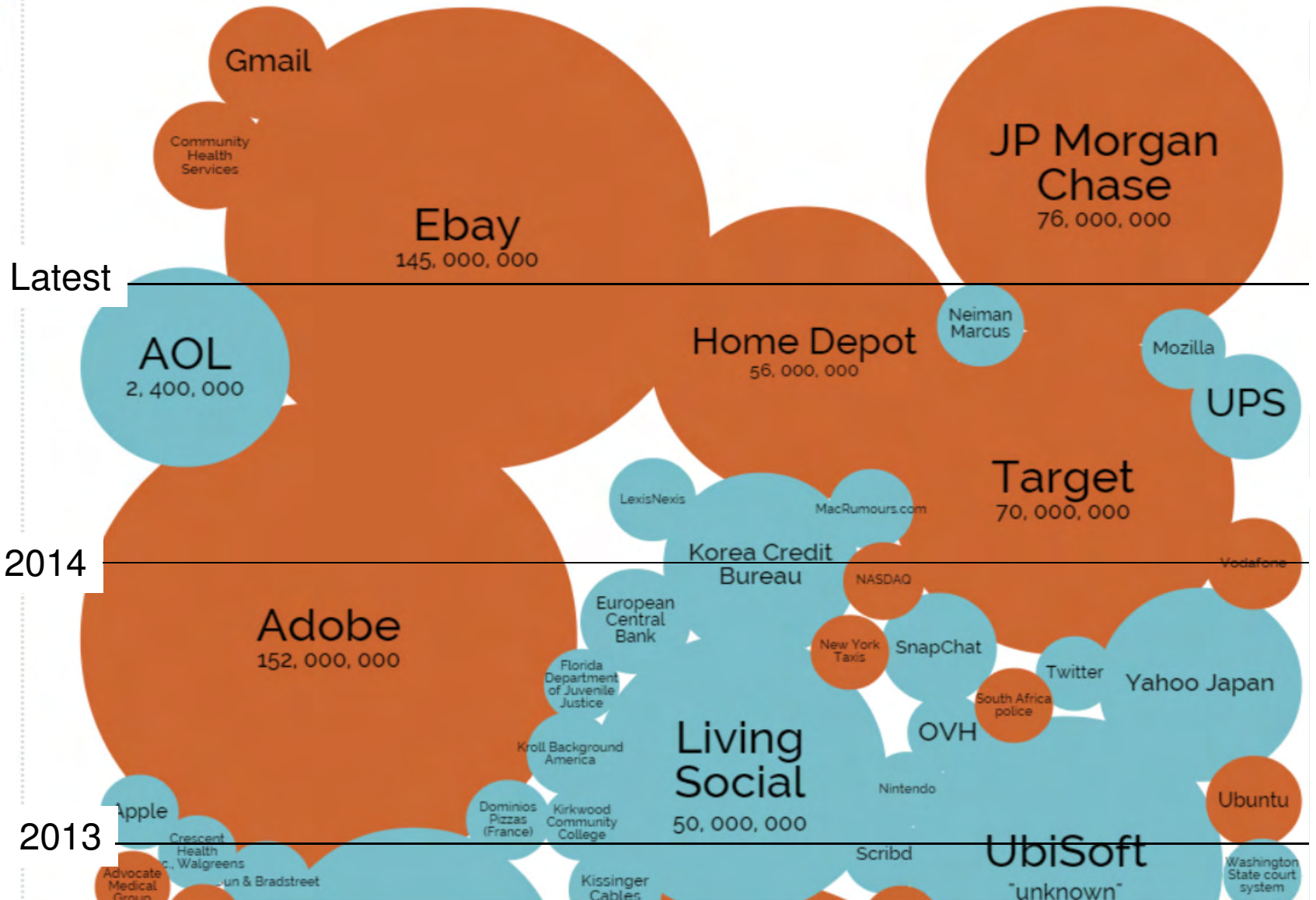
Oct 14
Undisclosed



Oct 13
7,000,000



Oct 12
200,000





Thousands of Snapchat pics leaked online



- **Explicit pictures and videos** taken with photo sharing app Snapchat were posted online (10/11/2014) from as many as **200,000 users**.
- The service specializes in photos, videos and messages users can send that "disappear" after a period of time. However, several services have popped up allowing others to save photos or videos.
- Snapchat says the service itself has not been compromised, but that users "**were victimized by their use of third-party apps**."
- As half of Snapchat's **users are aged between 13 and 17**, there is concern many of the indecent images might be of children



Data Breaches - Target



40 million – The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.

70 million – The number of records stolen that included the name, address, email address and phone number of Target shoppers.

46% – The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.

\$100 million – The number of dollars Target says it will spend upgrading their payment terminals to support Chip-and-PIN enabled cards.

- In the Target breach, it was a heating and air conditioning vendor that was exploited to gain entry.



Identity Theft Resource Center



2014 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details.

Report Date:
10/14/2014

<http://www.idtheftcenter.org/>

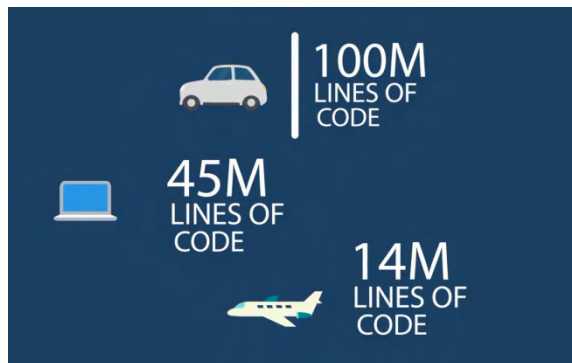
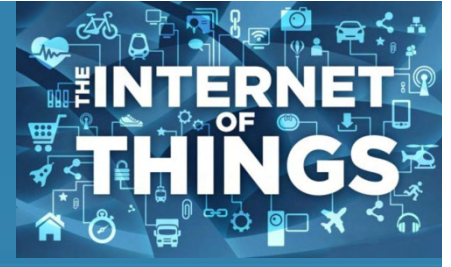
Totals for Category: Banking/Credit/Financial	# of Breaches: 24	# of Records: 1,172,320
	% of Breaches: 4.0%	%of Records: 1.5%
Totals for Category: Business	# of Breaches: 211	# of Records: 64,407,359
	% of Breaches: 34.8	%of Records: 83.0%
Totals for Category: Educational	# of Breaches: 44	# of Records: 1,222,361
	% of Breaches: 7.3%	%of Records: 1.6%
Totals for Category: Government/Military	# of Breaches: 68	# of Records: 3,623,626
	% of Breaches: 11.2	%of Records: 4.7%
Totals for Category: Medical/Healthcare	# of Breaches: 259	# of Records: 7,151,542
	% of Breaches: 42.7	%of Records: 9.2%
Totals for All Categories:	# of Breaches: 606	# of Records: 77,577,208
	% of Breaches: 100.0	%of Records: 100.0%

2014 Breaches Identified by the ITRC as of: 10/14/2014

Total Breaches: 606
Records Exposed: 77,577,208



Internet of Things (IoT)



- **Every device in your house is connected to the Internet:** Refrigerator, Toaster, Thermostat, Water meter, Door Locks, TV Webcam, etc.
- Security researcher sitting at home within 20 minutes found 22 remotely exploitable vulnerabilities in a handful of devices.
- **100M Lines of Code in new cars;** 14M Lines of Code in Boeing 787 Dreamliner.
- **Hackers broke into more than 100,000 consumer gadgets** (home-networking routers, connected multi-media centers, televisions, and one refrigerator), and
- Used those objects to **send more than 750,000 malicious emails** to enterprises and individuals worldwide.



Protecting Yourself and Your Family



- Social Engineering
- Identity Theft
- Creating a Hackproof PassPhrase



Social Engineering

HOW MUCH EMAIL IS SENT?

107 TRILLION ANNUALLY | **294** BILLION EACH DAY

90% OF ALL EMAIL IS SPAM & VIRUSES

77% Phishing represents 77% of all socially-based attacks

37.3 MILLION Users reported phishing attacks in the last year

Clicking links within email accounted for 88% of all reported phishing

88% Most common phishing attacks mimicked banking institutions

1.8 MILLION VICTIMS IN 2013

Medical identity theft on the rise due to websites impersonating medical providers

TOP PLACE FOR THEFT IS WORK AREA

80% of thefts involved disabling or bypassing controls

88% OF REPORTED STOLEN ASSETS WERE PERSONAL DATA

Phishing 01

Practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information



Practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system

Impersonation 03

Vishing 02

Practice of eliciting information or attempting to influence action via the telephone, may include such tools as "phone spoofing"



2.4M CUSTOMERS TARGETED FOR PHONE FRAUD FOR ALL OF 2012



2.3M CUSTOMERS TARGETED FOR PHONE FRAUD FOR FIRST HALF OF 2013

AVERAGE LOSS FOR TARGETED BUSINESSES \$42,546 per account

AVERAGE VICTIM OF IMPERSONATION
41.7 YEARS OLD | **\$4,187** DOLLARS LOST

60% of US Adults Who send and receive text messages received mobile spam in 2012

14% REPLY TO TEXT | **26%** CALL A NUMBER | **60%** CLICK A LINK
WHAT DO SMISHERS* ASK FOR? *phishing in text messages



Common Email Phishing Attack Subject Lines



- Subject: [IMPORTANT] Amount overdue
- Subject: [IMPORTANT] Regarding payment overdue
- Subject: [IMPORTANT] Recent invoice
- Subject: [IMPORTANT] Final letter before commencing legal action
- Subject: [IMPORTANT] Payment overdue notification
- Subject: [IMPORTANT] Amount overdue notification
- Subject: [IMPORTANT] Final notification before commencing legal action
- Subject: [IMPORTANT] Invoice overdue notification
- Subject: [IMPORTANT] Notification about the amount overdue
- Subject: [IMPORTANT] Latest invoice
- Subject: [IMPORTANT] Invoice overdue
- Subject: [IMPORTANT] Recent invoice unpaid
- Subject: [IMPORTANT] Last letter before commencing legal action
- Subject: [IMPORTANT] Latest letter on invoice overdue
- Subject: [IMPORTANT] Last notification before commencing legal action



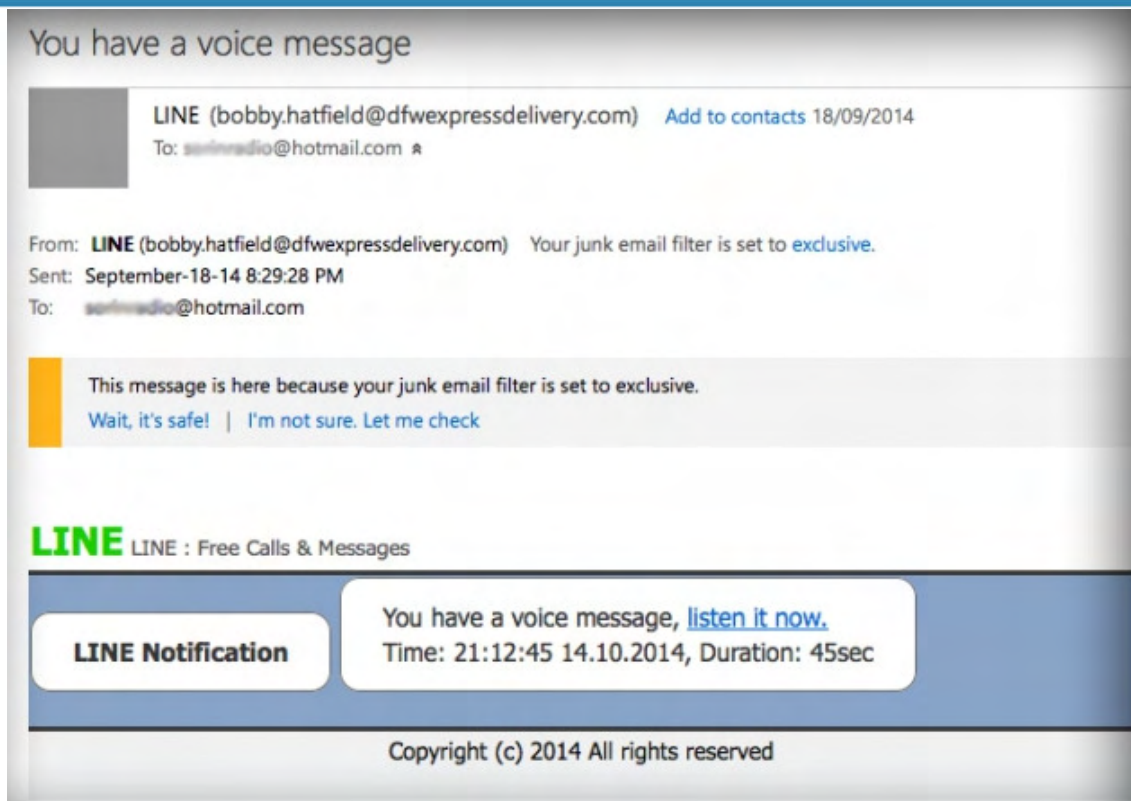
Social Engineering

- Fake offers for free cell phone minutes accounted for the **largest number of attacks on Facebook users** in 2013.
- **12%** of social media users say **someone has hacked into their social network account** and pretended to be them.
- **25%** continue to **share their social media passwords** with others.
- **33%** connect with **people they don't know**.



Voice Message E-mail Scam

1. Someone leaves you a voicemail via email.
2. You are **invited to 'Listen' to your message**. By clicking "listen is now".
3. Clicking the button takes you to a malicious website that will download and install a file called "Browser 6.5" on your computer or phone.
4. If you then click the "Agree" button in the "browser", **text messages will be sent to premium rate phone numbers**.



This scam **does not work on Macs** as "Browser 6.5 is not compatible with your computer". However it **does work on a jailbroken iPhone** as jailbroken phones cannot be protected.



Fake Travel Agency

1. Tricksters create great websites for “new” travel agencies offering amazing deals.
2. The **scammers**, usually using amazing pictures stolen from the Internet to promote their destinations, **create fake travel agencies** for a month at a time.
3. **Goal is to get hundreds of avid tourists who pay on the spot**, and then close down the "business".



High quality websites. Hard to differentiate from a real business. **Scammers buy Google AdSense or Facebook ads and close deals on spot.**



Credit Card Charges

1. You **receive a call** from someone who says he's **working for your credit card provider**, whether VISA, Mastercard, or American Express:
2. **Will ask if you just made a large purchase.** If you say no, will then ask if you have lost your credit card or if it's still in your possession.
3. He **will read off** the full **card number** on front and first 4 digits on back. **Will ask you to confirm last 3 digits on back.**



4. If you give him the 3 numbers on back he will say, "That's correct" and tell you your money will be refunded in 5 business days.
5. There will be no refund, the **scammer now has your CVV number and can use your card to make online purchases.**



Stolen PIN With Infrared Camera

1. In line at shopping counter; man behind you appears to be texting on his cell phone.
2. Later you find a number of charges on your credit card bill you didn't make.
3. The guy behind was actually activating his camera and recording those seconds when your credit card is passed back and forth, registering the numbers on it.
4. After you left the counter, he used a **FLIR One infrared camera** to steal your PIN.



5. FLIR One is an infrared **attachment to smartphone** which allows scammer who comes right after in you in line to see the numbers you pressed on the PIN pad.



Identity Theft

- In 2012, more than **12 million Americans** were affected by identity theft
- Impact to U.S. economy – **\$41 billion** (Ponemon Institute)
- **Every three seconds**, a consumer's identity is comprised





Who's at risk of identity theft?



- ANSWER – **Everyone**
- 12% of Americans age 18 or older have been subject to identity theft in just the past 12 months.
- Over half (52%) of Americans do not check their free credit report annually.
- Just 14% of Americans say they subscribe to identity theft protection services such as Lifelock, Identity Guard, or LegalShield.
- Just 17% of Americans check their credit regularly with one of the credit bureaus.



Child ID Theft



- The rate of identity theft for children was **35 times higher** than the rate for adults in the same population.
- **10.2% of children** have had their Social Security numbers stolen
- Child IDs were **used to purchase homes and automobiles, open credit card accounts,** secure employment and obtain driver's licenses.
- **Children are easy targets.** Their identities are often a blank slate.
- The probability of discovery is low. Parents typically don't monitor a child's identity and the crime can go undiscovered for many years.



Child ID Theft



CHRIS FROM ARIZONA

AllClear ID discovered that a 17-year-old girl has over \$725,000 in debt. Chris's daughter's Social Security number was linked to eight different suspects living in border states. The suspects opened 42 open accounts including mortgages, auto loans, credit cards, and bills in collections including medical, credit cards, and utilities.



Child ID Theft



NATHAN FROM KENTUCKY

Nathan, a 14-year-old, had a credit history that went back more than 10 years. Several credit cards and a foreclosed mortgage were already in his credit history, all from a suspect living in California. The thief established good credit for the first 10 years and was able to finance a \$605,000 home in CA through first and second mortgages. He also used the boy's SSN to open several credit accounts.



Medical ID Theft



- Rapidly growing; **impacts almost 6% of Americans.**
- Ponemon Institute's 2012 study, "The National Study on Medical Identity Theft," **more than 1.85 million victims** of medical ID
- Estimated economic impact in United States at **\$41.3 billion**
- **33% of medical ID theft** occurred when **a friend or family member** used an individual's medical information without their knowledge.



Creating a Hackproof PassPhrase



How to Create a Hackproof PassPhrase

- Example: The quick brown fox jumps over the lazy dog, becomes **tqbfjotld**.
- Next add a Special Character (@\$!)
- Last, add a year followed by a letter (a,b,c)
- Hackproof passphrase **tqbfjotld\$1932a**

It would take a desktop PC about
325 million years
to crack your password

- Long enough to be hard to guess
- Not a famous quotation from literature, holy books, et cetera
- Hard to guess even by someone who knows the user well
- Easy to remember
- Not reused between sites, applications and other different sources.

<https://howsecureismypassword.net/>



Password Managers



Pros

Convenience and security - can generate strong secret questions

Portability – May be portable if combined with something like Google or Firefox

Secure storage - Sensitive information is encrypted in storage and protected by a master password.

Not just for passwords – Can store bank details, insurance numbers, credit cards, passport numbers

Recommendation 1. Only use password managers that store your encrypted password vault in cloud; your key's remain on your computer.

Cons

Single point of failure - If your master password is weak then you could lose everything if attacker cracks password.

Keys to the kingdom - If you forget your master password, you may not be able to recover your keys.

Trust in the cloud – If your encrypted keys are stored in the cloud, and the cloud is breached, hackers may be able to crack your password.

Recommendation 2. Use two factor authentication for your really sensitive information and a password manager for the rest.



Password Insecurity

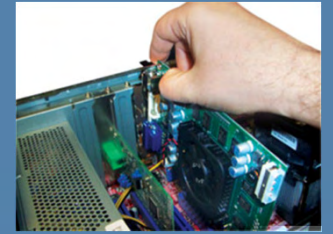


The 25 most popular passwords 2013

1. 123456	11. 123123	21. password1
2. password	12. admin	22. princess
3. 12345678	13. 1234567890	23. azerty
4. qwerty	14. letmein	24. trustno1
5. abc123	15. photoshop	25. 00000
6. 123456789	16. 1234	
7. 111111	17. monkey	
8. 1234567	18. shadow	
9. iloveyou	19. sunshine	
10. adobe123	20. 12345	



Brute Force Attack



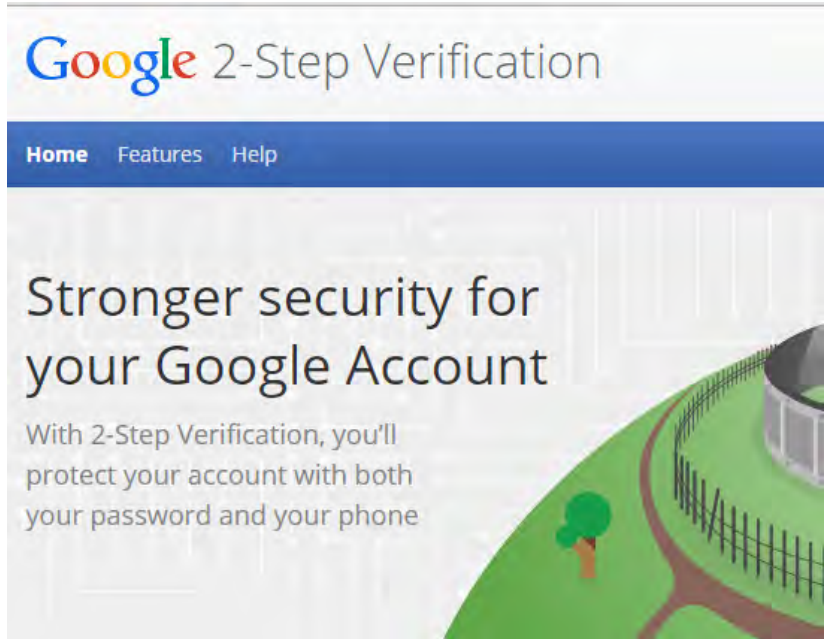
Today ***any 7 character password can be cracked by brute force in hours*** using a regular personal computer with a GPU graphics card.

- Time to break a five character random password like 'xnZyr' – **24 seconds** at a rate of 9.8 million password guesses per second. (normal CPU)
- Time to break same password with the addition of a GPU graphics card – **1 second**

Source: <http://howsecureismypassword.org/using-passwords-guide/>



Google 2-Step Verification



Signing in to your account will work a little differently

- 1 Enter your password**
Whenever you sign in to Google, you'll enter your password as usual.
- 2 Enter a verification code**
Then, you'll be asked for a code that will be sent to your phone via text, voice call, or our mobile app.

An extra layer of security

Most people only have one layer - their password - to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone to get into your account.





Using Social Media Safely

1. Social Media Oversharing
2. Facebook Privacy Checkup
3. Social Networking Do's and Don'ts
4. Disabling Smartphone Locational Services





Social Media Oversharing



Keep yourself and your information safe, **pay careful attention to your online activity**. Avoid posting information including:

- Travel plans
- Bank account information
- Your full address and birthdate
- Your children's' names, school, and birthdates
- Location information, such as the name of your work place
- Your daily schedule





Facebook Privacy Checkup



The screenshot shows the Facebook interface with the Privacy Shortcuts menu open. The menu is titled "Privacy Shortcuts" and contains the following items:

- Privacy Checkup**: Represented by a padlock icon and a blue dinosaur character sitting at a laptop.
- Who can see my stuff?**: Represented by a globe icon.
- Who can contact me?**: Represented by a person icon.
- How do I stop someone from bothering me?**: Represented by a minus sign icon.

At the bottom of the menu is a button labeled **See More Settings**. A mouse cursor is pointing at the top right of the menu.

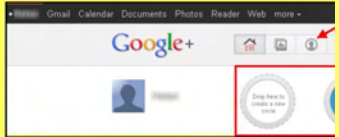
Google+ Smart Card

Social Networks - Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family. Do not post anything you would not want your family, friends, or colleagues to see.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos or videos that clearly show your face.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Managing Your Google+ Profile

Google+ provides privacy and sharing options using Circles. You can share content with your family, friends, or colleagues. Content is shared only with the people you specify in your Circles.



Profile Settings

Apply and save the Profile settings shown below to ensure your profile is secure.

LinkedIn Smart Card

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family. Do not post anything you would not want your family, friends, or colleagues to see.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos or videos that clearly show your face.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Managing Your LinkedIn Profile

LinkedIn is a professional networking site whose users are employees and employers. Users post and share information about their work and professional life.



Profile Settings

Apply the Profile settings shown with arrows below to ensure your profile is secure.

- Users tend to share information related to their work and professional life.
- LinkedIn profiles tend to be more visible and searchable.
- Paid LinkedIn accounts have access to more information.
- The type of information users can see about each other is more extensive.

Twitter Smart Card

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family. Do not post anything you would not want your family, friends, or colleagues to see.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos or videos that clearly show your face.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Managing your Twitter Account

Twitter is a social networking and microblogging platform with over 300 million active users as of 2014.



Following are people you subscribe to. Tweets are refer to a post protected by your account.

Hashtags (#topic) are used to mark a keyword. Posts with hashtag are categorized in Twitter search engine. Hashtagged words that become Trending Topics (ex. #jan25, #egypt, #egypt).

Mentions (@username) are used to tag a user update. When a public user mentions a private account, the link to the private account profile is shown.

Profile Settings

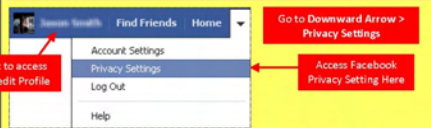
Apply the Profile settings shown below to ensure your profile is secure.

Facebook Smart Card

Social Networks - Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about you or your family. Do not post anything you would not want your family, friends, or colleagues to see.
- Ensure that your family takes similar precautions with their social media accounts.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Minimizing your Facebook Profile



Facebook has hundreds of privacy and sharing options. To control how your personal information is shared, you should use the settings shown below (such as Only Me, Friends Only) for (1) Privacy, (2) Connecting, (3) Tags, (4) Apps/Websites, (5) Info Access through Friends, and (6) Past Posts.



Disabling Locational Services



(U) Disabling Locational Services

(U//FOUO) Turning off locational services—collectively or individually—on mobile devices may help reduce geotagging of personal information through mobile device functions and social media applications available through many mobile devices.

(U) To reduce the effects of locational services and geotagging, the following steps can be taken:

1. (U) On Android® devices, tap the **Location** option from the **Settings** menu. Most Android devices will allow you to turn off location services for your entire phone, such as GPS services, and other companies' location services. Generally, by leaving a box unchecked, the location service is turned off.
2. (U) On iPhone® and Windows® phones, tap **Settings**, then tap **Location Services** and toggle the switch to **OFF**.
3. (U) On many social media platforms, an account's security is only as good as its weakest link. Consider un-tagging yourself from geotagged posts made by other users on social media.

UNCLASSIFIED



(U) iPhone® locational services menu.

(Image Source: [Apple](#))



Recovering from a Compromise

**DON'T
PANIC**

1. Don't Panic!
2. Check to see if your user information has been posted online
(<https://haveibeenpwned.com/>)
3. If your information was compromised by a company, contact them to see if they will be providing credit monitoring services.
4. Immediately change your passwords!
5. Notify Phoenix Police Department
(<https://www.phoenix.gov/policesite/Documents/066344.pdf>)



What to Do After Identity Theft

Place an Initial Fraud Alert

- Contact 1 of the credit reporting companies.
- Report that you are an identity theft victim.
- Ask the company to put a fraud alert on your credit file.
- Confirm that the company you call will contact the other 2 companies. Placing a fraud alert is **free**. The initial fraud alert stays on your credit report for 90 days. Be sure the credit reporting companies have your current contact information so they can get in touch with you.

Credit Reporting Companies

Exquifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

Order Your Free Credit Reports

- Contact each of the 3 nationwide credit reporting companies.
- Explain that you placed an initial fraud alert.
- Order your free copy of your credit report. Ask each company to show only the last 4 digits of your Social Security number on your report.

(<http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft>)



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS



<https://haveibeenpwned.com/>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

randell.smith@phoenix.gov

pwned?

Oh no — pwned!

Pwned on 1 [breached site](#) and found no [pastes](#)

[✉ Notify me when I get pwned](#)

[₿P Donate](#)



<https://haveibeenpwned.com/>

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



The big one. In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Pastes you were found in

A "paste" is information that has been published to a publicly facing website designed to share content, usually anonymously. Often these are indicators of a data breach so review the paste and determine if your account has been compromised then take appropriate action such as changing passwords. Pastes are often removed shortly after having been posted. Read more on the [pastes page](#).

33

pwned websites

174,451,409

pwned accounts

10,105

pastes

4,993,147

paste accounts



Identity Theft Recovery Services

Third party services offered to help victims of ID fraud reclaim their identity.

- **Fraud Alert Reminders** - The company will remind you when the fraud alert on your account is about to expire so you can renew it.
- **Fraud Specialist** - The company provides access to fraud specialists to help you manage your fraud case.
- **Identity Theft Insurance** - The company offers insurance to reimburse you for costs related to restoring your identity.
- **Lost Wallet Protection** - The company offers assistance with canceling and replacing lost or stolen debit/credit cards.

<http://www.reviews.com/identity-theft-protection-services/>

LifeLock | AllClear ID | Identity Force | ID Patrol | Trusted ID | ID WatchDog



Getting Help – FBI

THE **FBI** FEDERAL BUREAU OF INVESTIGATION



[REPORT THREATS](#) • [A-Z INDEX](#) • [SITE MAP](#)

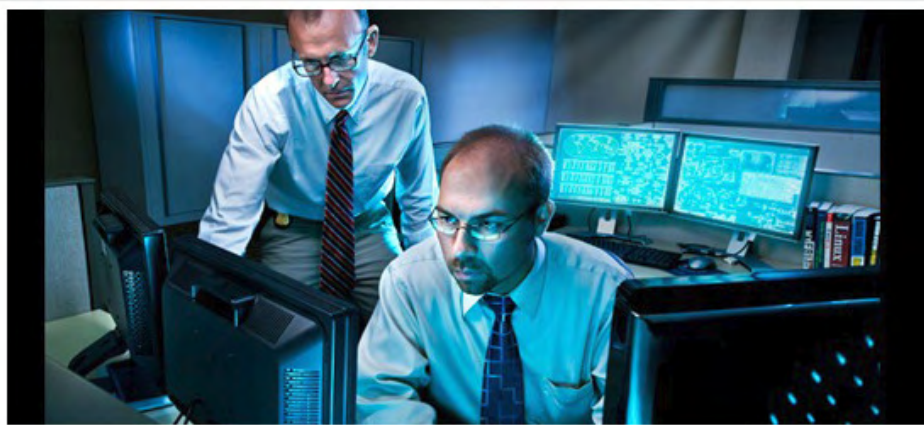
[SEARCH](#)

[CONTACT US](#) | [ABOUT US](#) | [MOST WANTED](#) | [NEWS](#) | [STATS & SERVICES](#) | [SCAMS & SAFETY](#) | [JOBS](#) | [FUN & GAMES](#)

Cyber Crime

[Get FBI Updates](#)

[Home](#) • [About Us](#) • [What We Investigate](#) • [Cyber Crime](#)



We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

The FBI certainly is. We lead the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. To stay in front of current and emerging trends, we gather and share information and intelligence with public and private sector partners worldwide.

In the News

- 10.08.14 Albuquerque** : Governor's Former Campaign Manager Sentenced to Prison for Computer...
- 10.06.14 San Diego**: StealthGenie Mobile Device Spyware Application
- 10.03.14 San Diego**: National Cyber Security Awareness Month
- 10.02.14 Headquarters**: Cyber Security
- 10.02.14 San Diego**: FBI Offers \$5,000 Reward for Cyber Fugitive

[More News](#)

Cyber Fact Sheet

Learn how the FBI is working to address cyber-based threats to national security.
[Details](#) | [Story](#)



<http://www.fbi.gov/about-us/investigate/cyber>



Getting Help – FTC

FEDERAL TRADE COMMISSION ESPAÑOL

CONSUMER INFORMATION

[MONEY & CREDIT](#)

[HOMES & MORTGAGES](#)

[HEALTH & FITNESS](#)

[JOBS & MAKING MONEY](#)

[PRIVACY & IDENTITY](#)

[BLOG](#)

[VIDEO & MEDIA](#)

SCAM ALERTS

[Veja esta página en español](#)

IDENTITY THEFT

Identity theft happens when someone steals your personal information and uses it without your permission. It's a serious crime that can wreak havoc with your finances, credit history, and reputation — and can take time, money, and patience to resolve.

What to Do Right Away
[Immediate Steps to Repair Identity Theft](#)
Here's how to begin to limit the harm from identity theft.

What to Do Next
[Extended Fraud Alerts and Credit Freezes](#)
Placing both extended fraud alerts and credit freezes on your credit reports can make it more difficult for an identity thief to open new accounts in your name.

[Repairing Your Credit After Identity Theft](#)
Here are step-by-step instructions for disputing fraudulent charges and accounts related to identity theft.

Related Items

What is Identity Theft?

FREE RESOURCES

<http://www.consumer.ftc.gov>



Getting Help – FCC

FCC Smartphone Security Checker

This tool is designed to help the many smartphone owners who aren't protected against mobile security threats. To use this tool, choose your mobile operating system below and then follow the 10 customized steps to secure your mobile device. [More about the Smartphone Security Checker.](#)

Select Your Mobile Operating System

- Android
- Apple iOS
- BlackBerry
- Windows Phone

Generate Your Checker

<http://www.fcc.gov/smartphone-security>



Getting Help – StaySafeOnline

StaySafeOnline.org
Powered by National Cyber Security Alliance

About Us | Blog | News | Events | Contact Us

SEARCH

STOP | THINK | CONNECT

I WANT TO Stay Safe Online | I WANT TO Teach Online Safety | I WANT TO KEEP MY Business Safe Online | I WANT TO Get Involved

 #ncsam
National Cyber Security Awareness Month

Get involved and do your part to make the Internet safer and more secure for everyone. This year's NCSAM theme is Our Shared Responsibility.

[LEARN MORE](#)

STOP.THINK.CONNECT.
STOP. THINK. CONNECT. is the national cybersecurity education and awareness campaign.

[GET INVOLVED](#)

NATIONAL CYBER SECURITY AWARENESS MONTH
Celebrated each October, NCSAM is a time to learn ways to stay safe and secure online.

[GET INVOLVED](#)

DATA PRIVACY DAY
Recognized annually on January 28, DPD is an international effort to recognize the importance of protecting privacy, safeguarding data and enabling trust.

[GET INVOLVED](#)

RE: Cyber
Dedicated to CEO & Board Cybersecurity Risk Management with a purpose to ascertain cyber risk to their companies.

[GET INVOLVED](#)

SO YOU WANT TO WORK IN CYBERSECURITY...
Almost two-thirds of young Americans don't know or aren't sure what the "cybersecurity profession" is according to the 2014 Raytheon-NCSA Millennial Survey. So what's the good news?
[LEARN MORE](#)

TIPS & ADVICE
View the latest tip sheets, studies and infographics for:

<http://staysafeonline.org>



Questions & Answers

Reproduced by permission. Please see
www.SecurityCartoon.com for more
material



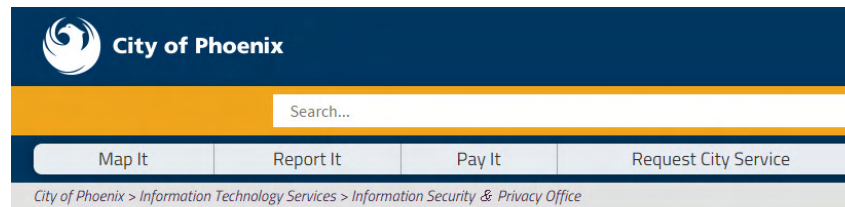
Copyright 2007, Srikanan & Jakobsson, SecurityCartoon.com

Srikanan & Jakobsson



Thank You!

For more information, please visit... Phoenix.gov/INFOSEC



Info Security and Privacy

More Information

[Info for Everybody](#) >

[Resources](#) >



City of Phoenix wins "Best of the Web" for second year in a row!

What's New

"Cloudy with Chance of Malware" Lunch and Learn Oct. 22

Every day we use computer applications, mobile communications, and the Internet to enhance our work and personal lives, and we log in daily to social media sites for work and leisure. Bring your family about protecting yourself and your family against hackers and cybercriminals, using social media information compromised. Noon to 1 p.m., Calvin C. Goode Building, 251 W. Washington. Registration required. Questions? Send us an email at ispo@phoenix.gov.

August 2014 Security Snippets Newsletter

Read the latest edition to find out what's going on in the security and privacy world.

Celebrity Scams and Fraud Presentation

With the passing of comedian and actor Robin Williams, be aware that bad guys always look out for emails and websites that promise scandalous, newsworthy, secret, and/or s death. The bad guys' goal is to get you to click on links that may cause malicious software before you click! Don't fall prey to bad guys' tricks. For more information, see the [Scam](#)