

# Phishing, Vishing, & Smishing, Oh My!

Jeromie Jackson- CISSP, CISM  
COBIT & ITIL Certified  
President- San Diego OWASP  
SANS Mentor  
619-569-9457

# Agenda

- Definitions
- Threat Landscape
- Recent Scams
- Organizational Profiling
- Phishing, Smishing, and Vishing Examples
- Tools of the Trade
- Mitigation Techniques

# About Me

- President- San Diego OWASP
- Vice President- San Diego ISACA
- CISM, CISSP Since 1996
- COBIT, & ITIL Certified
- SANS Mentor
- [www.linkedin.com/in/securityassessment](http://www.linkedin.com/in/securityassessment)
- [www.jeromiejackson.com](http://www.jeromiejackson.com)
- [www.twitter.com/security\\_sifu](http://www.twitter.com/security_sifu)

## Articles

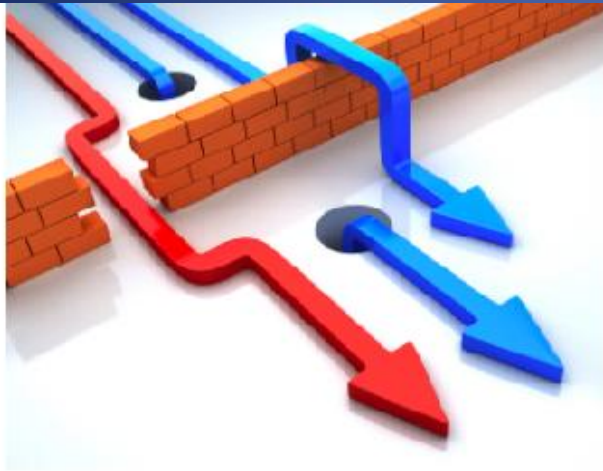
- \* Covered on Forbes Magazine
- \* Dark Reading
- \* Credit Union Business Magazine
- \* Credit Union Magazine
- \* CU Times
- \* Insurance & Technology Review
- \* CMP Media
- \* Storage Inc.

## Speaking Events

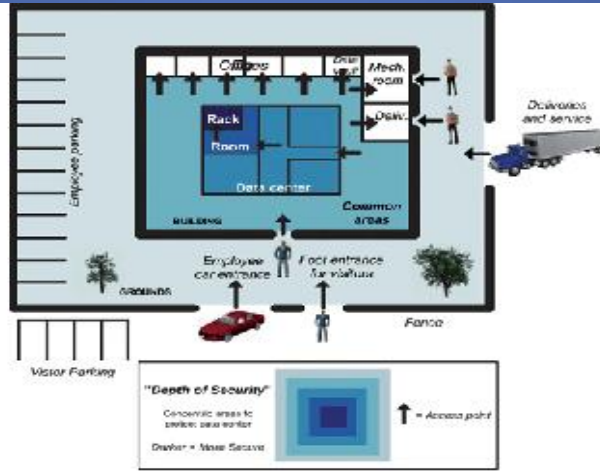
- \* CUISPA 2010/2011
- \* ISSA HI Discovery 2009/2010
- \* SPC 2009
- \* SecureIT 2009
- \* SecureIT 2008
- \* Interop
- \* Government Technology Conference (GTC)
- \* Many Credit Union Leagues



# What I Do



Penetration Testing & VA



Physical Pentest



Risk Management/GRC



Web Assessments



Soc. E. & Exec. Profiling



Regulatory Compliance/Readiness

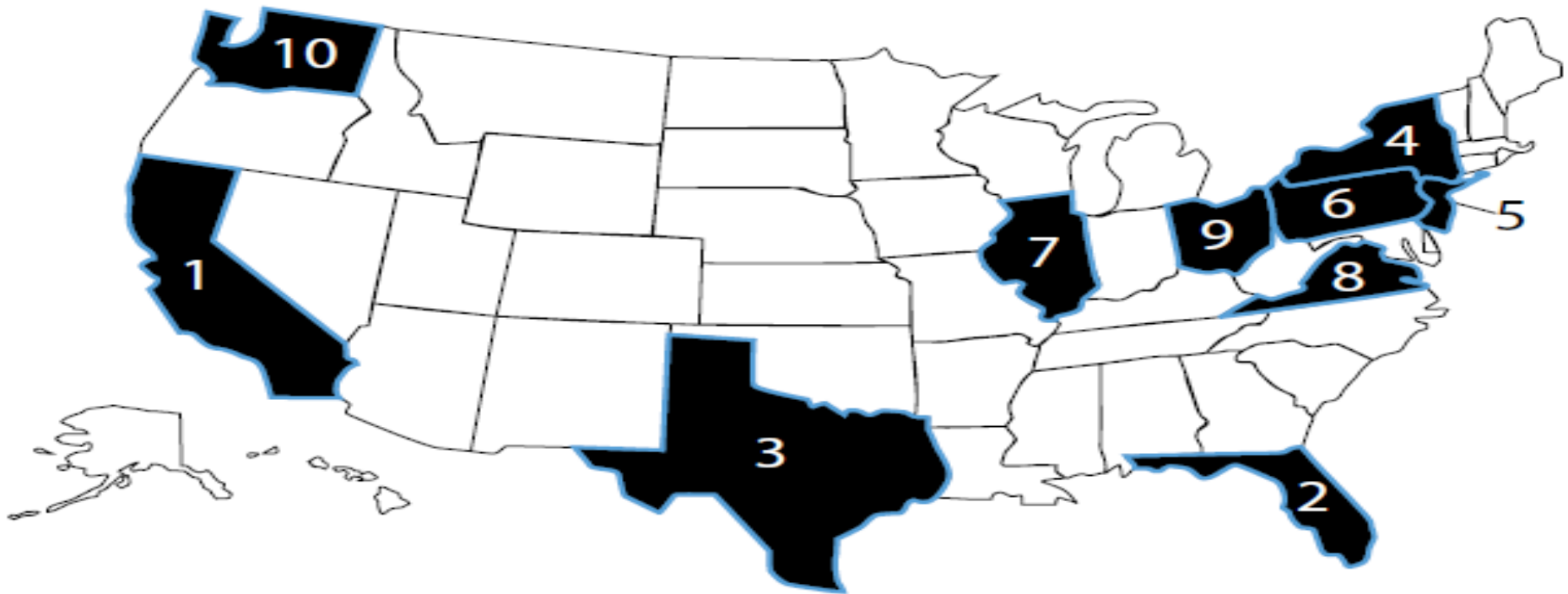
# Definitions

- All 3 attempt to acquire sensitive information by masquerading as a trustworthy entity.
  - Phishing- Emails & Instant Messages
  - Smishing- Short Messaging Service (SMS)
  - Vishing- Voice-based (VoIP & Landlines)



# Threat Landscape

**Map 2: Top 10 States by Count:  
Individual Complainants (Numbered by Rank)**

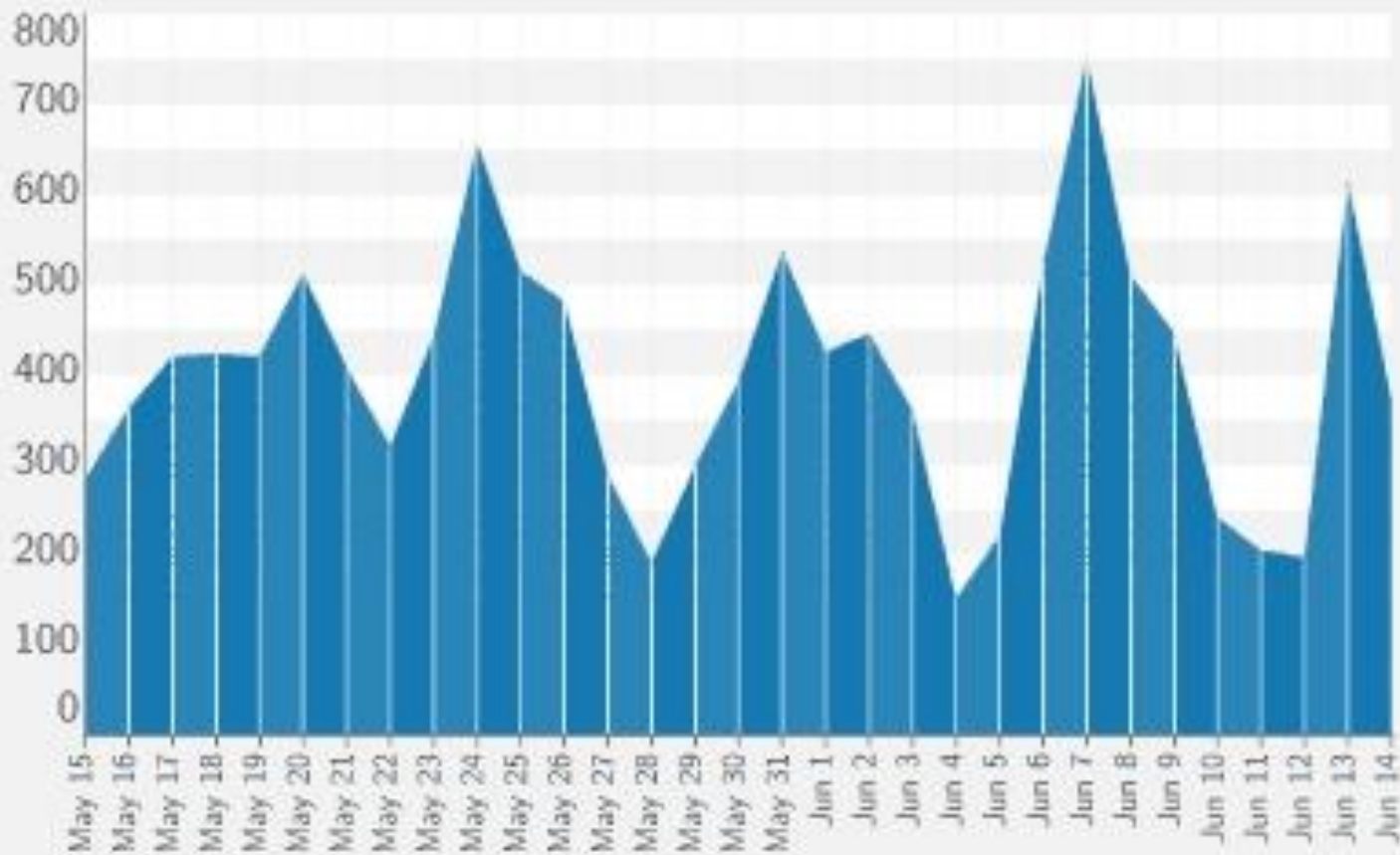


1. California	13.7%	6. Pennsylvania	3.6%
2. Florida	7.9%	7. Illinois	3.3%
3. Texas	7.3%	8. Virginia	3.0%
4. New York	5.8%	9. Ohio	2.9%

# Threat Landscape (Cont.)

## Daily Phishes Verified

chart created Jun 14 2011 22:15 UTC



# Who's Liable?

- Regulation E
- Sec. 205.6 Liability of consumer for unauthorized transfers.
- Consumer Liability Limits
  - If notice < 2 Days → No more than \$50
  - If Notice > 2 Days → Shall not exceed \$500
- Limits on Commercial Liability

***NONE!***



# Who's liable? (Cont).

- June 14, 2011- Dickinson, Mackaman, Tyler & Hagen, P.C Lawfirm
- Phishing attack that led to 97 wire transfer payments totaling more than \$1.9 million.
- A Michigan court has ruled against Comerica
- Bank should have prevented fraudulent wire transfers from the customer's account



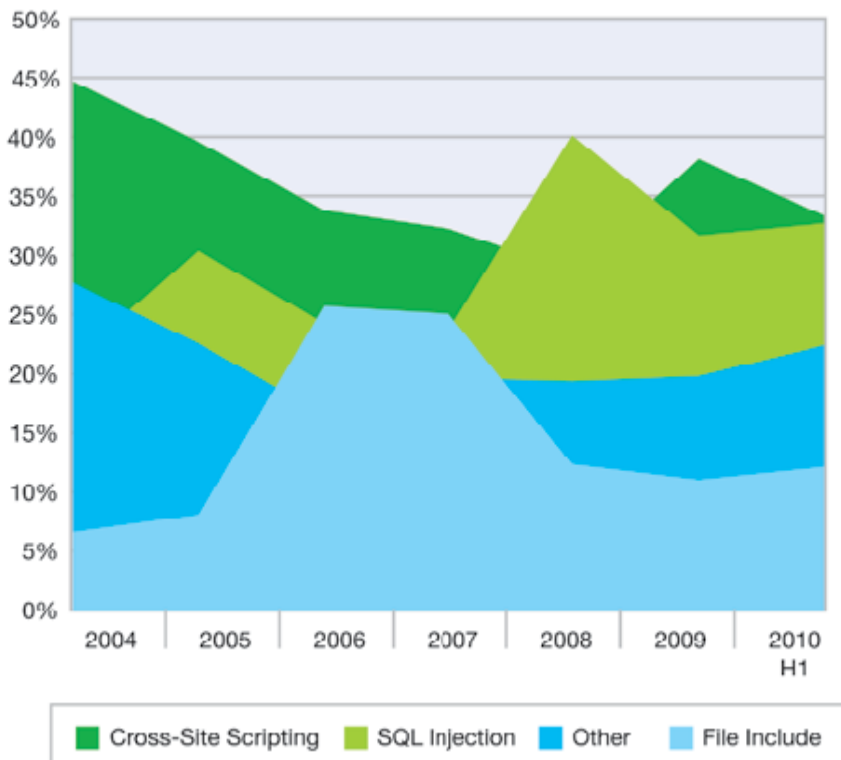
# Recent Reported Phishing Scams

- June 14, 2011 ANZ Bank - ANZ Online Internet Banking Has Sent You Secure Message. You are required to sign in below to Online Banking.
- June 14, 2011 Western Union - Account Statement
- June 14, 2011 American Express - New Alert Notice
- June 14, 2011 NatWest Bank - Reviewed your account
- June 13, 2011 Chase Bank - CHASE ACCOUNT STATEMENT | 2nd Notice
- June 13, 2011 AOL - AOL Account Status: Payment failed - Action Required
- June 13, 2011 Clydesdale Bank - Message Alert from Clydesdale Bank
- June 12, 2011 PayPal - Your account has been limited until we hear from you
- June 11, 2011 Chase Bank - Security Alert from Chase Online
- June 10, 2011 AOL - AOL : Billing Information
- June 10, 2011 PayPal - Account Notification !
- June 10, 2011 Capital One Bank - Capital One Account Security Routine Update.
- June 10, 2011 TD Waterhouse - Status Notification.
- June 10, 2011 Western Union - Account Statement
- *June 3, 2011 FDIC- FDIC: Your business account*

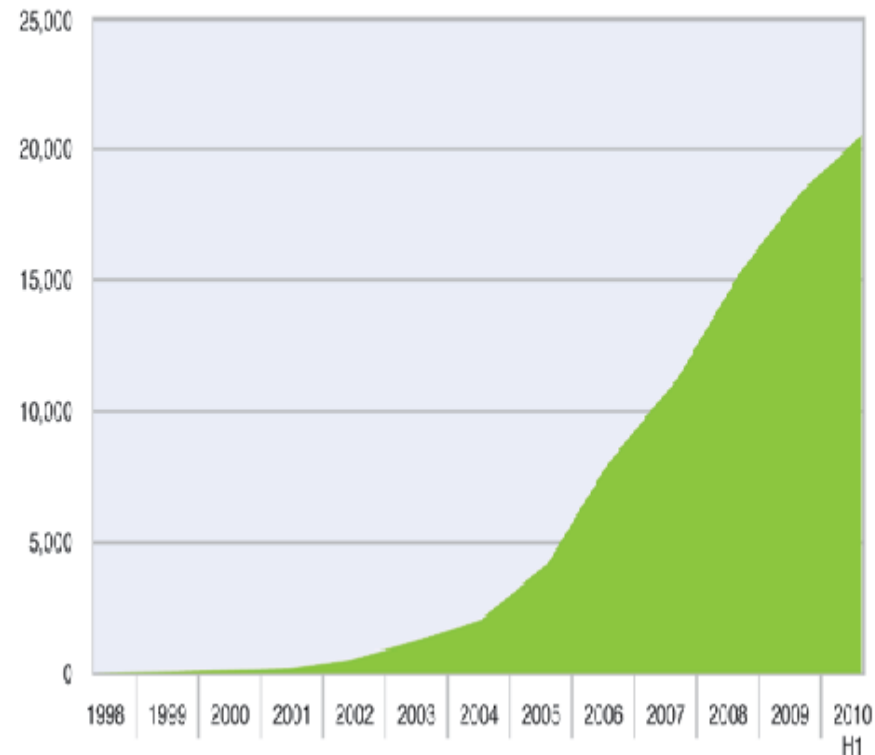
# Web Vulnerability Statistics

“Web application vulnerabilities have inched up to the 55 percent mark, accounting for fully half of all vulnerability disclosures in the first part of 2010.” - IBM X-Force® 2010 Mid-Year Trend and Risk Report

**Web Application Vulnerabilities by Attack Technique**  
2004-2010 H1



**Cumulative Count of Web Application Vulnerability Disclosures**  
1998-2010 H1



*The web is highly vulnerable and thus a great vehicle to spread malware*

# Organization Profiling

Organizational relationships are often exploited.

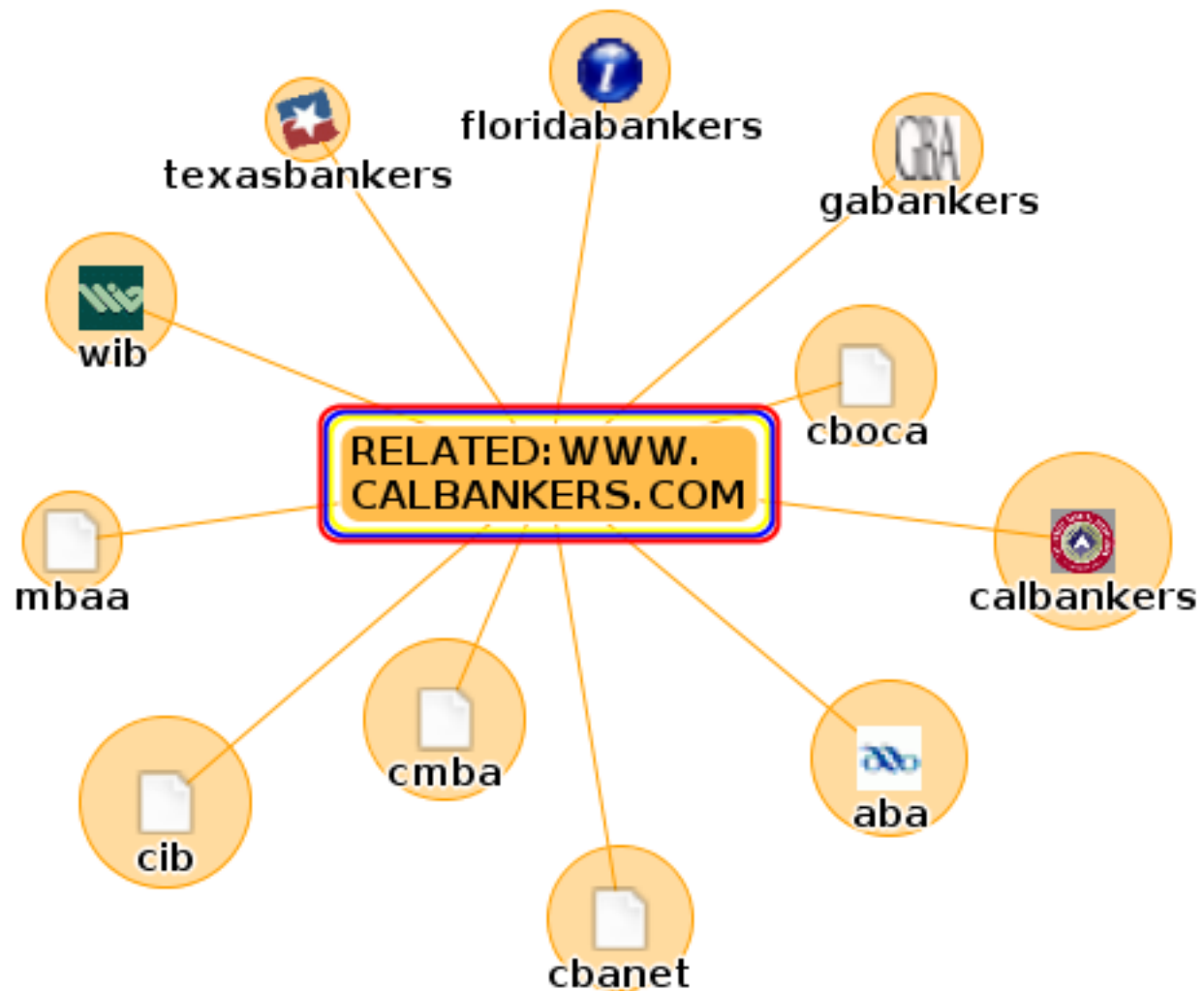
- ISP
- Vendors
- Property Management
- Janitorial
- Air Conditioning

Ruse impersonating employees & internal roles are equally common.

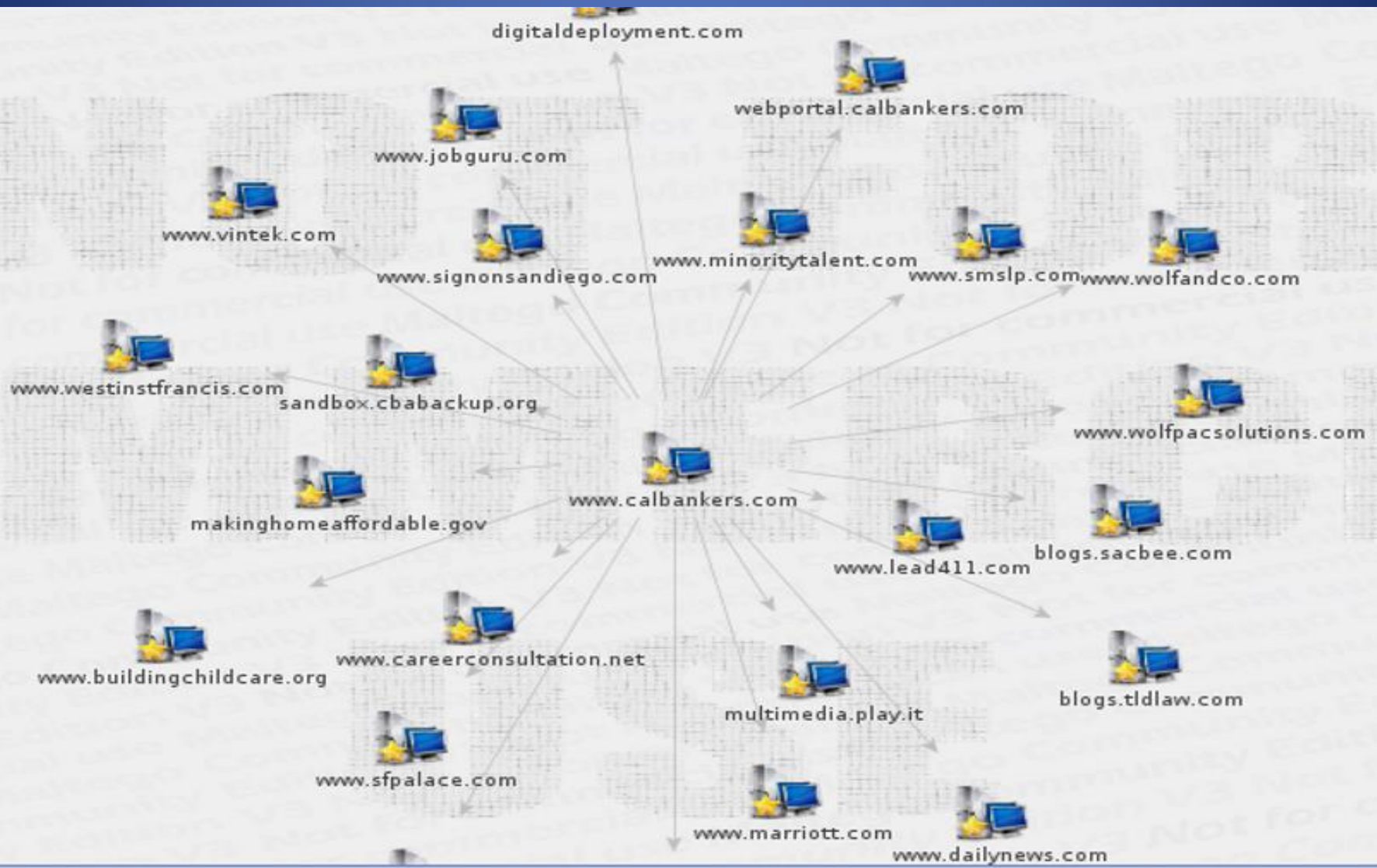
- CIO
- HR
- Legal
- Helpdesk



# Touchgraph



# Maltego



# Website Profiling

http://www.calbankers.com/strategic-partners



California Bankers Association

HOME | CONTACT | LOG IN

Search the site  GO  
Check out our strategic partners

About CBA » Newsroom » Legislation & Advocacy » Events » Education & Training » Member Resources » Consumer Center »

## Member Resources

Dodd-Frank Information Center

Strategic Partners

Partner Spotlight

CBA | ABA  
Co-Endorsements

Affiliate Members

Publications

Banker Resources

Job Bank

## CBA's Strategic Partners Program

This program identifies the vendor with the highest quality products and services in a service category. Partners are selected based on their ability to meet our high expectations for product and service quality.



**BancInsure, Inc.**  
Bankers are the experts at understanding banking needs



**Harland Clarke**  
A leading provider of integrated payment solutions, marketing services and security solutions

**Kurt Kessler & Associates**

**Kestler Associates**  
Total Insurance Solutions



**Standard Register**  
Nearly a century of industry expertise



**USI Benefits Partners**  
Delivering high-quality insurance and financial products



**VINtek**  
Electronic Lien and Tinting Services



**Wolters Kluwer Financial**



**Clark Consulting**  
Industry Leading Executive Benefit Plans and Strategic Funding Solutions



**Insperity**  
Trusted Advisor Providing HR and Business Solutions



**Pii Promontory Interfinancial Network, LLC**  
Profit-Enhancing Solutions, including ICS (in pilot mode) and CDARS



**Staples**  
That was easy.



**Verafin**  
One of North America's leading BSA/AML Compliance and Fraud Detection software providers



**Wolf & Company, P.C.**  
WolfPAC Integrated Risk Management®

## Join the program!

Contact Stephen Clark for more information on CBA Strategic Partners

## Banking Compliance Solutions

When your compliance partner understands the nuances of your business, it's reflected in the effectiveness of your solutions

WE'RE HERE FOR  
**YOU**  
Wolters Kluwer  
Financial Services

# Website to Social Media

The image shows a browser window with two pages. The top page is the California Bankers Association website, and the bottom page is a LinkedIn profile for Mary Curran.

**California Bankers Association Website:**

- URL: <http://www.calbankers.com/about-cba/executive-committee>
- Page Title: Executive Committee | Cali...
- Logo: California Bankers Association
- Navigation: About CBA, Newsroom, Legislation & Advocacy, Events, Education & Training, Member Resources, Consumer Center
- Section: **Steven Buster - Chairman**  
President/CEO, Mechanics Bank  
Steven K. Buster has been chief executive officer of Mechanics Bank since July 1, 2004. During his tenure, Mechanics Bank increased annual profit to \$29 million in 2007 from \$24 million in 2004, and increased shareholder's million in 2007 from \$230 million in 2004. Before joining M&B with U.S. Trust Company, where he was managing director of United States banking activities.
- Section: **Mary Allis Curran - Chairwoman-Elect**  
Executive Vice President, Union Bank, NA  
Mary Curran joined Union Bank in May 1999 in her position President of The Private Bank, she oversees Private Bank Management Sales and Private Wealth Planning for the Bank as Market President, Commercial Banking for San Diego as Global and Wealth Markets umbrella. The Private Bank is a services, planning, brokerage services, trust and estate fee management for high net worth individuals, business owner professional service firms.
- Section: **Richard Smith - Immediate Past Chairman**  
President/CEO, Tri Counties Bank  
Richard P. Smith serves as president and CEO for Tri Count is responsible for establishing and implementing long-range policies, directing bank activities such as acquisition, brand augment the bank and maximize returns on capital and ass representative for the bank with shareholders, major custom industrial associations, regulatory agencies and the press.
- Section: **Felix Fernandez - Treasurer**  
Regional President, Wells Fargo Bank, NA  
Felix Fernandez is Regional President of Community Bank banking in the Northern California region. Based in Sacra more than 2,400 team members at 140 locations throughout

**LinkedIn Profile:**

- URL: [http://www.linkedin.com/profile/view?id=15239800&authType=NAME\\_SEARCH&authToken=if4&locale=en\\_US&srchid=e91](http://www.linkedin.com/profile/view?id=15239800&authType=NAME_SEARCH&authToken=if4&locale=en_US&srchid=e91)
- Page Title: Executive Committee | Cali...
- Section: **Mary Curran**  
Executive Vice President at Union Bank of California  
Greater San Diego Area | Banking
- Current: **Executive Vice President at Union Bank**
- Education: **San Diego State University**, **University of Colorado at Boulder**
- Connections: **145 connections**
- Public Profile: <http://www.linkedin.com/pub/mary-curran/512b/3b4>
- Experience:
  - Executive Vice President Union Bank**  
Privately Held, Banking Industry  
1999 - Present (22 years)
  - EVP Head of The Private Bank at Union Bank** 2006 to present
  - SVP Market President San Diego and Orange County Commercial Banking** 1999-2006
- Education:
  - San Diego State University**  
MBA
  - University of Colorado at Boulder**  
BS, Journalism
- Contact Settings:
  - Interested In: **expertise requests**, **getting back in touch**
  - reference requests
- Buttons: Share, PDF, Print
- Advertisement: "Ducati is ready for retail business. Are you? get ready! Ready for Real Business. XEROX"
- How you're connected to Mary:
  - You
  - Marshall Staneik
  - Jennifer Edwards
  - Brian Toland
  - Gordon W. Romney
  - Bruce Geier
  - ...and 26 others
  - Mary's connections
  - Mary Curran
- Viewers of this profile also viewed...:
  - Terry Negendank, Senior Vice President, Managing...
  - Wanda Guttas, Executive Vice President at Union Bank
  - Luanne Bas, Co-Vice President at Union Bank of California

# Social Media Profiling



# Phishing Examples

Fraudulent Alert : Your Online Account Has Been Locked - Message (HTML)

Message Adobe PDF

Reply Reply Forward Delete Move to Create Other Block Safe Lists Categorize Follow Mark as Related Find  
To All Forward Delete Move to Create Other Block Safe Lists Categorize Follow Mark as Related Find  
Respond Actions Junk E-mail Options Find

From: Chase Online@ [cchinking@chase.com] Sent:

To:

Cc:

Subject: Fraudulent Alert : Your Online Account Has Been Locked

**CHASE**

Dear Chase Bank customer

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us.

If this is not completed by **January 24, 2011**, we will be forced to suspend your account indefinitely, as it has been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:  
[https://chaseonline.chase.com/Logon.aspx?I\\_OE=COLLogon/](https://chaseonline.chase.com/Logon.aspx?I_OE=COLLogon/)

Thank you for your patience in this matter,  
Chase Bank Customer Service

NatWest Secure Message Center - 1 new message alert. - Message (HTML)

Message Adobe PDF

Reply Reply Forward Delete Move to Create Other Block Safe Lists Categorize Follow Mark as Related Find  
To All Forward Delete Move to Create Other Block Safe Lists Categorize Follow Mark as Related Find  
Respond Actions Junk E-mail Options Find

From: NatWest Online Services - nocbe@natwest.com Sent:

To:

Cc:

Subject: NatWest Secure Message Center - 1 new message alert.

Dear NatWest Customer,

To protect your account Our monitoring Unit Dept has temporarily suspended your online access. This has been done due to the number of incorrect log-in attempts on your account online.

At NatWest, we take the job of protecting our customers very seriously, So for your protection we are proactively notifying you of this activity.

Due to this, You are requested to follow the provided steps in order. To restore your online access please click on the Log on link below:

[Online banking Log on](#)

Thank you,

NatWest Online Services.  
e-banking service  
19 January 2011

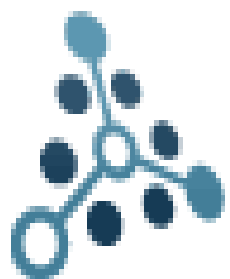
# Vishing Examples

- “We have seen anomalous transactions on your account and need to validate some information.”
- “During a system migration there was some data corruption. Could you please verify...”
- “A large check has been posted against your account causing a negative balance...”

# Smishing Examples

- Credit Union N.A. Please call us immediately at 1-888-xxx-xxxx regarding a recent restriction placed on your account. Thank you.
- Alert!! Honolulu City & County Employees has limited your account pending verifications. Contact us NOW at 213-xxx-xxxx.
- Your BANK web service is expired, for renewal please login using [www.attackerwebsite.com](http://www.attackerwebsite.com) ASAP

# Tools of the Trade



TouchGraph



MALTEGO3  
OPEN SOURCE INTELLIGENCE

METASPLOIT



SocialEngineer  
Toolkit



# Metasploit

- Metasploit community constantly expands the exploit database:
  - Covers 565+ unique CVEs
  - 551+ remote exploits
  - 261+ auxiliary modules
  - Hundreds of payloads.
- Remote shells & remote desktop
- Keylogging
- Camera utilization
- Smart brute forcing
- Smart exploitation
- Advanced pivoting



# Social Engineering Toolkit

## Attack Vectors

- 3.1 Spear-Phishing Attack Vector
- 3.2 Java Applet Attack Vector
- 3.3 Metasploit Browser Exploit Method
- 3.4 Credential Harvester Attack Method
- 3.5 Tabnabbing Attack Method
- 3.6 Man Left in the Middle Attack Method
- 3.7 Web Jacking Attack Method
- 3.8 Multi-Attack Web Vector
- 3.9 Infectious Media Generator
- 3.10 Teensy USB HID Attack Vector



# Browser Exploitation Framework

- **BeEF (Browser Exploitation Framework) often used**
- Creates zombies on compromised browsers
- Javascript embedding, confirmation window embedding, system commands, portscanning, etc.



# Mitigation Techniques





# PASSWORDS ARE LIKE SOCKS



**CHANGE THEM OFTEN**

GET LAZY WITH YOUR PASSWORDS AND YOU COULD CAUSE A REAL STINK! CHANGE YOUR PASSWORD REGULARLY...



[www.ballarat.edu.au/is](http://www.ballarat.edu.au/is)

CRICOS Provider Number 00103D

# Prudently Manage Risk

- Identify & prioritize risk
- Map risks & regulations to controls
- Risk management program



# Mitigation Techniques

- Don't respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.
- Treat your mobile phone like you would your computer...don't download anything unless you trust the source.
- When buying online, use a legitimate payment service and always use a credit card because charges can be disputed if you don't receive what you ordered or find unauthorized charges on your card.
- Check each seller's rating and feedback along with the dates the feedback was posted. Be wary of a seller with a 100 percent positive feedback score, with a low number of feedback postings, or with all feedback posted around the same date.
- Don't respond to unsolicited e-mails (or texts or phone calls, for that matter) requesting personal information, and never click on links or attachments contained within unsolicited e-mails. If you want to go to a merchant's website, type their URL directly into your browsers

# Mitigation Techniques (Cont.)

- Fraud Alerting Services
- Tokens / plugins for users
- ACH whitelisting for business customers
- Guardian Analytics

# Toys of the Trade

Independent review

Internal and/or External Vulnerability Assessment

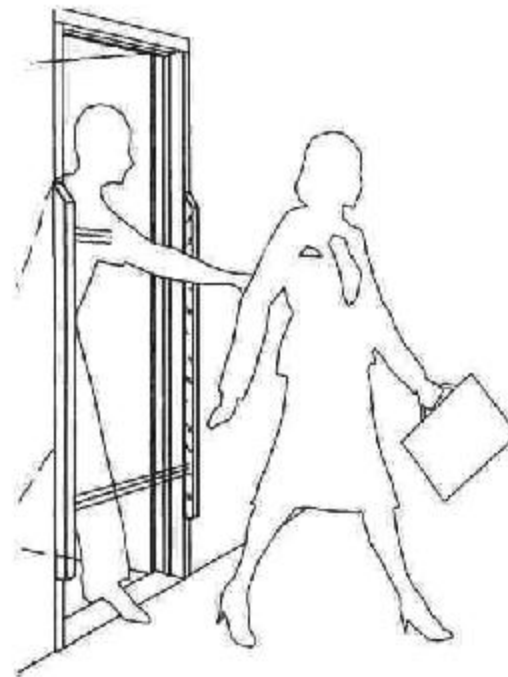
Wireless

Physical Security Pentest

Social Engineering

Phases

- Discovery
- Vulnerability Assessment
- Penetration Testing
- Reporting
- Debrief



# Questions

- Jeromie Jackson- CISSP, CISM
- COBIT & ITIL Certified
- President- San Diego OWASP
- SANS Mentor
  
- LinkedIn:  
[www.linkedin.com/in/securityassessment](http://www.linkedin.com/in/securityassessment)
- Twitter: [www.twitter.com/security\\_sifu](http://www.twitter.com/security_sifu)
- Phone- 619-569-9457

