# Data Protection and Cyber Threats:
## *Personal and Business Data at Severe Risk*

**Steve Cocco**
**President - Security Strategies Today**

Steve Cocco is a counterterrorism, business continuity and homeland security threat consultant.

Steve served with distinction in the FBI as a Special Agent and executive manager for nearly three decades, during which time he specialized in vulnerability and threat assessments affecting large public venues, such as hotels, conference halls and sports arenas.

# Data Protection and Cyber Threats:
## *Personal and Business Data at Severe Risk*

Presented by Steve Cocco, President,
Security Strategies Today

Global Conference On Travel Risk Management
Houston, Texas
October 13-14, 2014

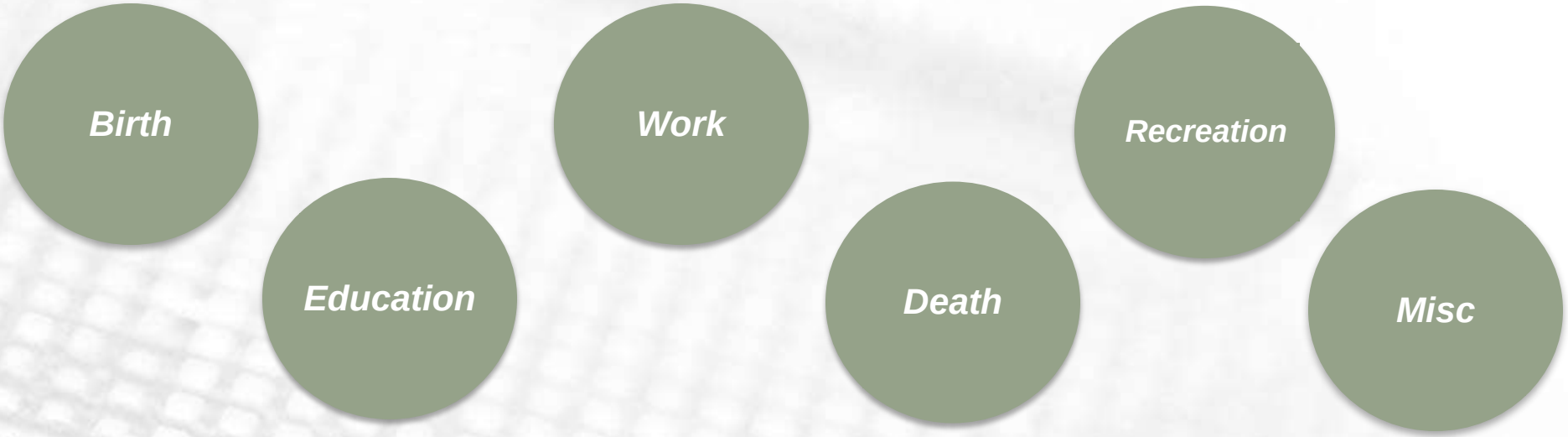
8 key personal identifiers

(These are the keys to the castle for a cyber criminal)

Name, DoB, PoB,
SSAN, DL#, Address,
Passport Number,
Birth Certificate

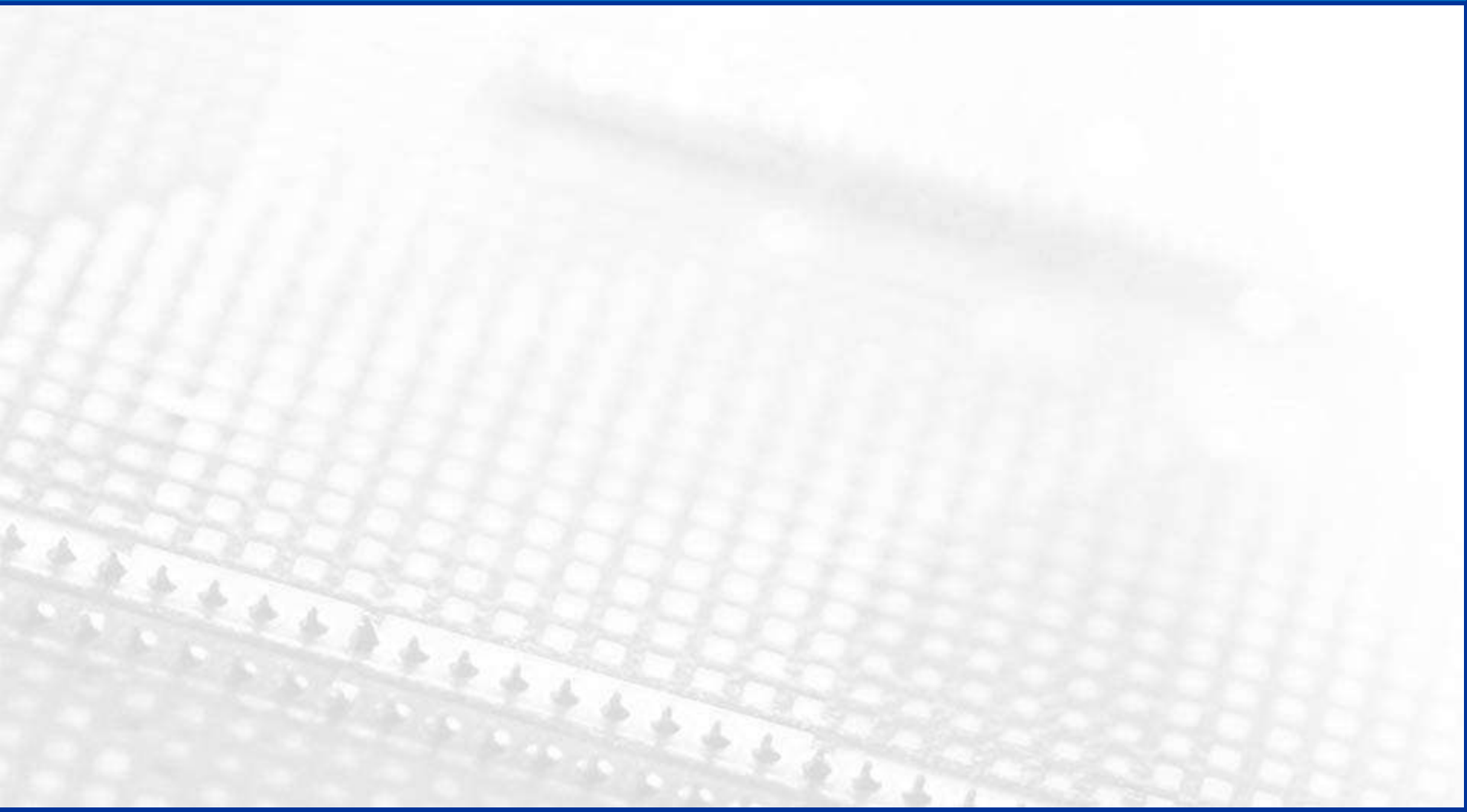
Physical

Virtual


Birth
Education
Work
Death
Recreation
Misc

# What are the Most Common Places to Locate Personal Data and Exfiltrate it?

- ✓ Search Engines
- ✓ Directories
- ✓ Social Networking




YAHOO!


twitter


D&B


ChoicePoint


INTELIUS
Live in the know.™


Ask
.com


ebay


ZABASEARCH


YouTube


bebo


zoominfo
People, Companies, Relationships


craigslist


myspace.com


RapLeaf


cuil


facebook


amazon.com


Live Search


pipl


gaia
ONLINE


Google


LexisNexis®


WORLD
WARCRAFT


hi5

# Two Types of Cyber Crime

- Traditional crime migrated to Internet

- Non-Traditional activity that was not a concern prior to the Internet

# Why Criminals Use Computers

- Anonymous
- Ease of contacting victims
- Find possible accomplices
- Efficient communication to plan crime

# Street Price of Stolen Identification Items

| Item | Percentage | Price |
|---|---|---|
| Bank Account Number | 23% | $10 -$1,000 |
| Credit Card Number | 13% | $0.40 - $2.00 |
| Full Identity | 9% | $1 - $15 |
| Online Auction Account | 7% | $1 - $8 |
| Email Addresses | 5% | $0.83/MB - $10/MB |
| Email Passwords | 5% | $4 - $30 |

Some Improvements Have Been Made in Recent Years in Document Security…….

-the addition of biometric characteristics;

-the addition of certain dyes and threads in documents that are difficult to replicate;


UNIONE EUROPEA
REPUBBLICA ITALIANA
PASSAPORTO


NEW DRIVER LICENSE
CALIFORNIA
DRIVER LICENSE
DL I1234568
EXP 08/31/2015
LN CARDHOLDER
FN IMA
2570 24TH STREET
SACRAMENTO, CA 95818
DOB 08/31/1977
RSTR NONE
CLASS C
END NONE
SEX F
HAIR BRN
EYES BRN
HGT 5'-05"
WGT 125 lb
DD
ISS
09/30/2010
TACTILE, LASER ENGRAVED SIGNATURE
CALIFORNIA BROWN BEAR
COLOR UV IMAGES

# Can You Hide?

If you find information about yourself you need to

"Opt Out"

Public Records

- Property & Utility
- Telephones
- Voter registration
- Vehicles & DLs
- Lawsuits
- Judgments
- Warranty cards
- Credit cards
- Cell phones
- Websites & media captures
- Photographs
- Liens/Loans

Conduct a search for your name using search engines to determine what is our there. Contact appropriate entities to rectify/delete erroneous information.

| | |
|---|---|
| Bulkdatabase.com | searchsystems.net |
| Melissadata.com | Myfamily.com |
| Peoplefinders.com | ancestry.com |

Search these in addition to Google, Yahoo

The problem is that “Opting Out” is not that easy, especially when retailers and other businesses sell or make their customer databases available to other entities.

In the European Union, retailers, banks, credit card companies are prohibited from provided customer data to other companies without the permission of the individual whose data is held.

The new EU “right to be forgotten” law mandating removal from the internet of erroneous or old data is unworkable, untenable.

# The Downside

1. Can affect credit rating
2. Almost impossible to completely disappear

Do what is reasonable; recognize you are findable

"***Security through obscurity is no security at all***"

# SPAM

Unsolicited Commercial Email

Represents **40%** of Internet Traffic

# Identity Theft

## Identity Theft: Annual Losses in Excess of $50 billion

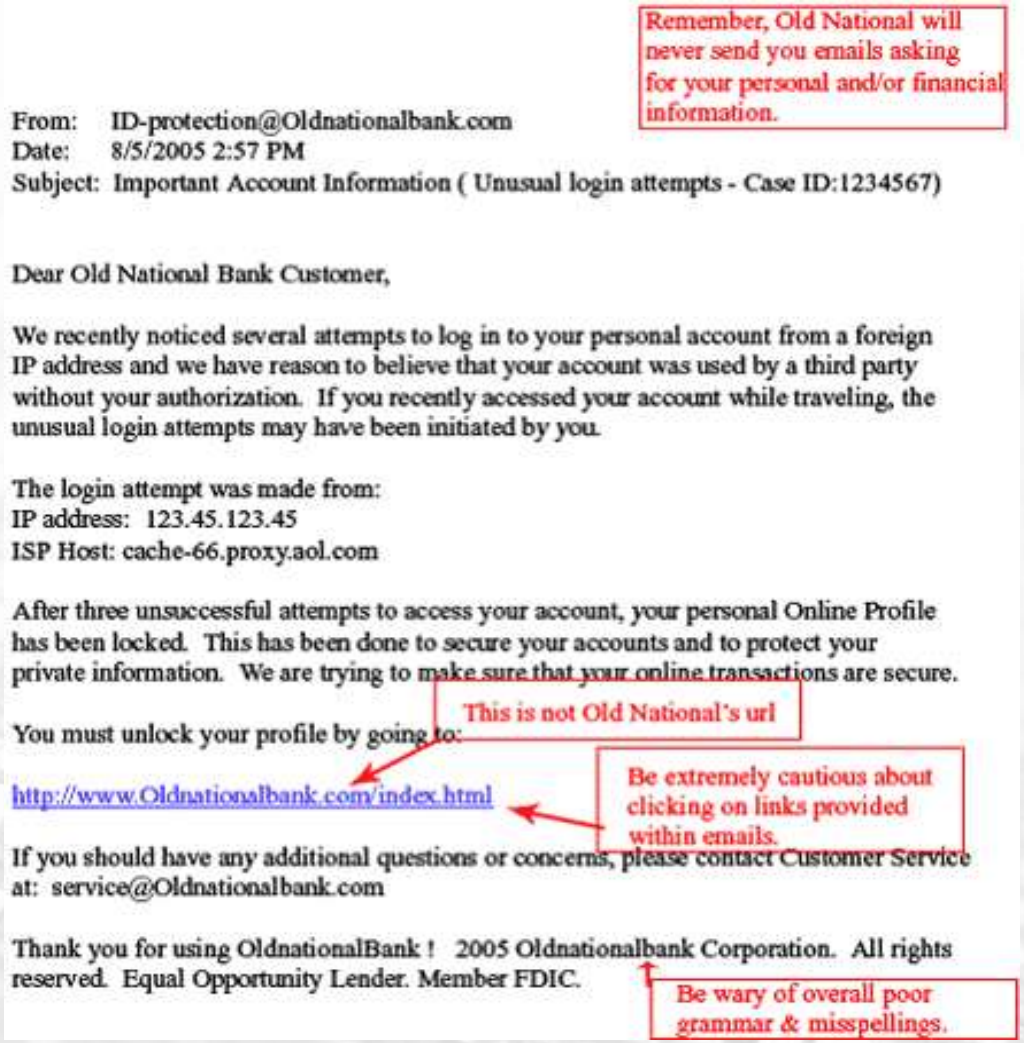
By Cyber Security Market

According to the Federal Trade Commission (FTC) estimates in 1 year, as many as 10 million people discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion.

A recent report of Market Research Media U.S. Federal Cybersecurity Market Forecast 2010-2015 predicts that the Federal government will spend $55 billion over the next five years to fight cyber crime.

The loss of personally identifiable information, such as an individual′s Social Security number, name, and date of birth can result in serious harm, including identity theft. Identity theft is a serious crime that impacts millions of individuals each year. Identity theft occurs when such information is used without authorization to commit fraud or other crimes. While progress has been made protecting personally identifiable information in the public and private sectors, challenges remain.

# Phishing Attacks



Remember, Old National will never send you emails asking for your personal and/or financial information.

From: ID-protection@Oldnationalbank.com
Date: 8/5/2005 2:57 PM
Subject: Important Account Information ( Unusual login attempts - Case ID:1234567)

Dear Old National Bank Customer,

We recently noticed several attempts to log in to your personal account from a foreign IP address and we have reason to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you.

The login attempt was made from:
IP address: 123.45.123.45
ISP Host: cache-66.proxy.aol.com

After three unsuccessful attempts to access your account, your personal Online Profile has been locked. This has been done to secure your accounts and to protect your private information. We are trying to make sure that your online transactions are secure.

This is not Old National's url

You must unlock your profile by going to:

http://www.Oldnationalbank.com/index.html

Be extremely cautious about clicking on links provided within emails.

If you should have any additional questions or concerns, please contact Customer Service at: service@Oldnationalbank.com

Thank you for using OldnationalBank ! 2005 Oldnationalbank Corporation. All rights reserved. Equal Opportunity Lender. Member FDIC.

Be wary of overall poor grammar & misspellings.

# Spear Phishing - Law Enforcement Targeted

E-mail spoofing fraud attempt that targets a specific person

Seeks unauthorized access to confidential data

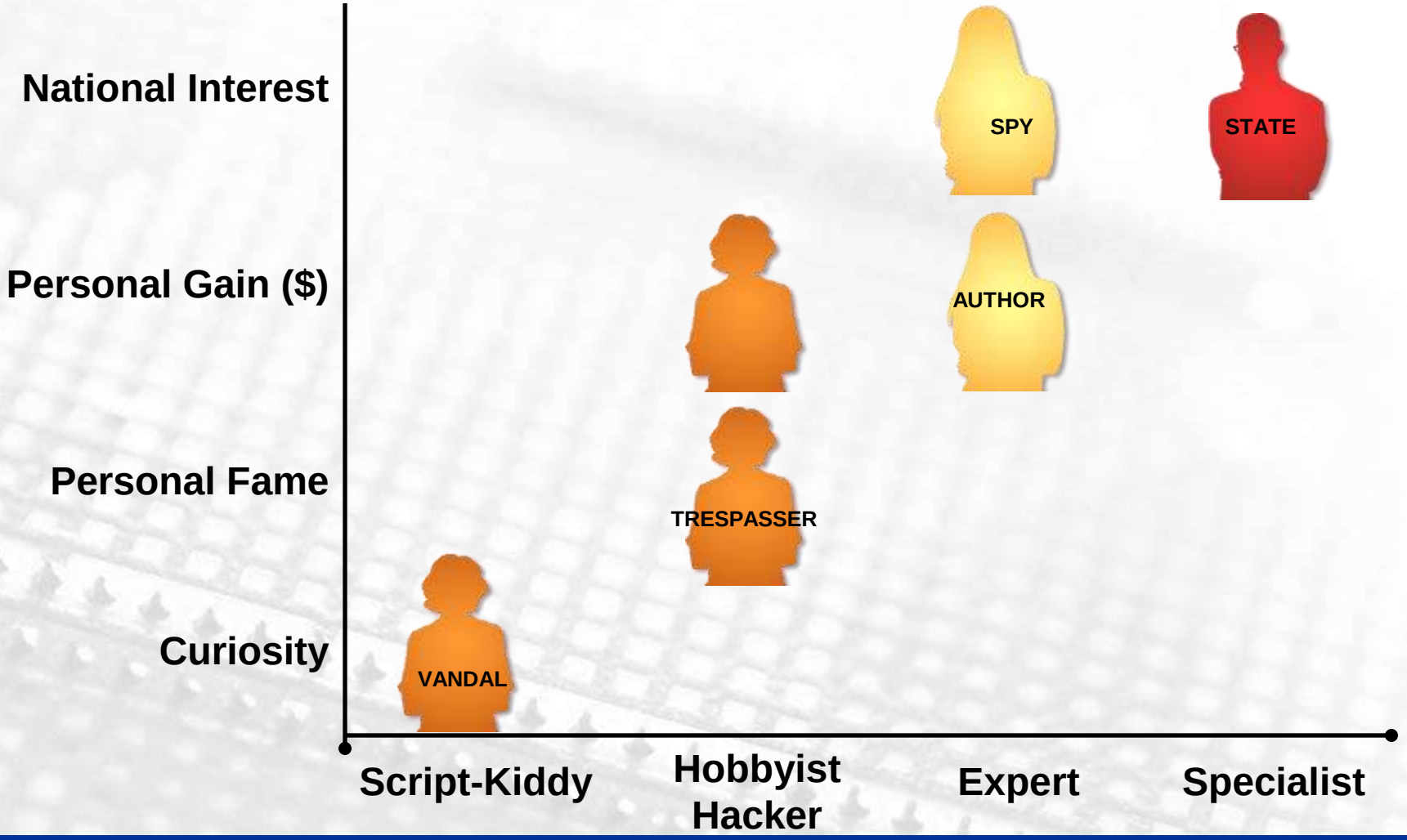
Attempts are NOT by random hackers

Perpetrators after financial gain, trade secrets, military info, etc.

# Skimming

# The Hacker

# Who Are The Hackers?



# How They Find You

1-480-555-1234

24.88.107.246

# Reality of Breaches

- 30% Cyber
- 70% Insider Threat
- 1 in 8 employees pose high level of risk

- Answer: RISK PREPAREDNESS AND EMPLOYEE AWARENESS EDUCATION !!!

# Protecting your Computer

# Hostile Sites

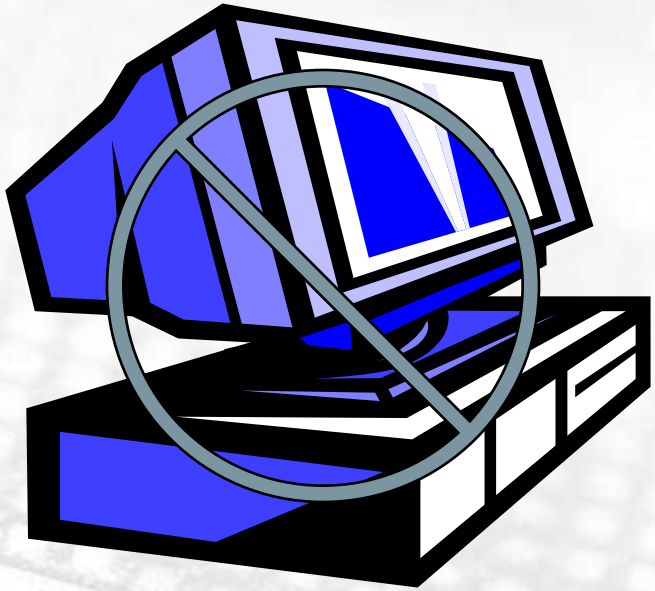
1. Visit site with hostile elements
2. Site attacks your computer
3. Computer gives up private or sensitive info

# Ransomware

1. Malware installed on computer
2. Victim contacted by hacker
3. Hacker provides decryption key upon payment

# Denial of Service

- Interrupts business computer service by continually sending phony authentication messages to targeted server
  - keeping it constantly busy
  - blocks legitimate users



# Spoofing

- Creates false copy of a reputable web site
- Victim connects to attacker′s web site
- Attacker acquires passwords, credit cards

# Safe Surfing 1 – Protecting Work and Home

- Install good anti-virus software
- Install reputable anti-spyware, scan weekly
- Install a good firewall
- Wireless:  Password – Don't be just "out there"
- Use strong **passwords** on your computer (12+ characters)
  - Example **300plus400=700**
- Never link to a site from an email, even a trusted source
- Never browse to unknown sites when logged in as administrator
- Avoid P2P and IRC files shares with anyone you don't know well.  Better yet, don't do it at all

# Defense in Depth

- Cable Modem with firmware firewall
- Fully patched Operating System
- Router (wireless running WPA-2)
- Firewall
- Anti-virus
- Intrusion detection system (IDS)
- Daily back-up to external drive
- ERUNT running in background
- Sandbox

# Safe Surfing 2

- Don't give out personal or financial information unless you are sure with whom you are communicating
- Use your ISP's anti-spam filters in your email
- Don't download ANY software without knowing exactly what it is and what it does
- Never click on an email attachment without first scanning it with an anti-virus application
- Turn OFF the preview pane in your email client
- Keep your computer up to date
- Back up, Back up, Back up
- It is not a matter of IF your computer will have problems, it is a matter of WHEN!

*Thanks For Your Attention*