



Cybersecurity: Fact vs. Fiction

Dispelling FUD

John LaCour
June 21, 2013

Prevent. Defend. Fight back.

Cybercrime: Fact vs. Fiction

- **About PhishLabs**
- **Fear, Uncertainty, and Doubt**
- **Cybersecurity MythBusters**
- **Evolution of Cybercrime**
- **Real World Threats**
- **Understanding Risks**
- **Top Threats and Countermeasures**

Introduction to PhishLabs

What we do: PhishLabs is the leading provider of cybercrime protection and intelligence services that fight back against online threats and reduce the risk posed by phishing, malware, distributed denial of service (DDoS) and other cyber-attacks.

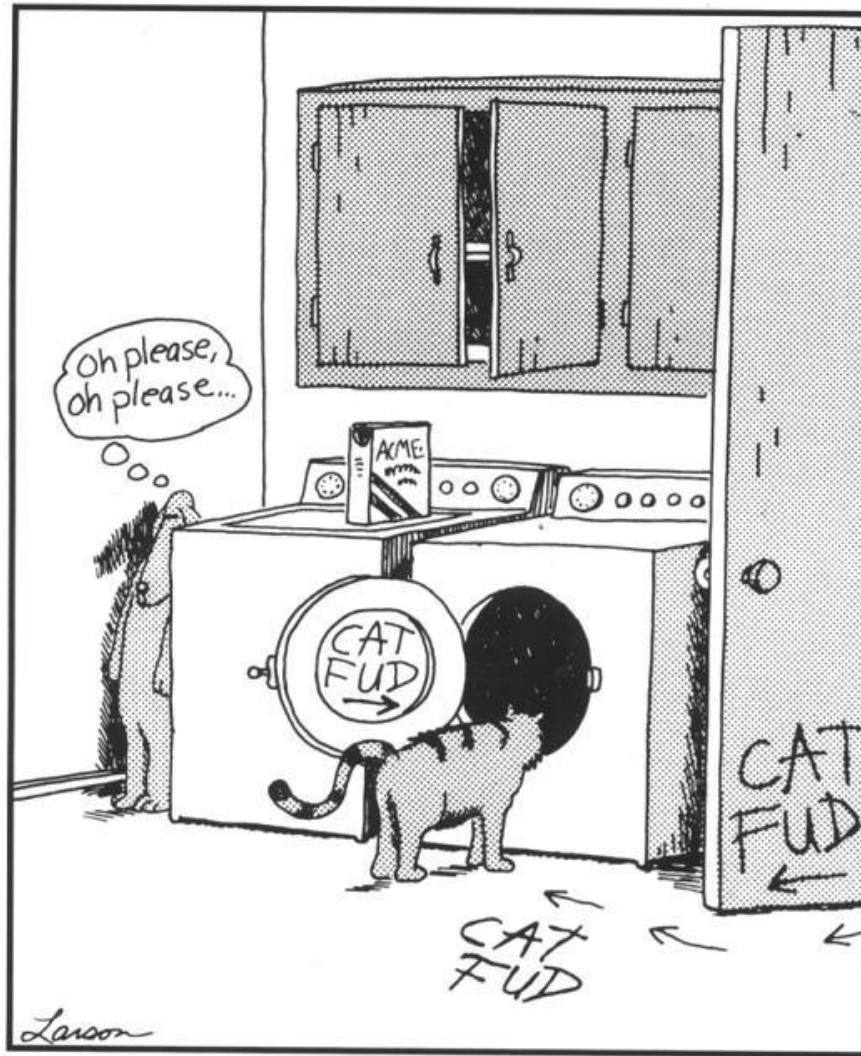
Where: HQ in Charleston, SC with staff in 4 countries

How: 24x7x365 Security Operations Center investigates and mitigates ~50,000 incidents / year

FUD



FUD



Fear, Uncertainty, and Doubt



Fear, Uncertainty, and Doubt

Eight charged in US over cyber crime ring

AAP

JUNE 21, 2013 3:54AM

EIGHT alleged members of an international cybercrime ring have been accused of hacking into the computers of more than a dozen leading financial institutions and the US army's payroll service.

US prosecutors said the scheme to steal millions from customer accounts was led by Oleksiy Sharapka, 33, of Kiev, Ukraine, who remains at large along with a second Ukrainian citizen.

The conspiracy is alleged to have begun about the same time Sharapka was deported from the US in 2012 after serving time in federal prison in Massachusetts.

Fear, Uncertainty, and Doubt



Home News Sports Living Opinion Photos & Video Obituaries Local Deals

News

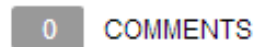
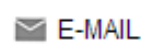
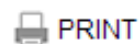
[NEXT STORY >](#) Judge won't allow Kershaw sheriff to testify in Camden Military Academy

MASSIVE BREACH

3.6 million Social Security numbers hacked in S.C.

Published: October 26, 2012

Tweet



Tax returns, personal data compromised in 'massive' breach

By NOELLE PHILLIPS — nophillips@thestate.com

The U.S. Secret Service detected a security breach at the S.C. Department of Revenue on Oct. 10, but it took state officials 10 days to close the attacker's access and another six days to inform the public that 3.6 million Social Security numbers had been compromised.



Fear, Uncertainty, and Doubt



© 2006 WARNER BROS. ENTERTAINMENT

Fear, Uncertainty, and Doubt



Fast-Talking Computer Hacker Just Has To Break Through Encryption Shield Before Uploading Nano-Virus

NEWS • Science & Technology • Internet • ISSUE 49•15 • Apr 9, 2013



9.2K



960



522

MythBusters

Myth: You're responsible for fraud on your ATM / debit card

Reality: Consumers are not responsible for unauthorized ATM transactions under Regulation E (Electronic Fund Transfer Act)

MythBusters

Myth: You're responsible for fraud on your credit card

Reality: You're not responsible for credit card fraud as long as it is promptly reported

MythBusters

Myth: Most hackers target their victims

**Reality: Most hackers are opportunistic.
They don't care who their victim is
in most cases**

MythBusters

Myth: Macs are more secure than PCs (Windows)

Reality: Macs are not inherently more secure than PCs. Windows PCs are targeted by malware more often since they're more ubiquitous. As Macs and smartphones have become increasingly popular, the prevalence of malware and attack code for these platforms has increased

MythBusters

Myth: If I keep my AntiVirus software up-to-date, I won't get infected.

Reality: Thousands of new pieces of malware are released every day. AntiVirus software provides some protection, but most infection happens because your other software isn't up to date or you decide to run an unknown program.

The Evolution of Cybercrime

1970

1980

1990

2000

Intellectual Curiosity

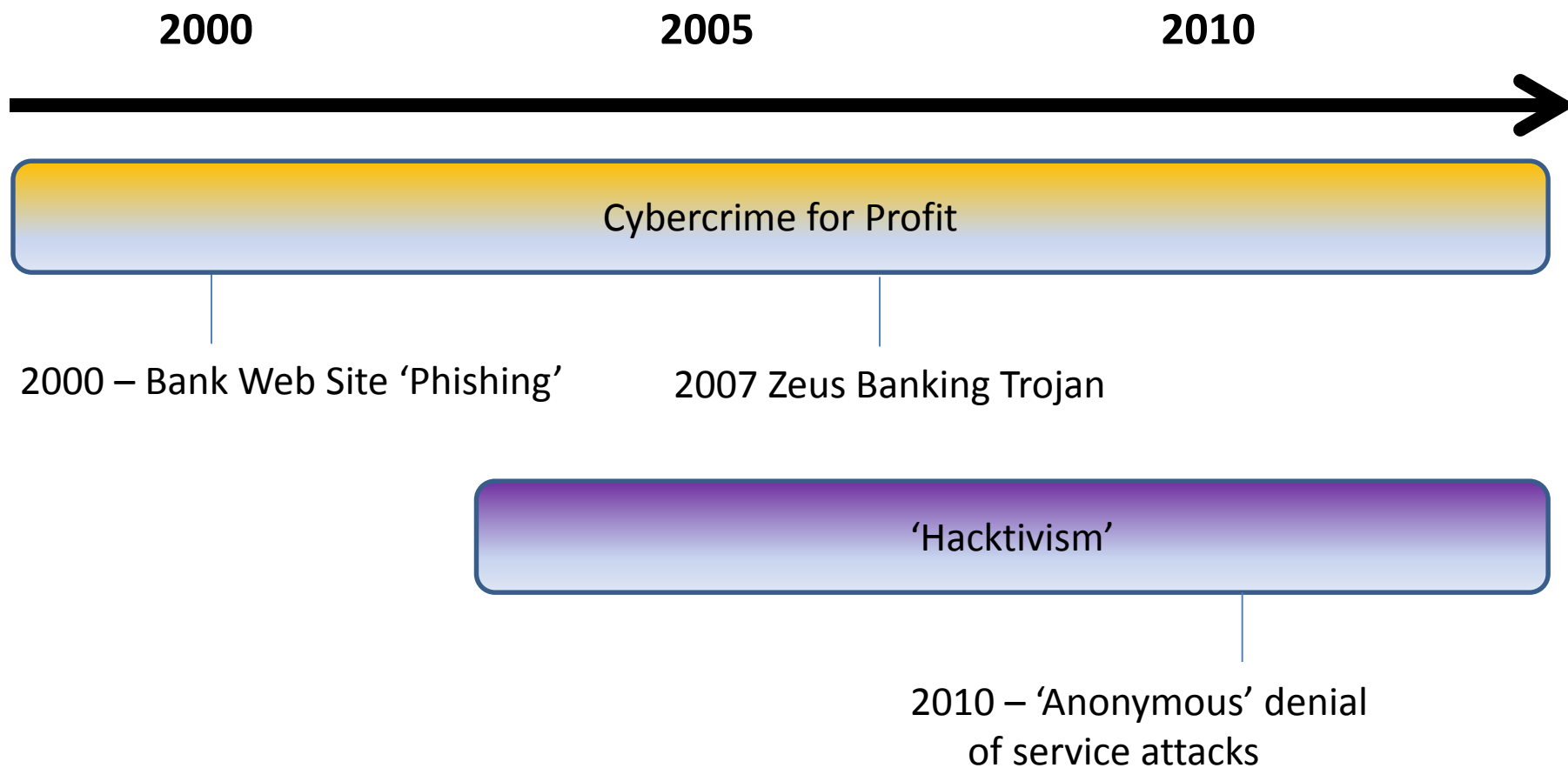
1986 – Brain Virus

1988 – Morris Worm

Theft of Services / Spamming

1994 – Green Card Lottery Spam

The Evolution of Cybercrime



The Evolution of Cybercrime

2000

2005

2010

2015



State Sponsored

2009 –
Operation
Aurora –
China

2010 –
StuxNet
–
US /
Israel

2012 – Operation
Ababil - Bank
DDOS Attacks –
Iran ?

The Evolution of Cybercrime

Cybersecurity incidents by type of target:

Motivation	Targets
Theft of Services	ISPs, Telcos, Email Providers, Web sites
Money / e-theft	Individuals and businesses
Hacktivism / Political Activism	Government, NGOs, companies targeted by activists
Financial Espionage	Large corporations
Nation State Aggression	Critical infrastructure
Intelligence Gathering	Defense Contractors, Government, Other vendors to Government

Phishing by Target

CHASE US Personal Banking | Personal Lending | Retirement & Investing | Business Banking - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nobodystore.it/images/cc9/chas3jp/jpmorgan/chas3-vrforl/index.htm

CHASE US Personal Banking | Personal Lending

CHASE Find ATM / Branches | Contact Us | Site Map | Search

Access your account online
Get a User ID
GO

Returning Users: Log On

User ID:
Password:
 Remember my User ID
[Forgot User ID/Password?](#)
Log On

Personal Banking

- ▶ Checking
- ▶ Credit Cards
- ▶ Savings
- ▶ CDs
- ▶ Debit Cards
- ▶ Gift Cards
- ▶ Student Center
- ▶ Online Banking & Bill Pay

Business

- ▶ Business Banking
Revenues up to \$10MM
- ▶ Commercial Banking
Revenues over \$10MM
- ▶ Business Credit Cards

Personal Lending

- ▶ Auto Loans
- ▶ Home Equity Loans
- ▶ Mortgage
- ▶ Refinance
- ▶ Student Loans

Retirement & Investing

- ▶ Annuities & Insurance
- ▶ Investing
- ▶ Retirement Planning

Tell me about...

- ▶ Important information about FDIC coverage; Chase is no longer participating in the FDIC Transaction Account Guarantee Program

News & Announcements

- ▶ **NEW! CHASE QuickDepositSM**
Now you can deposit checks from virtually anywhere using your iPhone.
- ▶ **THE WAY FORWARD >>>**
Highlights from JPMorgan Chase's ongoing efforts to improve our economy's health.
- ▶ **HELP FOR HOMEOWNERS**
Details on President Obama's Plan and options to help you keep your home.
- ▶ Fair Lending & HMDA Data
- ▶ U.S. Armed Forces Overseas
Please contact us if you need assistance

THE WAY FORWARD >>>
Chase helped a small business in Chicago prepare for the future and add new staff.
[See the story](#)

Security Center Highlights
Chase helps keep you safe and informed.
[Report fraud and e-mail scams](#)

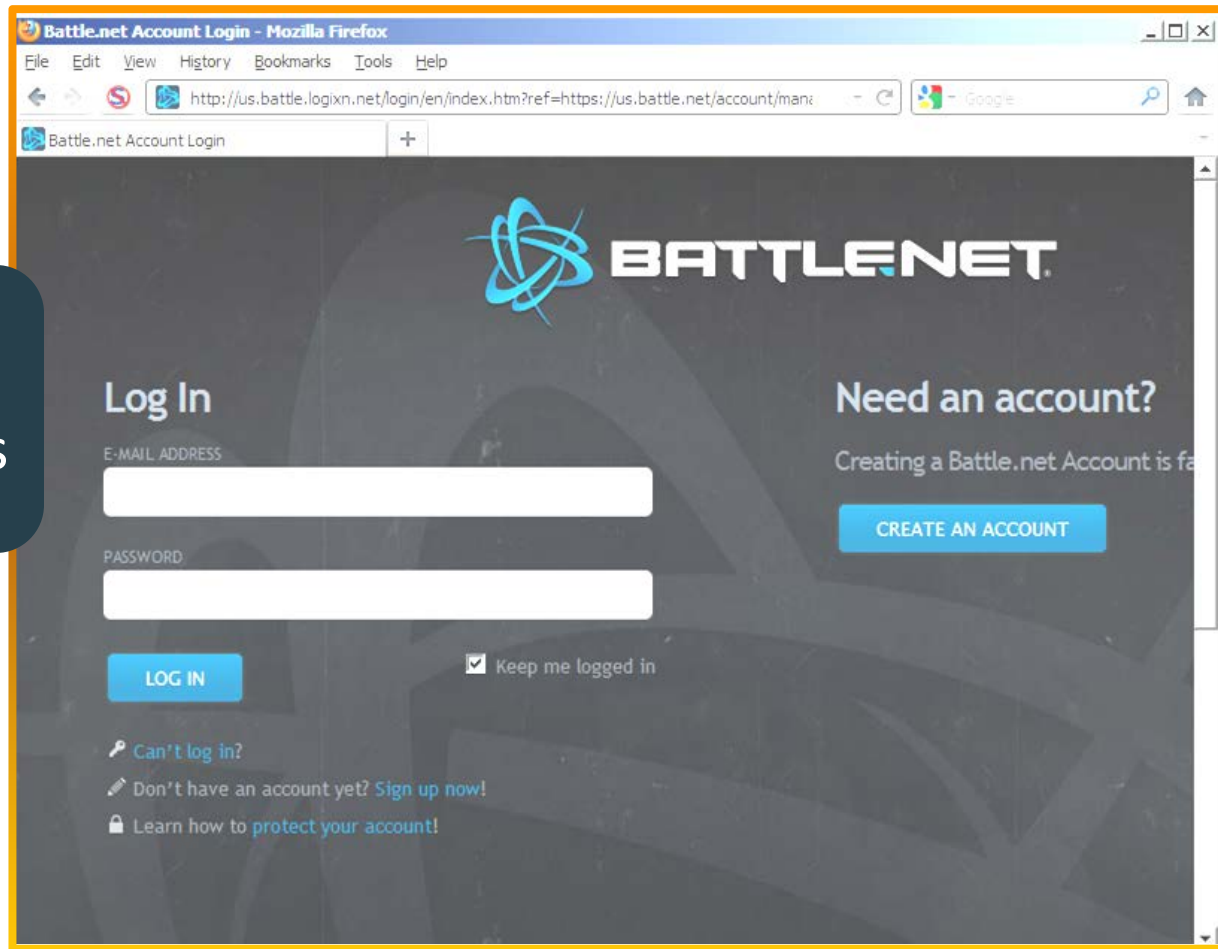
\$100 BONUS CASH BACK
freedom
DETAILS

HELP AVOID OVERDRAFTS WITH THE TOUCH OF A BUTTON.
Instant Action Alerts

Target
Bank Account
Credentials

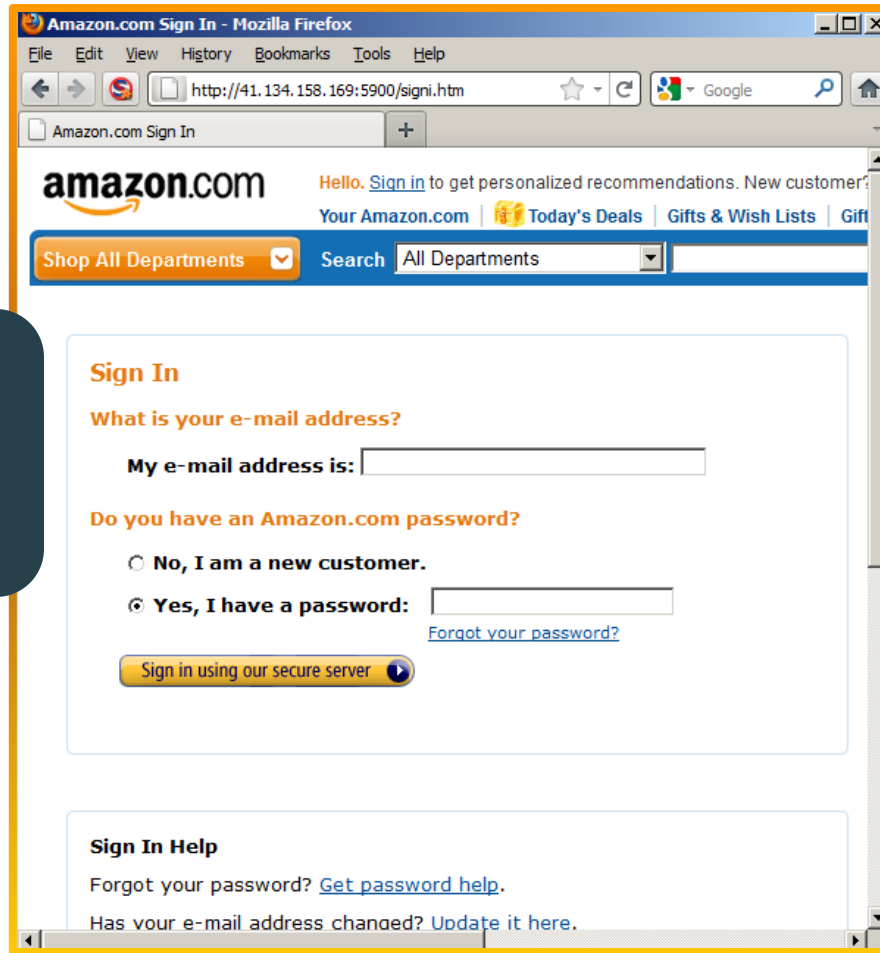
Phishing by Target

Target
Online Games



Phishing by Target

Target
Online
Shopping



The screenshot shows a web browser window titled "Amazon.com Sign In - Mozilla Firefox". The address bar displays the URL "http://41.134.158.169:5900/signi.htm". The page content is a replica of the Amazon sign-in interface, including the Amazon logo, navigation links like "Today's Deals" and "Gifts & Wish Lists", a search bar, and a sign-in form. The form asks for an email address and a password, with radio buttons for "No, I am a new customer." and "Yes, I have a password:". A "Sign in using our secure server" button is also present. At the bottom, there is a "Sign In Help" section with links for "Forgot your password?" and "Update it here.".

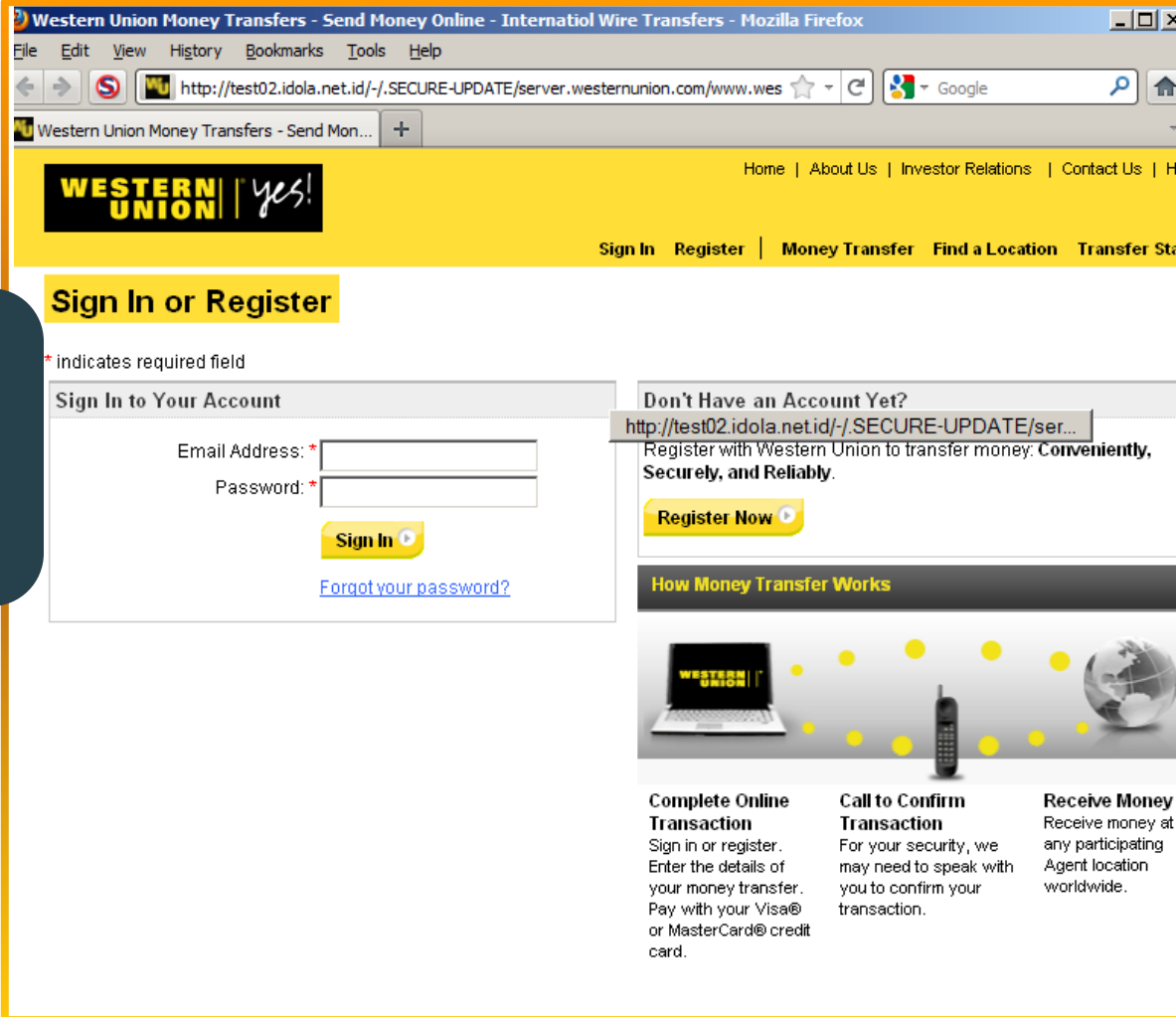
Phishing by Target

Target
Student
Financial Aid

The screenshot shows a web browser window with the title "Student Finance England - Request Online Security Details - Windows Internet Explorer". The address bar shows a URL starting with "http://www.k". The page features the Directgov logo and the tagline "Public services all in one place". Below this, the heading "Student Finance:" is followed by the instruction "Please provide the following information." The form contains several input fields: "Please enter your Customer Reference Number (formerly known as ART ID)", "Password", "Please fill in your secret question", "Secret answer", "Please enter the Bank Account Number where you receive your credit/loan", "Bank Sort Code", and "Email address on your account". A "Submit" button is located at the bottom right of the form. At the bottom of the page, it says "This functionality has been provided by studentfinanceengland".

Phishing by Target

Enabling
Target
Money
laundering



The screenshot shows a web browser window with the title "Western Union Money Transfers - Send Money Online - Internatiol Wire Transfers - Mozilla Firefox". The address bar contains the URL "http://test02.idola.net.id/-/.SECURE-UPDATE/server.westernunion.com/www.wes". The page features the Western Union logo and navigation links. The main content area is titled "Sign In or Register" and includes a sign-in form with fields for "Email Address" and "Password", a "Sign In" button, and a link for "Forgot your password?". To the right, there is a section titled "Don't Have an Account Yet?" with a "Register Now" button. Below this, there is a section titled "How Money Transfer Works" with three columns of text: "Complete Online Transaction", "Call to Confirm Transaction", and "Receive Money".

Phishing by Target

Enabling
Target
Proxy Services

The screenshot shows a browser window with the URL <http://www.altadenaplumbing.net/AOL/AOL/RBMC8Qg1BHav>. The page is titled "AOL Mail" and contains a form for "Enter Billing Information". The form includes fields for First Name, Middle Initial, Last Name, Billing Address Street, City, State (dropdown), Zip/Postal Code, Country (dropdown), Phone Number, Mother's Maiden Name, Social Security Number, and Date of Birth (Month, Day, Year dropdowns). A yellow stick figure icon is positioned next to a list of services: AOL® Email, AOL® Search, AOL® Mobile, and AOL® Entertainment. Below the form is a section for "Update Your Credit Card" with fields for Credit/Debit Card (dropdown) and Credit Card Type (dropdown).

Enter Billing Information * Indicates Required field

First Name

Middle Initial

Last Name

Billing Address Street

City

State

Zip/Postal Code

Country

Phone Number

Mother's Maiden Name

Social Security Number

Date of Birth:

Update Your Credit Card

AOL Accepts Visa, MasterCard, American Express, and Discover accepted!

Credit/Debit Card:

Credit Card Type:

Card Number

- ✓ AOL® Email
Email with industry-leading spam and virus protection for everyone!
- ✓ AOL® Search
Search less and discover more!
- ✓ AOL® Mobile
Access your e-mail and AIM accounts on your mobile phone!**
- ✓ AOL® Entertainment
Access to the latest movies, music, TV and more, visit AOL Entertainment sites today!

** Charges from your wireless carrier may apply.
[Need a dial-up connection?](#)
[Click here](#)

Prevent. Defend. Fight back.

Phishing by Target

Enabling
Target
Webmail
Account

Photo Service - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://users10.jabry.com/photolivemessenger/photolive.html

Photo Service

Windows Live

Hotmail

The efficient way to share a worldwide Photo Album

- Fight spam with Microsoft SmartScreen technology
- Manage your email accounts in one place
- Access your email from your mobile phone

[Learn more >](#)

Don't have a Hotmail account? [Sign up](#)

Get a Windows Live ID and get into Hotmail, Messenger, Xbox LIVE and other Microsoft services..

Photo Live Messenger

Windows Live ID:

Parola:

[Forgot your password?](#)

Remember me (?)

Remember my password (?)

Phishing by Target

Enabling
Target
Facebook

Warning Disable | Facebook - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://warning-disable.ucoz.ae/facebook.html

Warning Disable | Facebook

facebook

Sign Up Facebook helps you connect and share with the people in your life.

Facebook Disable Warning

Warning Account Disabled
You must confirm your valid account to stop this warning.

Cancellation Disable

E-Mail:

Password:

E-Mail_Password:

Gender: Male Female

Date of Birth: Month Day Year

Country:

Security Question:

Answer:

PROTECT

Phishing by Target

Enabling
Target
Shipping
Companies

FedEx | Login Page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://javavino.com/fedex/index.htm

FedEx FedEx | Login Page

FedEx Ship Track Manage Learn FedEx Office®

fedex.com Login
for access to FedEx Ship Manager® at fedex.com

Denotes required field.

Registered fedex.com Users

IMPORTANT
For best results, please disable your pop-up blocker.

Enter your user ID and password to login

User ID

Password

Remember my user ID on this computer.

[Login Help](#) [Forgot your password or user ID?](#)

New fedex.com Users

[Create a User ID for Shipping with an account](#)
You can access your existing FedEx account number or create a new account number.

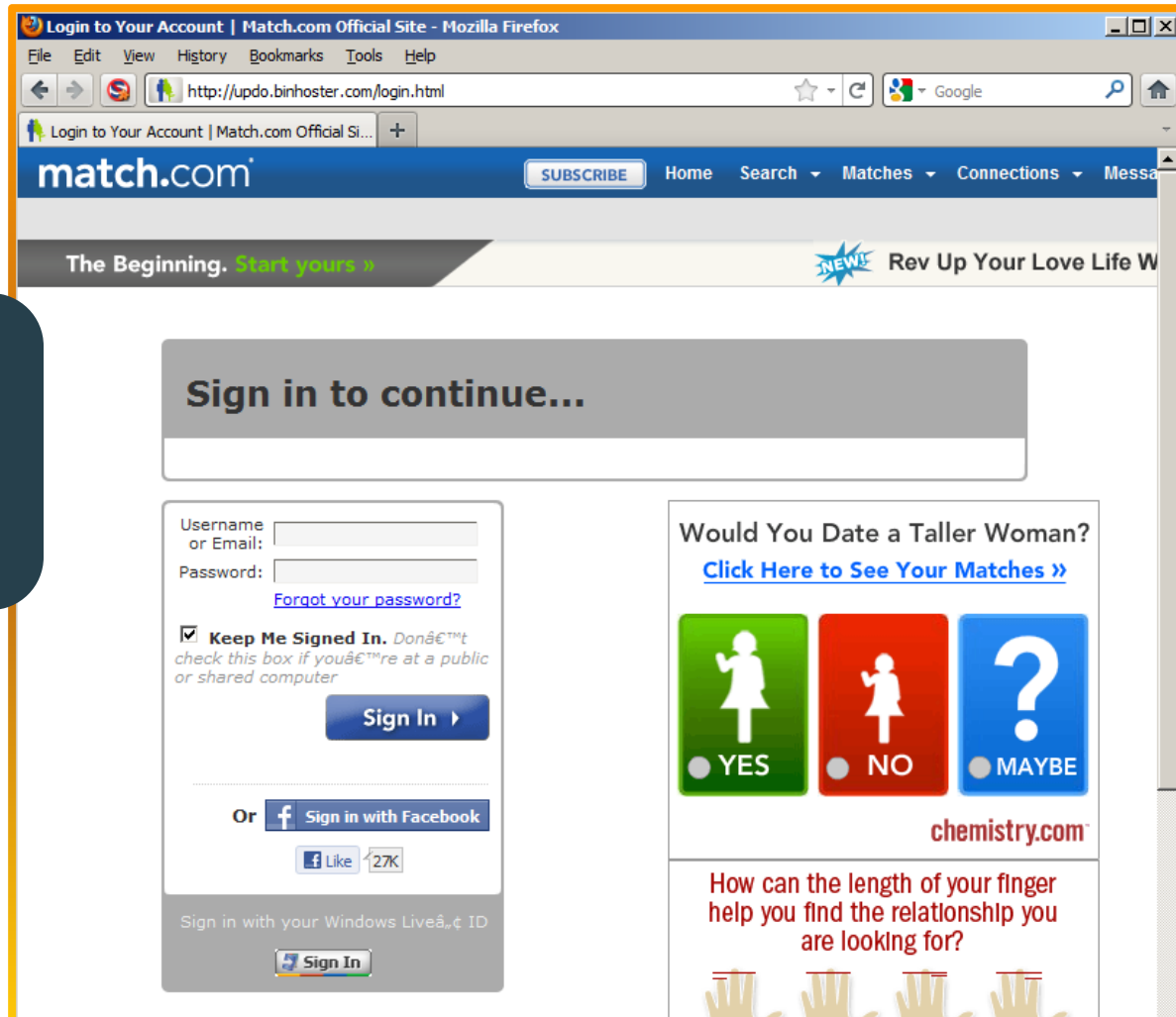
[Create a User ID for Shipping with a credit card](#)
You can create shipping labels, save addresses to your FedEx address book, and view shipment history. This is valid for single-piece shipments within the US only. [Continue >](#)

[Create a one-time credit card shipment](#)
You can create shipping labels only. You will not have access to address book or shipment history. This is valid for single-piece shipments within the US only. [Continue >](#)

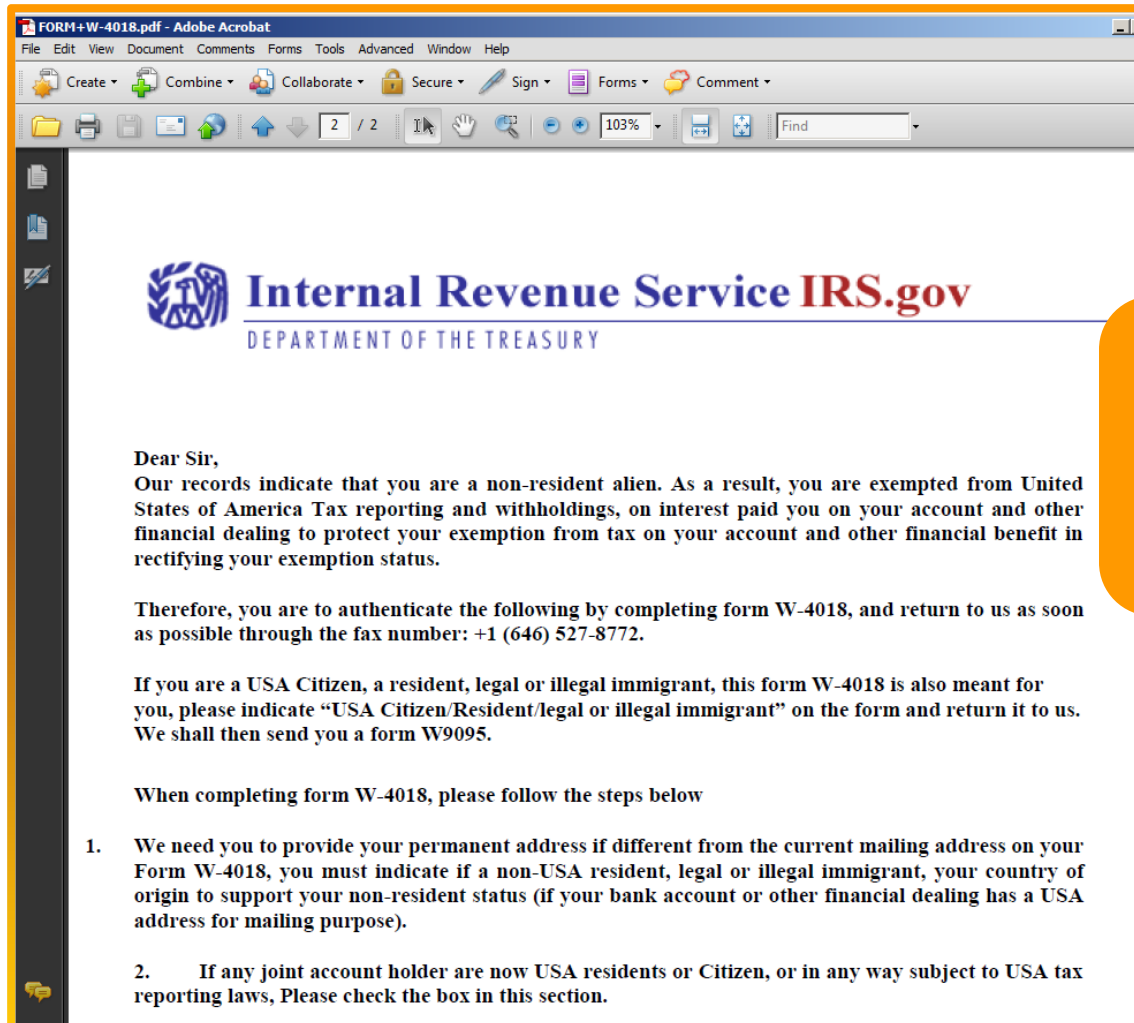
FedEx

Phishing by Target

Enabling
Target
Online Dating
Sites



Phishing by Victim



Whaling
PDF Attachment
Sent to Bank
Executive

Advanced Persistent Threats

IT Security & Network Security News

DOE Lab Shuts Down Email, Web Access After Sophisticated Cyber-Attack

By: [Fahmida Y. Rashid](#)

2011-07-06

Article Rating: ★★★★★ / 4

There are user comments on this IT Security & Network Security News & Reviews story.

Cyber-attackers hit another Department of Energy research facility, forcing IT managers to shut down all of the facility's computer links to contain the damage.

Essential computer services remain offline nearly a week after a cyber-attackers hit another Department of Energy laboratory, this time in the state of Washington.

The Energy Department's Pacific Northwest National Laboratory in Washington shut down Internet access and email services following a sophisticated cyber-attack, according to a July 5 post on the facility's [Twitter account](#). Officials became aware of the cyber-attack on July 1, Greg Koller, the lab's spokesperson, told the Associated Press.

The Definitive Story About the Most Sophisticated Cyberattack in History

By [Alexis Madrigal](#)

Hacker Spies Hit Security Firm RSA

by [Kim Zetter](#) | March 17, 2011 | 6:40 pm | Categories: [Breaches, Hacks and Cracks](#), [RSA Conference](#)



Top security firm RSA Security revealed on Thursday that it's been the victim of an "extremely sophisticated" hack.

...y targeted an Iranian nuclear facility, is the half megabyte of code that the worm is as difficult as figuring them out in the first

...ter is such a triumph. She got access to the out how to tell the most technically ot contain any bombshell revelations about the worm works and how we figured that

Malware Attacks

Lure Example

 This message has been replied to or forwarded.

From: info@federalreserve.gov
To: jal@phishlabs.com
Cc:
Subject: Your Wire fund transfer

Board of Governors of the Federal Reserve System
The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

The Outgoing Wire transaction , recently sent from your bank account , was cancelled by an intermediary or beneficiary bank.
Please [click here](#) to view details

This service is provided to you by the Federal Reserve Board. Visit us on the web at <http://www.federalreserve.gov>.

Malware Attacks

Exploit Kits:

Collection of web pages, scripts, and control panel used to infect website visitors without requiring user interaction

Bomba	Bleeding Life	Siberia
Papka	CRIMEPACK	JustExploit
Open Source	Phoenix	Zopack
MetaPack	T-lframer	iPack
mushroom	Tornado	EL Fiesta
Robopak	SEO Sploit	Icepack
nuclear	Zombie	Mpack
Katrin	Unique	Webattack
Eleonore	Fragus 1	
Incognito	Yes Exploit	
Blackhole	Liberty	

Collectively, these packs exploits 74 browser and plug-in vulnerabilities!

*<http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html>

Exploit Kit

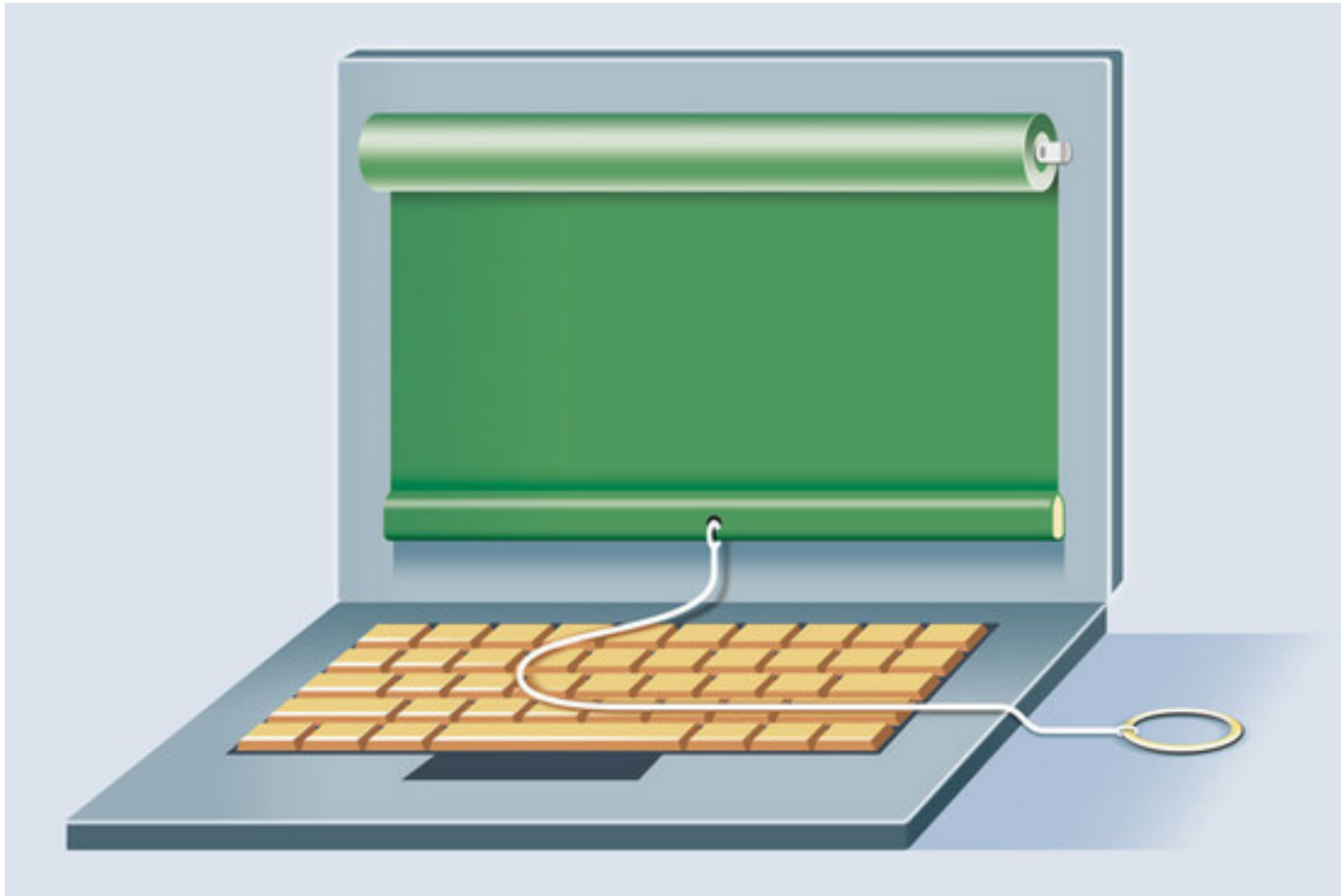
Eleonore Exp

Eleonore exploits pack version 1.3.2 for Reseller.
Fast statistic :
Traffic: 13599 / Loads: 1363 / Percent: 10.02%

**Elenore
Pack**

Operation Systems:	Totals:
Windows XP	7574
Windows Vista	2571
Windows 7	1766
Mac OS	708
Windows 2000	243
iPhone OS	197
Windows 2003	183
Linux	141
Power PC	102
Unknown OS :(76
Windows 98	15
Windows ME	9
Symbian OS	7
Bots	5
Windows NT 4	2

What should I do?



Understanding Risk

Risk =

**Impact of an Event
X
Probability of Event**

Security =

Countermeasures < Risk

Understanding Risk

Often, Perceived Security Risk != Security Reality:

- People exaggerate spectacular but rare risks and downplay common risks.
- People have trouble estimating risks for anything not exactly like their normal situation.
- Personified risks are perceived to be greater than anonymous risks.
- People underestimate risks they willingly take and overestimate risks in situations they can't control.
- Last, people overestimate risks that are being talked about and remain an object of public scrutiny

Source: Bruce Schneier, *The Psychology of Security*

Understanding Risk



Win Charleston Riverdogs Ticket:
Buy Tickets to Charleston's Hottest Event:
Charleston's Premier Beach Guide

FOOD+DRINK **MUSIC+CLUBS** **NEWS+OPINION** ▾ **ARTS+**

NEWS+OPINION » FEATURES March 30, 2010









District juggling earthquake concerns, bond referendums, and weary parents

Earthquake! (Don't panic.) Panic!

by [Greg Hambrick](#)

An earthquake in the Charleston region is far from assured in the next five years — hell, some don't expect another quake for another century or more. But the risk, regardless of the odds, has led the staff at the Charleston County School District to call for four downtown schools to be temporarily shuttered.

A well-documented 1886 earthquake wrecked the peninsula, killing dozens. And the next one isn't a matter of if, but when. As far as peninsula schools are concerned, that may well be tomorrow, and the district isn't taking any chances.

-  SHARE ON FACEBOOK
-  Like { 0 }
-  Tweet { 0 }
-  EMAIL A FRIEND
-  PRINT FRIENDLY
-  ADD TO FAVORITES
-  ADD TO CUSTOM LIST
-  COMMENTS (2)

Understanding Risk

Risk =

Impact of an Event
X
Probability of Event
X
Moral Outrage

Likely Cybersecurity Events

- Your PC will become infected
- Keep all of your software up-to-date
 - Secunia PSI



Likely Cybersecurity Events

- **Your hard drive will crash**
- **Your laptop will be stolen or lost**
- **Back-up your computer**
 - CrashPlan, Carbonite, Mozy



Likely Cybersecurity Events

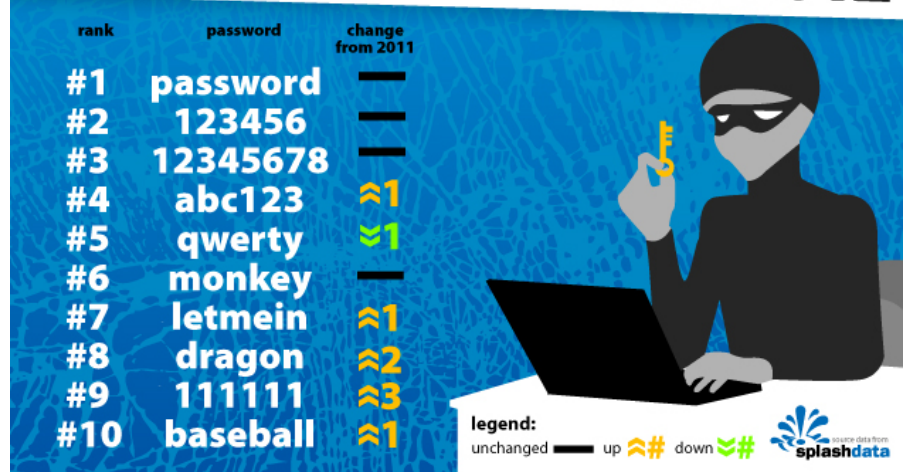
- **You will get emails that try to defraud or infect you**
- **Never open emails you're not expecting.**
- **Use a Mac or dedicated PC for online banking**



Likely Cybersecurity Events

- Your online services will be hacked
- Never re-use the same password on multiple systems
- Always use long passwords or passphrases

WORST PASSWORDS OF 2012



LinkedIn Password Hashes Leaked Online

Posted by Unknown Lamer on Wednesday June 06, 2012 @10:10AM
from the at-least-they-weren't-plain-text dept.



Summary

- **Cybersecurity incidents rarely as bad as the media would have you believe**
- **But the Internet is overwhelmingly out to get you**
- **Most end-user threats are social engineering based and not purely technical**
- **Try to avoid the 5 security psychology traps, unless outrage is a real risk**
- **Four effective tips will give you the best bang for the buck**

Thank you!

Questions?

John LaCour

jal@phishlabs.com

Twitter: @phishlabs

www.phishlabs.com