

Online Threats for 2010 and Beyond

**Presented by:
James Brooks
August 30, 2010**

Overview

Latest threats explained

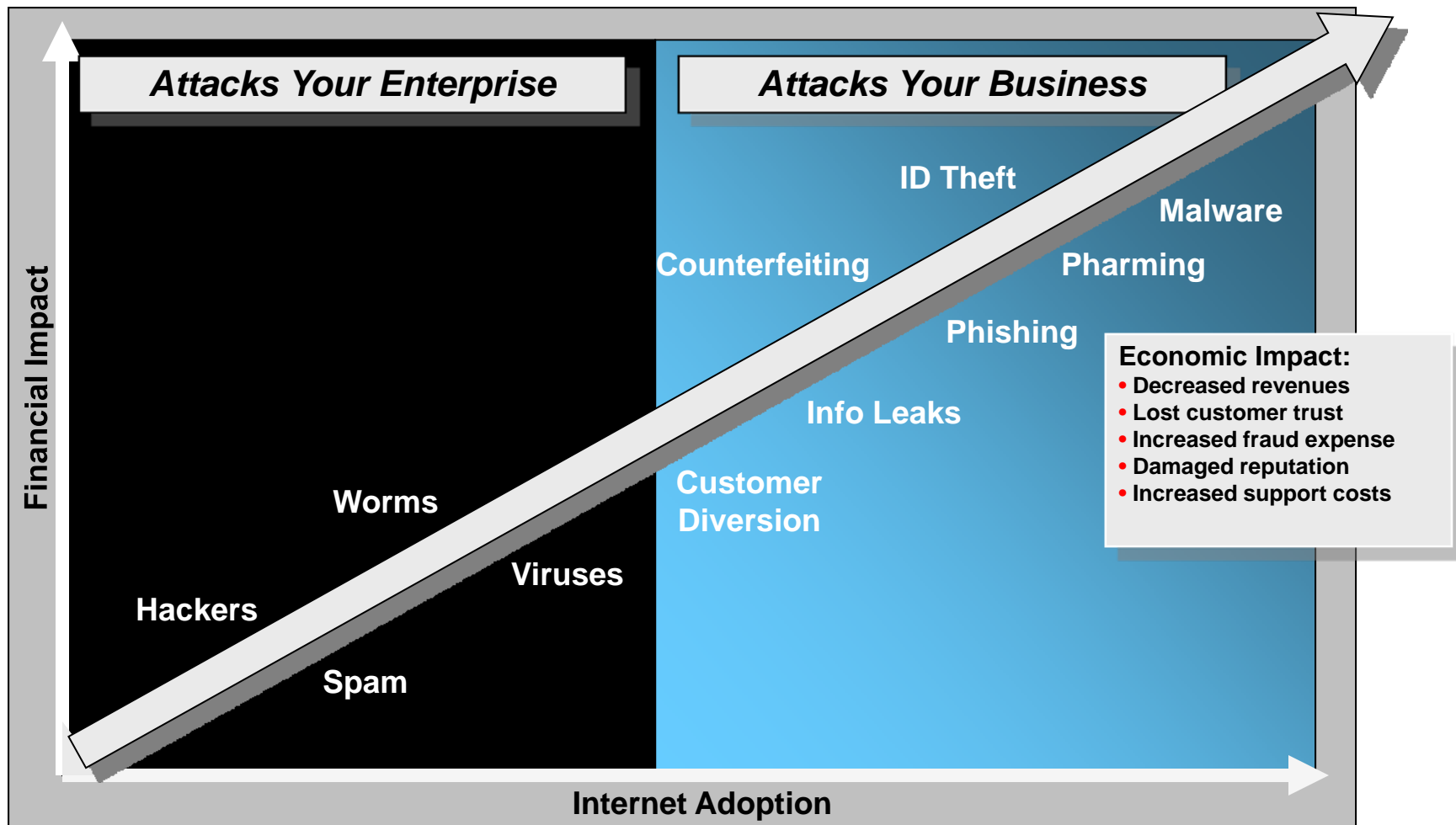
Trends

What to expect in 2010 and beyond

Impact of phishing

Best practices

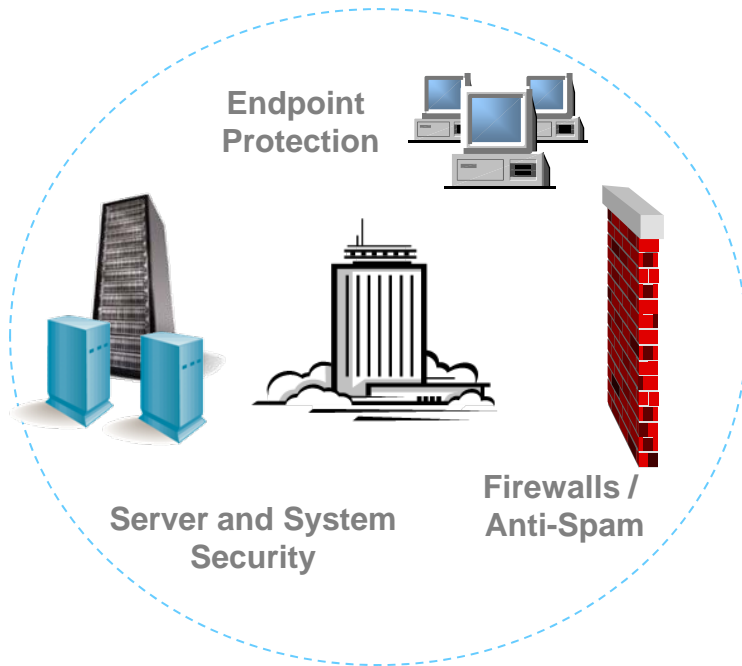
Impact of Online Threats



The New Imperative for Security

“Security for a borderless perimeter.”

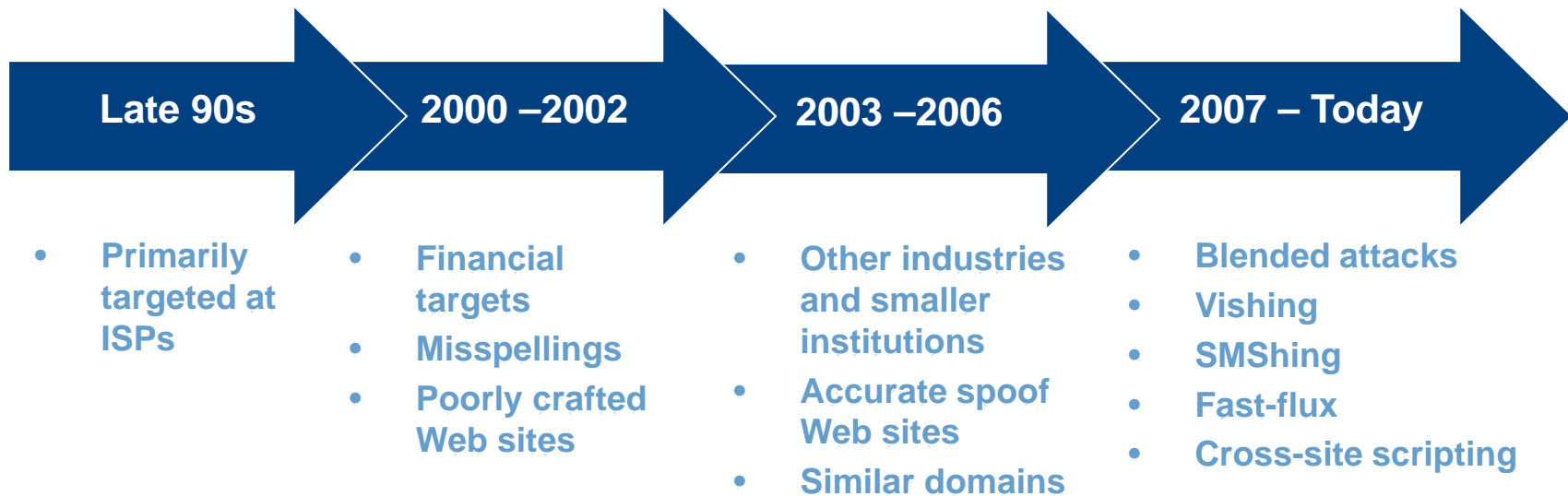
Old Security “Protect the Enterprise”



New Security “Protect Your Business”



Phishing – Historical Perspective



Phishing Example

Address http://88.45.97.19/.chaseonline.chase.com/online/home/index.php

CHASE

Start banking online now
Get a User ID
GO

Home Equity SALE

Returning Users: Log On

User ID:

Password:

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

Log On

Personal Banking

- ▶ Checking
- ▶ Credit Cards
- ▶ Savings
- ▶ CDs
- ▶ Online Banking & Bill Pay

Personal Lending

- ▶ Home Equity
- ▶ Mortgage
- ▶ Auto/Vehicle Loans
- ▶ Education Loans

Beware of Fraudulent E-mails
Learn how to protect your accounts and personal information

CHASE

Date: Jun 14 6:44AM

Dear JPMorgan Chase & Co. Bank Member,

Chase Bank is devoted to keeping a safe environment for its community of consumers and producers. To guarantee the safety of your account, Chase Bank deploys some of the most advanced security measures in the world and our anti-fraud units regularly screen the Chase Bank database for suspicious activity.

We recently have discovered that multiple computers have attempted to log into your JPMorgan Chase & Co. Bank Online Banking account, and multiple password failures were presented before the lessons. We now require you to re-validate your account information to us. If this is not completed by **June 15, 2006**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. In order to confirm your Online Bank records, we may require some specific information from you.

Please click the link below to verify your account.

<https://chaseonline.chase.com/online/home/>

If you choose to ignore our request, you leave us no choice but to temporary suspend your account.
Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

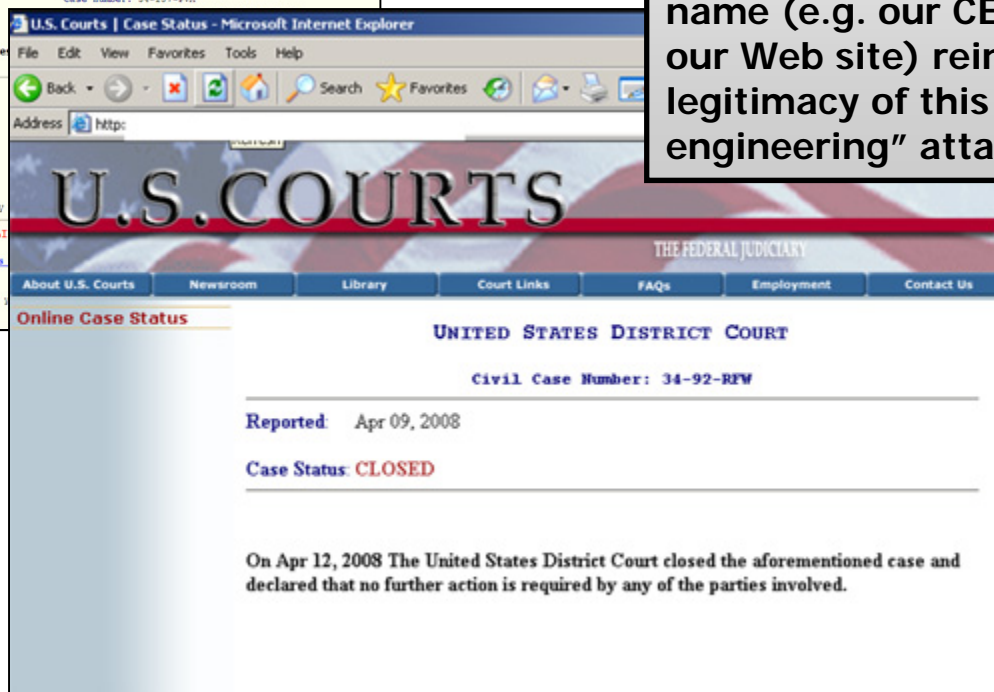
We apologize for any inconvenience.

The JPMorgan Chase & Co. Bank Security Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your JPMorgan Chase account and choose the "Help" link in the header of any page.

©2006 JPMorgan Chase & Co.

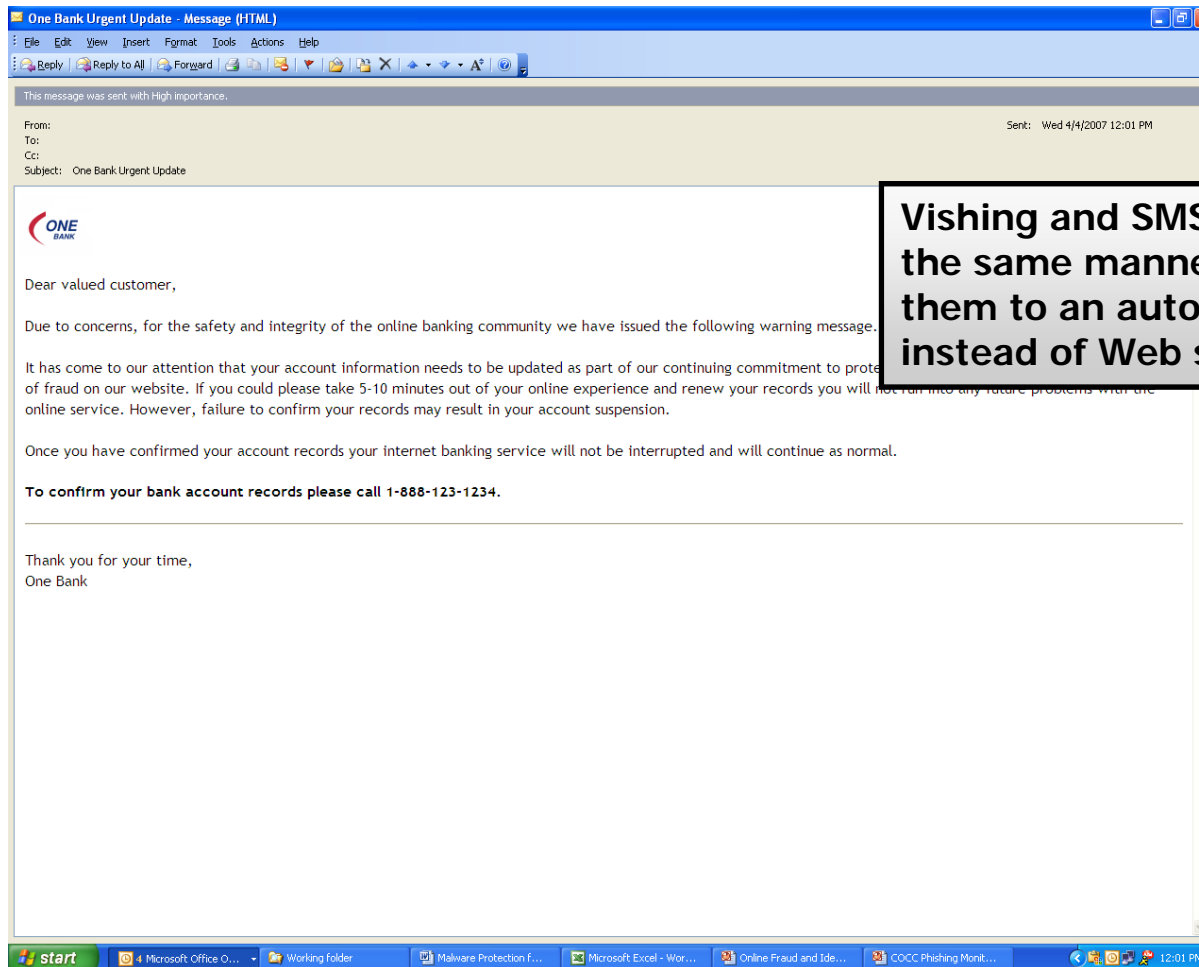
Spear Phishing



This variant of Phishing targets individual users, but for company specific information such as a network login, or financial information.

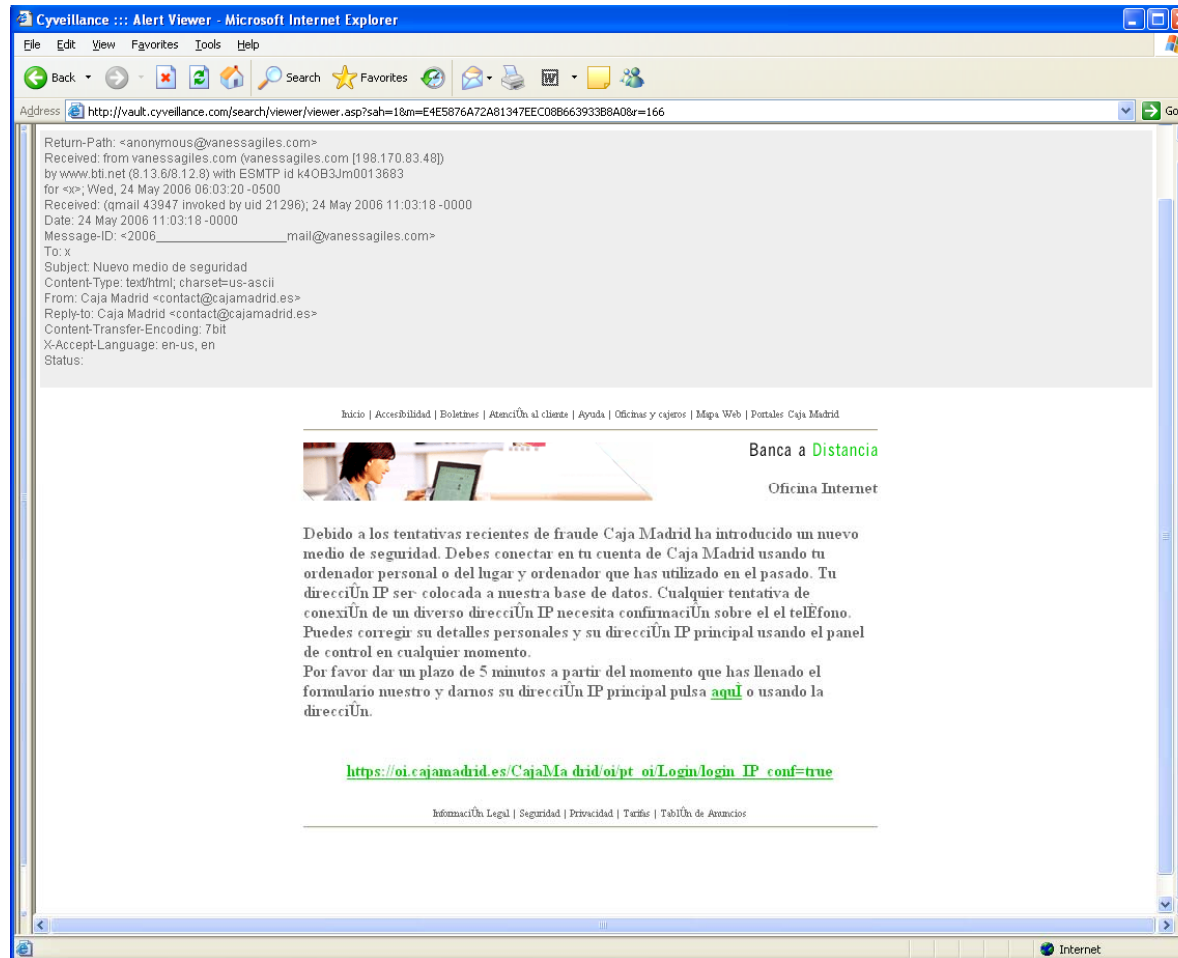
This example shows how an executive's name (e.g. our CEO, easily garnered from our Web site) reinforces the seeming legitimacy of this classic "social engineering" attack.

Vishing/SMShing



Vishing and SMShing target individuals in the same manner as phishing, but lures them to an automated phone system instead of Web site.

“Traditional” Phishing with Malware



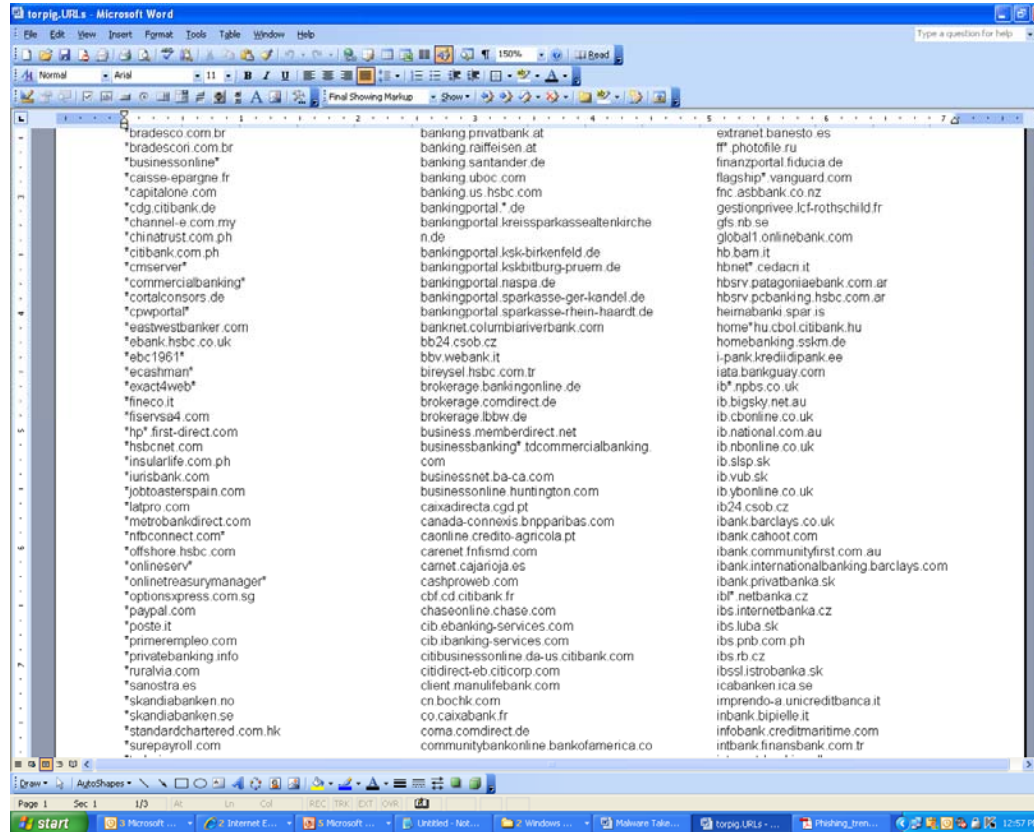
“Traditional” Phishing with Malware

The screenshot shows a Microsoft Internet Explorer window displaying a phishing page for 'CAJA MADRID oficina internet'. The page contains a login form with fields for 'D.N.I.' and 'Clave', and an 'Enter' button. A warning window titled 'Auto-Protect Results' is overlaid on the page, showing a yellow warning icon and a table of detected risks.

Risk	Action	Count	Filename
JS.Trojan.Blinder	Deleted	2	MATTHE~1.HTM

Buttons in the Auto-Protect Results window include 'Remove Risk', 'Reboot', and 'Close'.

Target-Specific Malware-based Phishing

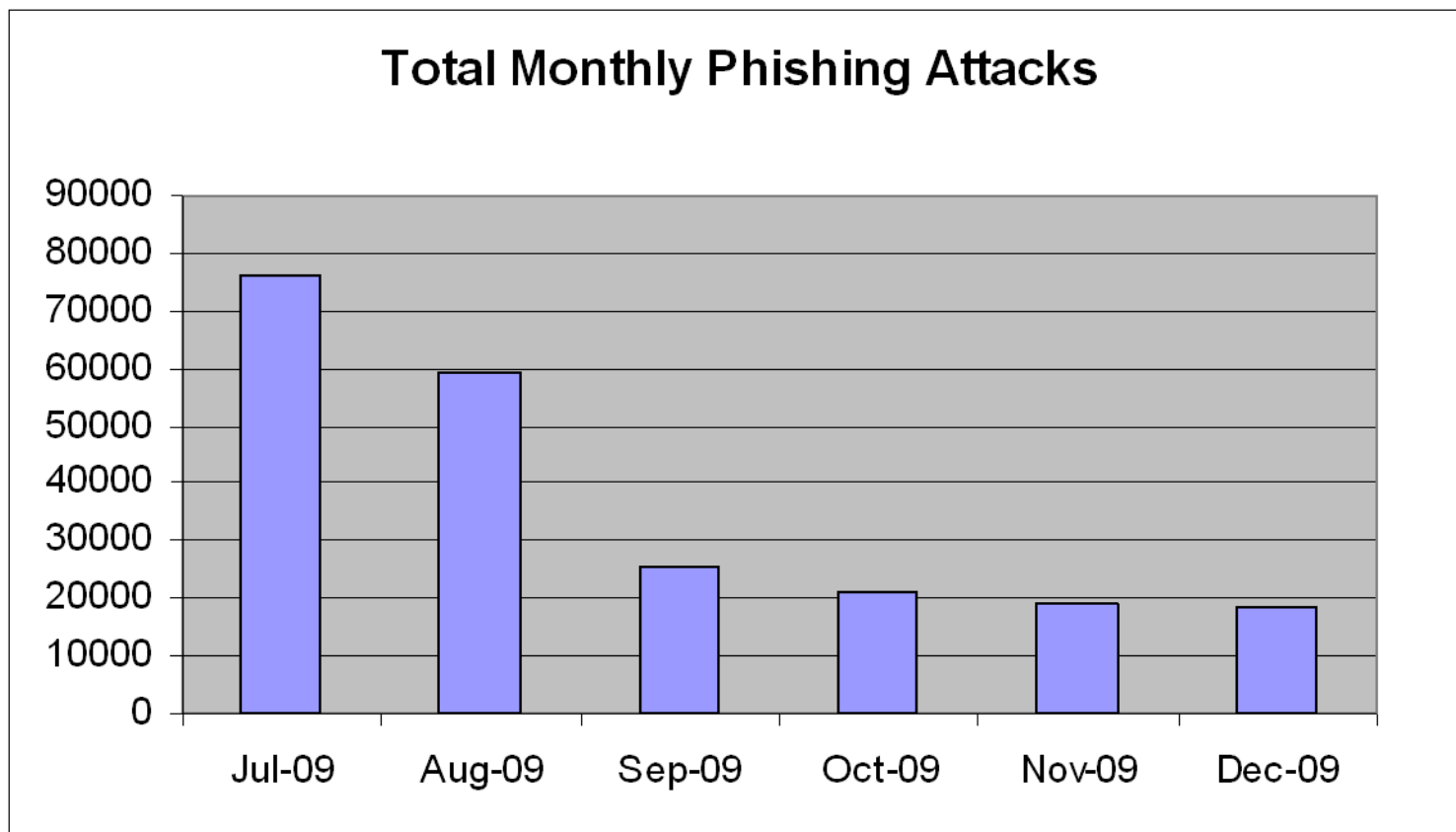


- **Social media has become a mainstream attack vector for fraudsters**
- **Both companies and consumers have cause for concern**

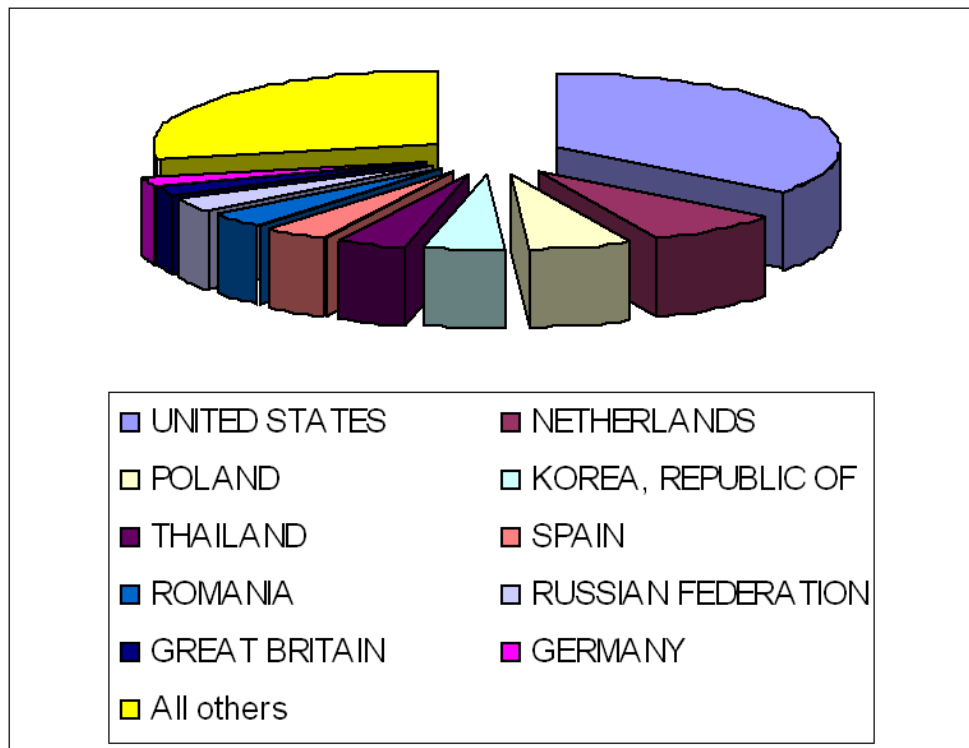


- **Fraud schemes targeting smart phones on the rise**
- **Lack of security for ever-growing amount of new mobile applications create a new set or problems for CUs**





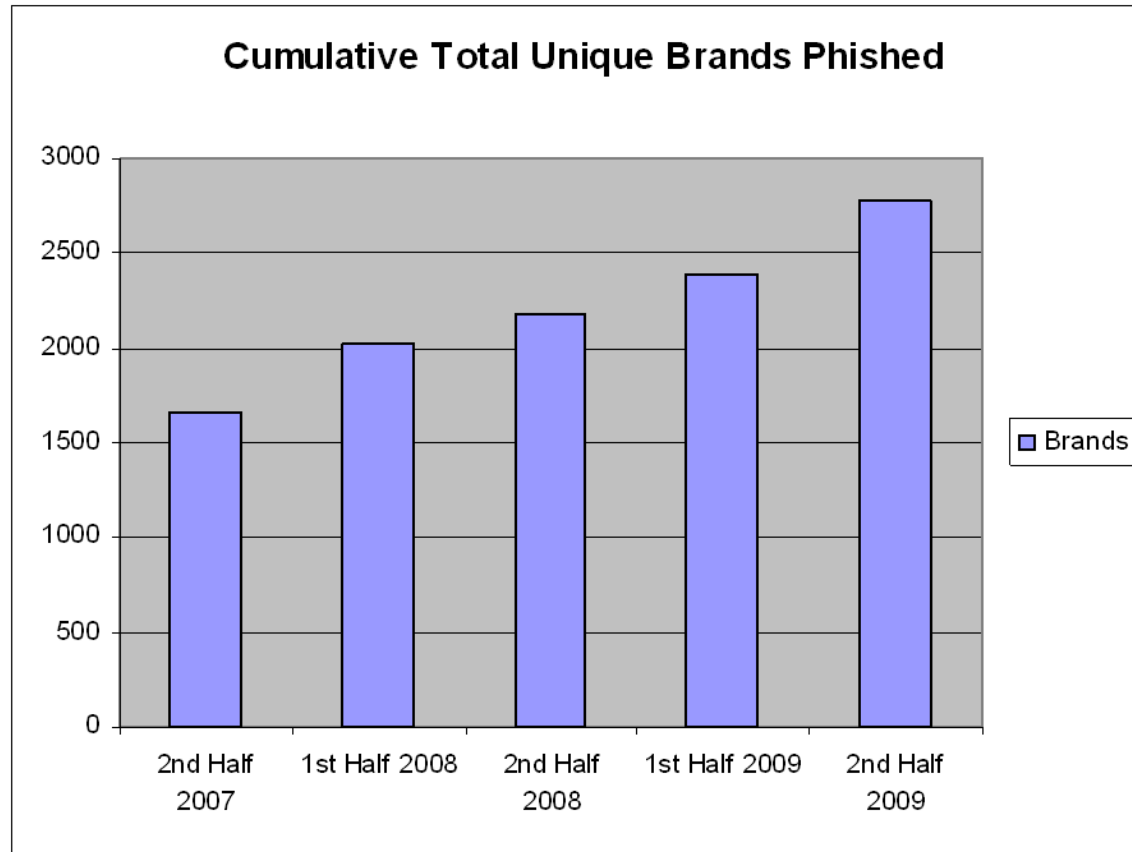
Phishing Attack Volume 2H 2009
Source: Cyveillance



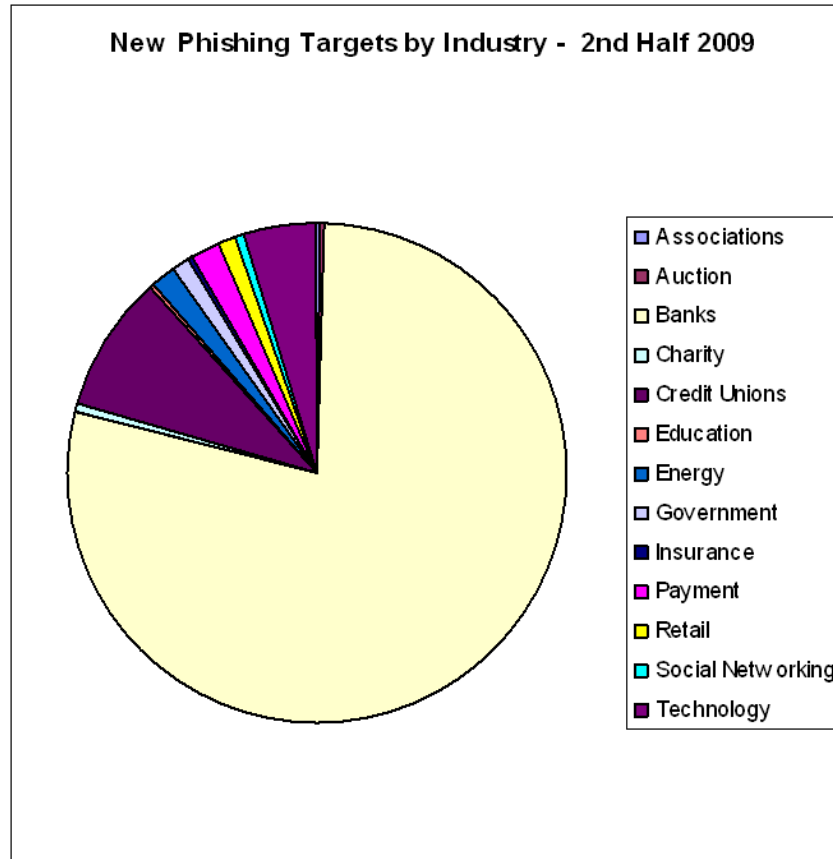
Country	% of All Sites
UNITED STATES	35%
NETHERLANDS	8%
POLAND	6%
KOREA, REPUBLIC OF	5%
THAILAND	4%
SPAIN	3%
ROMANIA	3%
RUSSIAN FEDERATION	3%
GREAT BRITAIN	2%
GERMANY	2%
All others	28%

Phishing Hosting Locations 2H 2009

Source: Cyveillance

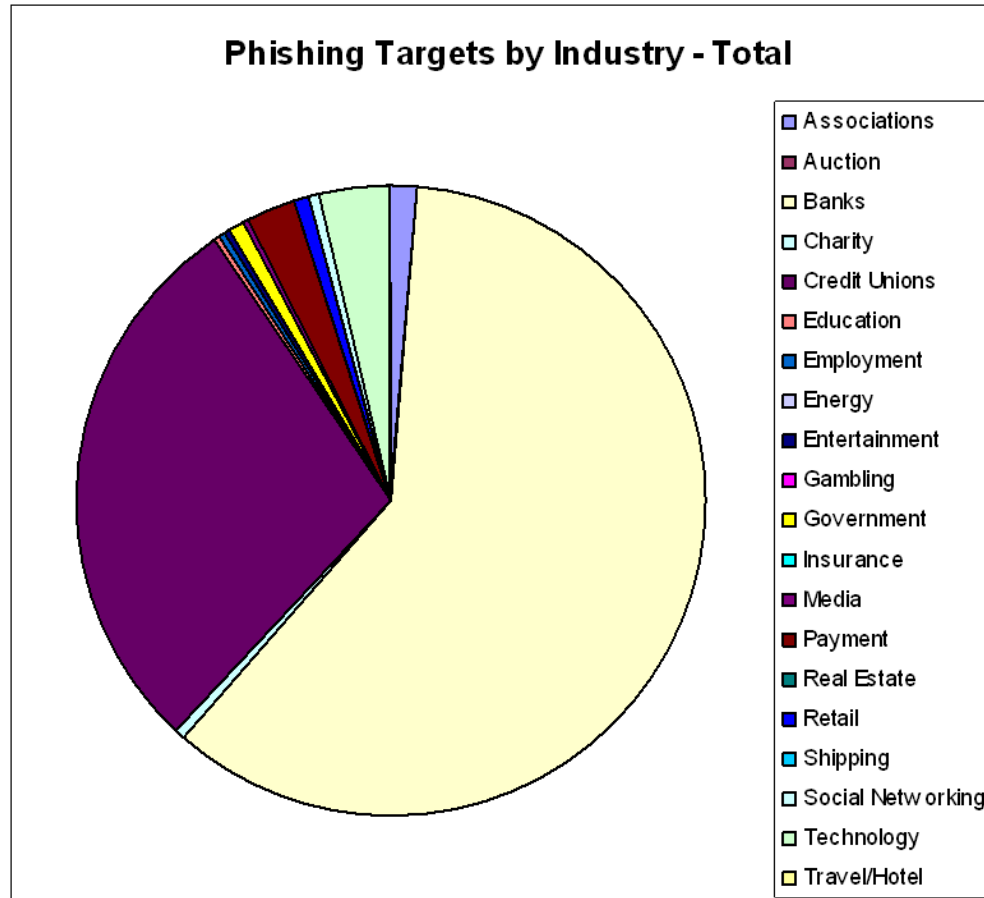


Total Unique Brands Phished 2H 2009
Source: Cyveillance



New Brands Attacked for First Time in 2H 2009

Source: Cyveillance



New Brands Attacked for First Time since 2005

Source: Cyveillance

Average daily detection rate from 7/1/09 to 12/31/09	F-Secure	Kaspersky	McAfee	Sunbelt	Sophos	Trend Micro	Symantec
	19%	38%	37%	17%	29%	26%	25%
	Dr. Web	AVG	Eset Nod32	F-Prot	Virus Buster	Norman	Avira Antivir
	26%	19%	37%	20%	11%	18%	29%

Anti-Virus Vendor Test Results 2H 2009

Source: Cyveillance

Vendor	Average Detection Rate Upon Initial Test	Average Detection Rate After 7 Days	Improvement
Sophos	34%	37.5%	3.5%
McAfee	51%	55.1%	4.1%
Kaspersky	32.5%	62.3%	29.8%
AVG	25.5%	49.6%	24.1%
Norman	21%	35.4%	14.4%
Symantec	24%	44.1%	20.1%

Anti-Virus Vendor Test Results Over Seven Day Period

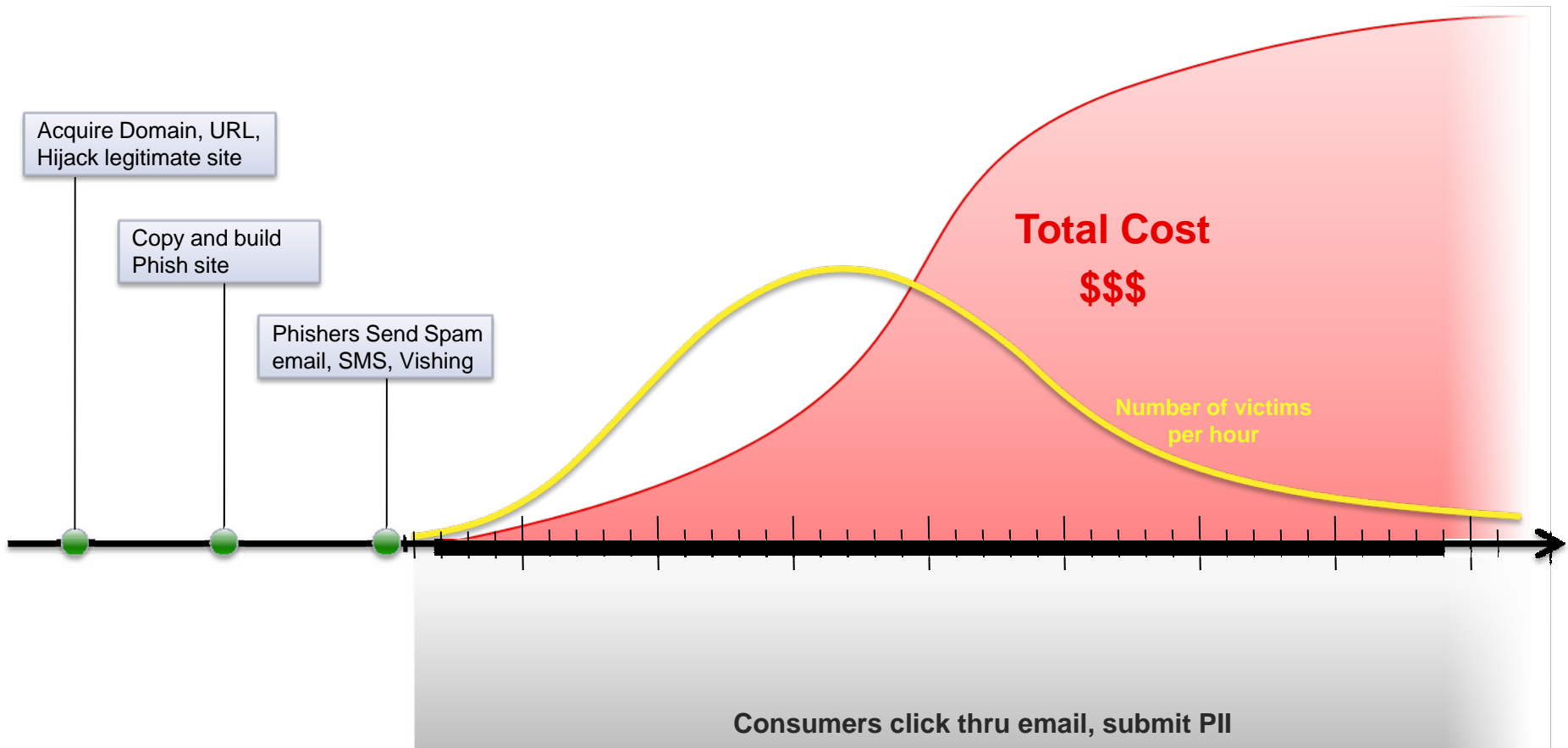
Source: Cyveillance

- **Traditional phishing attacks remain a major problem**
- **Continued expansion of the use of advanced technologies**
- **Increased targeting of smart phones for fraud schemes**

- **The continued exploitation of social networking sites and Web 2.0 functionality for purposes of online fraud**
- **The continued use of brand abuse tactics for the distribution of malware**
- **Lawsuits for inadequate protection?**

- **What are your costs associated with an attack?**
 - Hard costs
 - Soft costs
 - Time
 - Private life
- **Do you have adequate response procedures in place?**
 - Speed of detection and takedown
 - URL blocking
 - Recovery of Credentials
- **Have you made your organization a “hard” target?**

Anatomy of a Phish



Example

Emails Spammed	100,000
Percent filtered by spam filters	90%
Percent of people who GET the email that will EVENTUALLY open the email	50%
Percentage of those who will read the email and click on the link to the attack Web page	10%
Of those who clicked on the link, % that fall for the attack	10%
Total Number of people successfully phished	50

Cost Assumptions*:

Cash cost per members compromised	\$1,800.00
Personnel per-hour costs for each hour a site is up	\$400.00

*The cost assumptions above are based on input and feedback from credit unions of varying size. Many credit unions have their own specific values for the average costs of credentials (login, credit card, etc...) compromised by a criminal and the per-hour costs of responding to an attack.

Needs

- Create and implement plan
- Establish ownership
- Process training
- Preparedness testing
- Industry best practices
- Marketing and PR strategy
- Education

Monitoring

- Email
- Suspicious domains
- Web
- Security partners
- Fraud inbox

Alerting

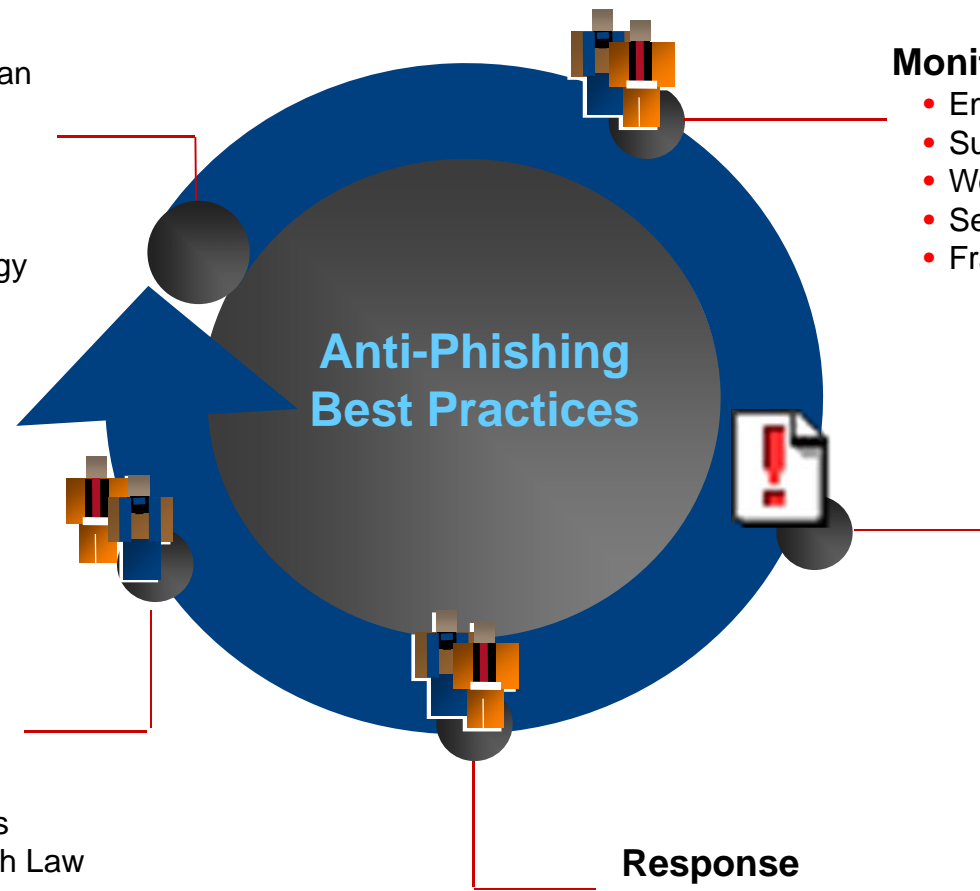
- Contact list
- Escalation

Response

- Site takedown actions
- URL blocking

Recovery

- Site monitoring
- Data recovery
- Summary reports
- Collaboration with Law Enforcement



Questions?

Contact info:

James Brooks
Director, Product Management
jbrooks@cyveillance.com
(703) 351-2405