wombat®
security technologies

Social Engineering & How to Counteract Advanced Attacks

Ralph Massaro, VP of Sales
Wombat Security Technologies, Inc.

Agenda

- Social Engineering
- DEFCON Competition
- Source of Problem
- Countermeasures

wombat security technologies

Change Behavior. Reduce Risk.

Social Engineering Scenarios

- Email
- In-person
- Smartphone
- Social networking
- Snail mail
- Fixed phone

wombat security technologies

Change Behavior. Reduce Risk.

Def Con Hacking Conference

- Held in Las Vegas
- Social Engineer Capture the Flag (SECTF)
- Social-Engineering.org
- Raise Awareness of social engineering threats and to demonstrate how damaging information is freely available

http://social-engineer.org/resources/sectf/Social-EngineerDefcon20SECTFResultsReport-Final.pdf

wombat security technologies

Change Behavior. Reduce Risk.

SECTF

- Contest where participants collect information called Flags (37)
- Flags are assigned a point value
- Participant with the highest # of points wins

wombat security technologies

Change Behavior. Reduce Risk.

SECTF

- Contestants:
  - 20 participants out of 198 candidates
    - 10 Women and 10 Men
  - First time participants
  - Backgrounds
    - Security Experts
    - Red Team
    - Marketing Researchers
    - Sales
    - Students

wombat security technologies

Change Behavior. Reduce Risk.

SECTF

- Target Companies:
  - Fortune 500
  - Diverse Industries
  - Common Brands
  - Contest unknown to target companies

Apple, Boeing, Chevron, Exxon, General Dynamics, General Electric, General Motors, Home Depot, J&J, Disney

wombat security technologies

Change Behavior. Reduce Risk.

Competition Process

- Target industries – transportation, telecom, oil, retail, entertainment & technology
- Upfront research – publicly available only
  - Google, Twitter, Facebook, Linkedin, Craigslist, Foursquare, Whois, Wikipedia, Vimeo, etc, etc, etc
- Phone calls at DEFCON – spoofed or not
- Points range from 3 to 25
  - 3 for "Do you block sites?"
  - 25 for getting target to go to URL

wombat security technologies

Change Behavior. Reduce Risk.

SECTF

- What were they looking for?
  - Get them to visit a fake URL – 25 points
  - What browser do they use? – 10 points
  - What version of that browser? – 15 points
  - What anti-virus system is used? - 10 points
  - What operating system is in use? - 10 points
  - What service pack/version? – 15 points
  - What program to open PDFs and what version? – 10 points
  - What mail client is used? – 10 points
  - What version of the mail client? – 10 points
  - Who is their 3rd party security company? – 10 points
  - When was the last time they had security awareness training? – 10

wombat security technologies

Change Behavior. Reduce Risk.

Success Rates in High Value Targets

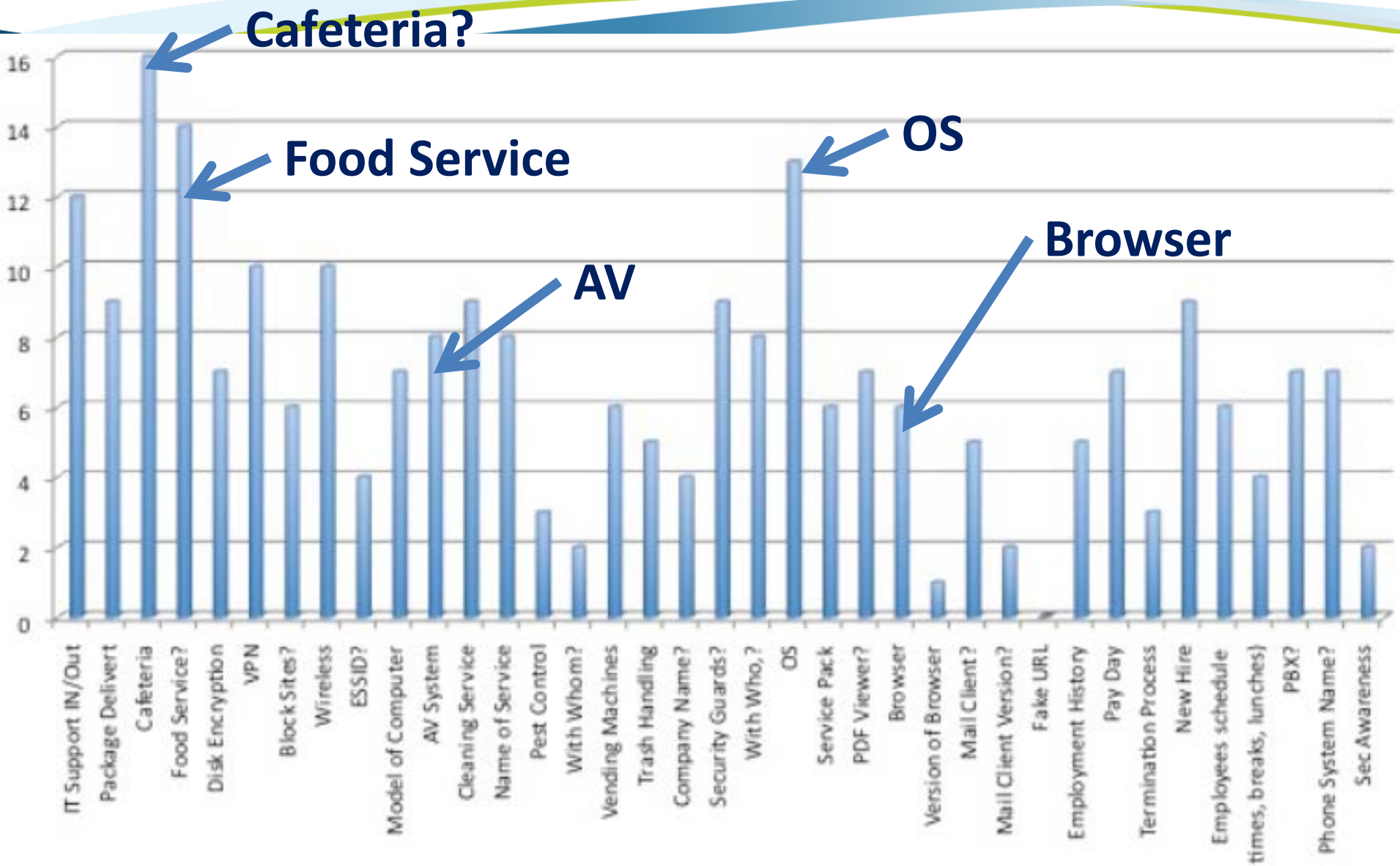
- Get them to visit a fake URL – 30%
- What browser do they use? – 70%
- What version of that browser? – 25%
- What anti-virus system is used? – 65%
- What operating system is in use? – 120%
- What service pack/version? – 40%
- What program to open PDFs and what version? - 70%
- What mail client is used? - 55%
- What version of the mail client? - 25%
- Who is their 3rd party security company? - 50%
- When was the last time they had security awareness training? - 25%

wombat security technologies

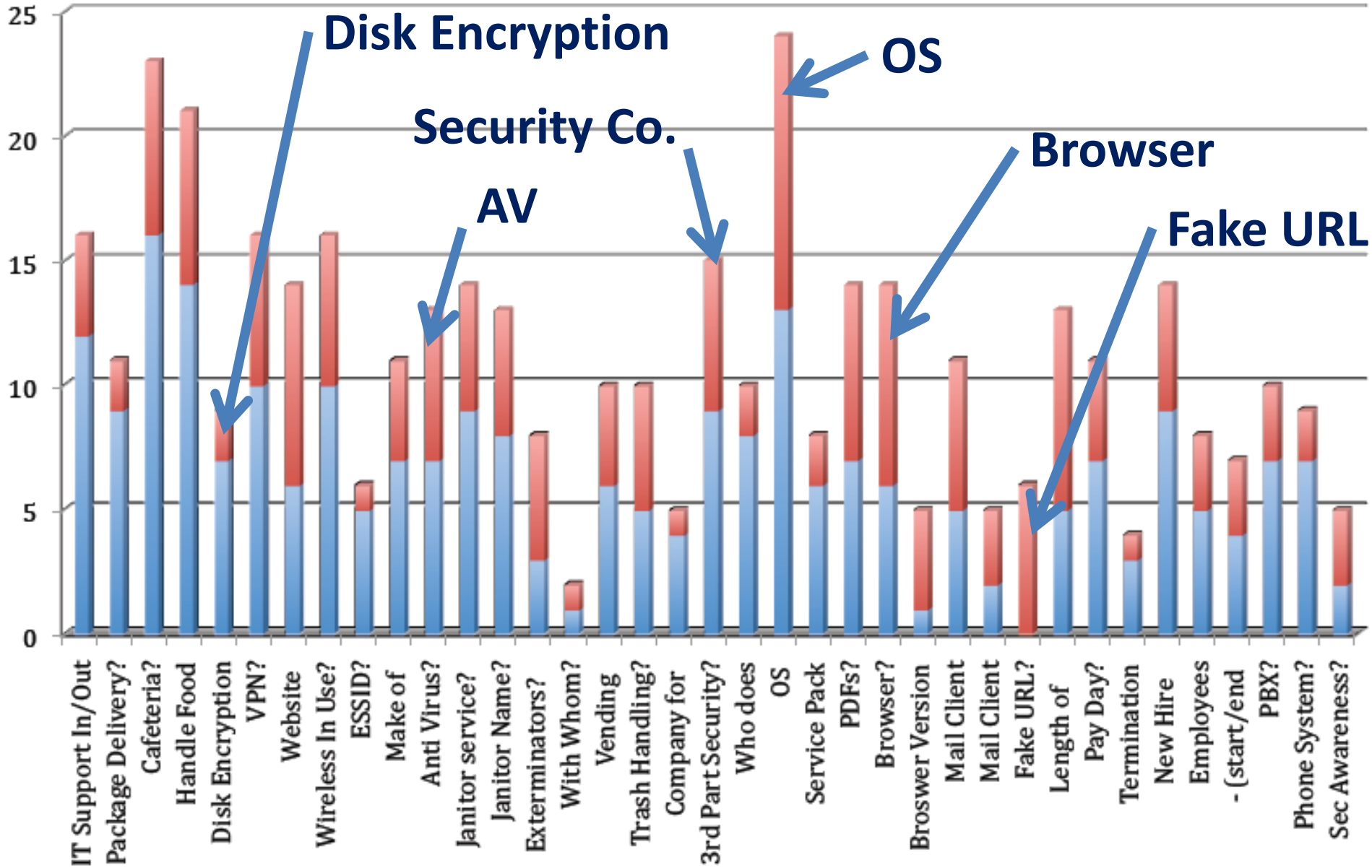
Change Behavior. Reduce Risk.

1 Social-Engineering.org, DEFCON 20 Social Engineering CTF 2012

What did they find through research?



What else did they get on the phone?



Pretexts Used

Who is the most susceptible?

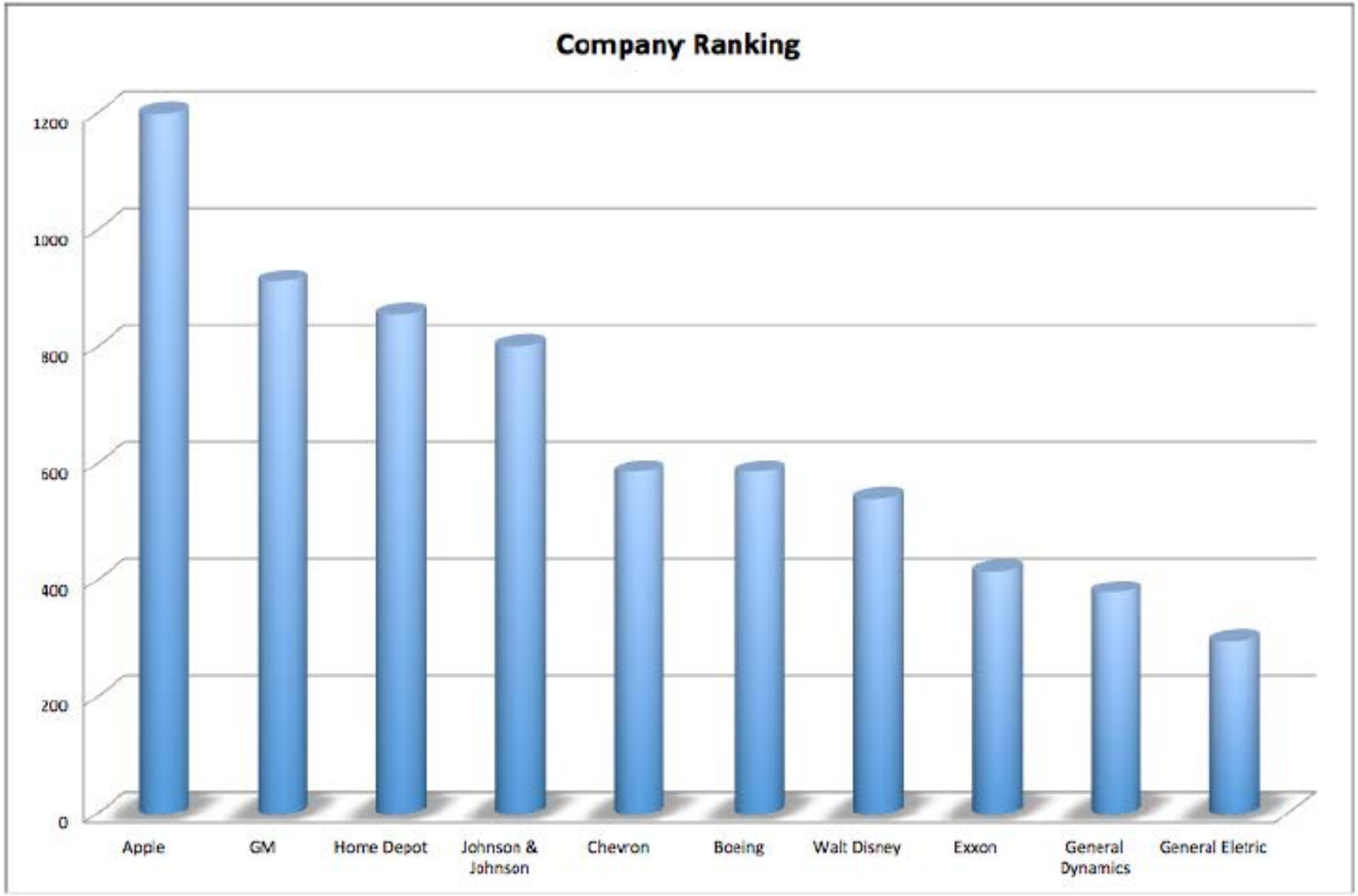


Figure 8: 2013 SECTF Target Company Performance

Results

- Improvement in contestants perparation
- Higher number of “unskilled”or “inexperienced callers”
- More advanced pretenses
- More information available on line
- No improvement by companies to better educate or prepare for social engineering attacks

wombat security technologies

Change Behavior. Reduce Risk.

Social Engineering Scenarios

- Email
- In-person
- Smartphone
- Social networking
- Snail mail
- Fixed phone

wombat security technologies

Change Behavior. Reduce Risk.

Social Engineering Roads Converge

- The end user is the target
- Exploits human weakness
- The end user is the problem
- Technology can’t solve the issues
- Countermeasures must be taken

wombat security technologies

Change Behavior. Reduce Risk.

Increasingly Sophisticated Attacks

- Spear-phishing targeting specific groups or individuals
- Leveraging information about your organization, group or you
- No more misspellings or easy red flags
- Social phishing 4 to 5 times more effective

Bob Smith is retiring next week, click here to say whether you can attend his retirement party

Email subpoena from the US District Court in San Diego with your name, company and phone number, and your lawyers name, company & phone number…

Would you fall for this?

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hello,

Please read the following article, it's very important :

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

Someone You Know

Generic Title

Link Looks Legitimate

Change Behavior. Reduce Risk.

1 **Source: Slate.com Would you click the link in this email that tricked the AP? April 23, 2013**

Technology Alone Won't Work

- Tempting to just buy software or hardware that promises to solve these problems
- Many social engineering scenarios are not impacted by technology
- Attackers are very resourceful, constantly looking to circumvent defenses
- Security controls lag behind technology adoption

wombat security technologies

Change Behavior. Reduce Risk.

Training has a Big Role to Play

- Lack of understanding of risks
- Wide range of scenarios

What if you combine education & assessments?

in

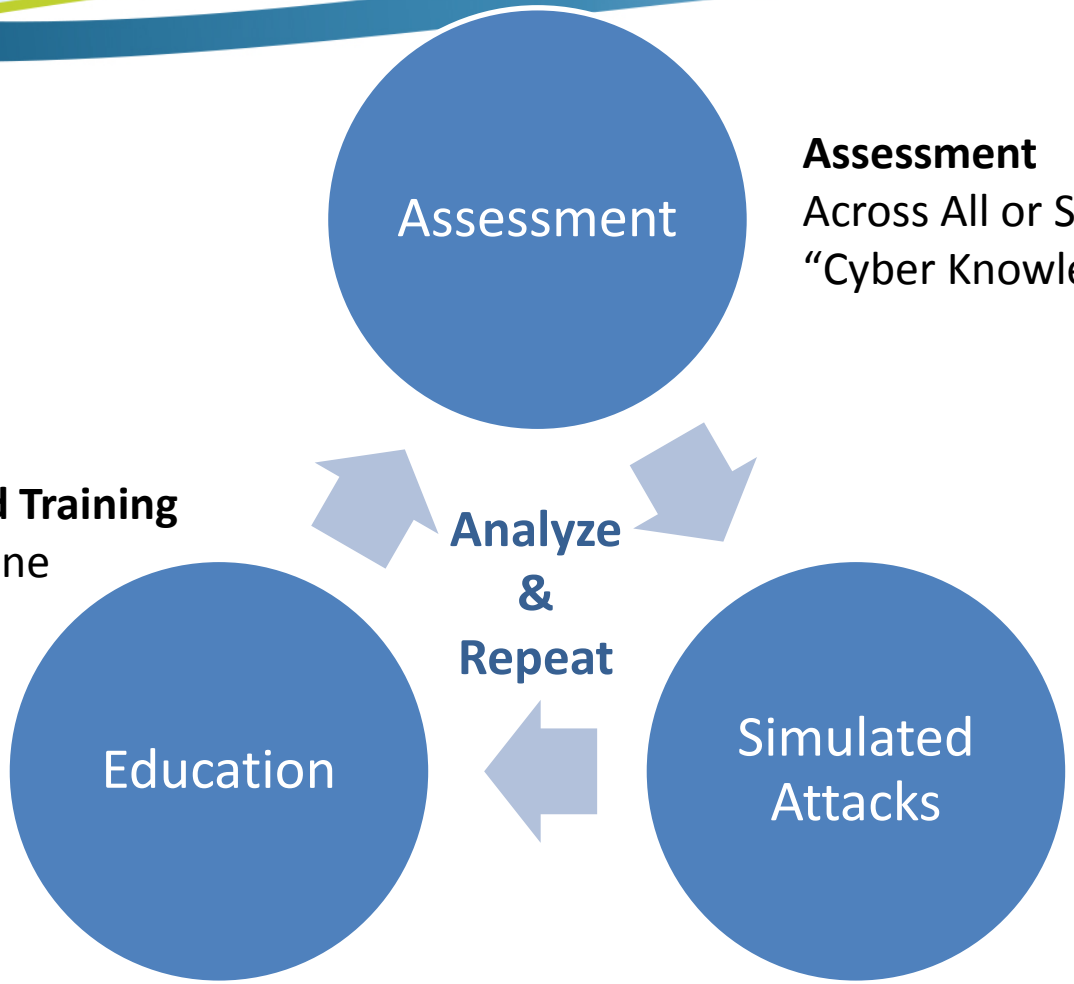
educating staff about security risks"

PWC Information Security Breaches Survey (April 2012)

wombat security technologies

Change Behavior. Reduce Risk.

Continuous Training Methodology



Assessment
Across All or Some Topics
"Cyber Knowledge"

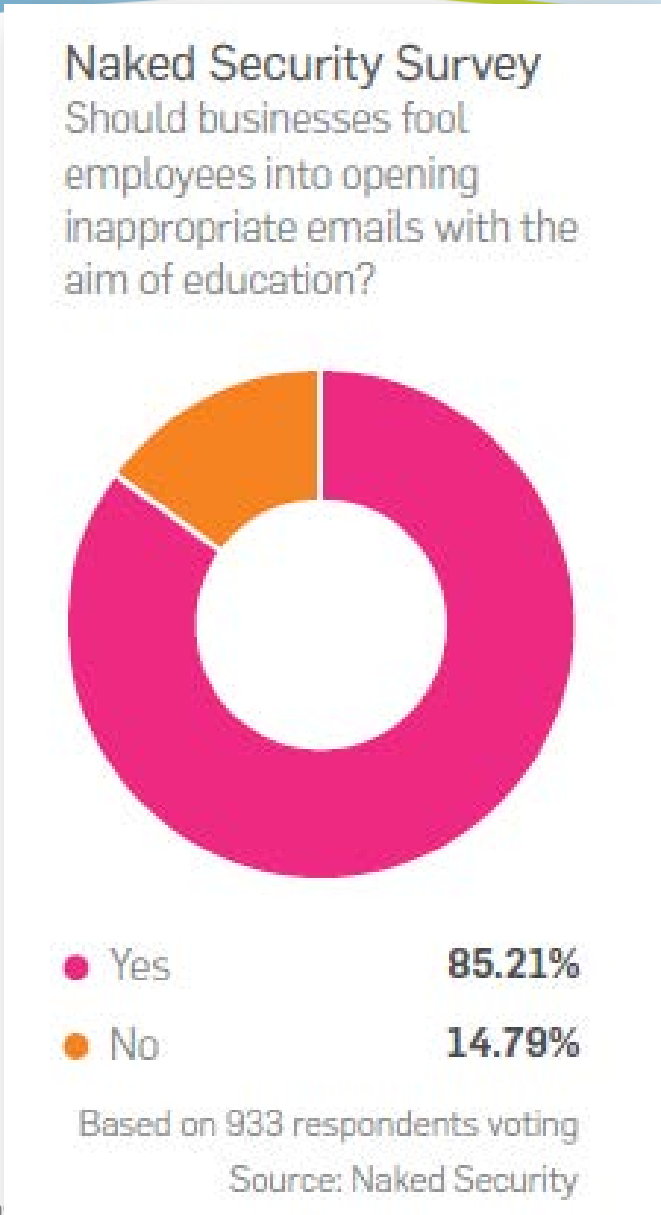
Scheduled Training
for Everyone

Simulated Attacks
Email, Smish,
Memory Device

wombat security technologies
Change Behavior. Reduce Risk.

Social Engineering Assessments

- **Links education & assessments**
- **Automates much of the process with do-it-yourself capabilities**
- **Detailed reports to develop & target training**
- **Attack services covering:**
  - email phishing attacks
  - memory device attacks
  - SMS/text message attacks



Wombat's Definition of Effective Training

Present concepts and procedures together

Bite-sized lessons

Learn by doing

Story-based environment

Create teachable moments

Provide immediate feedback

Use conversational content

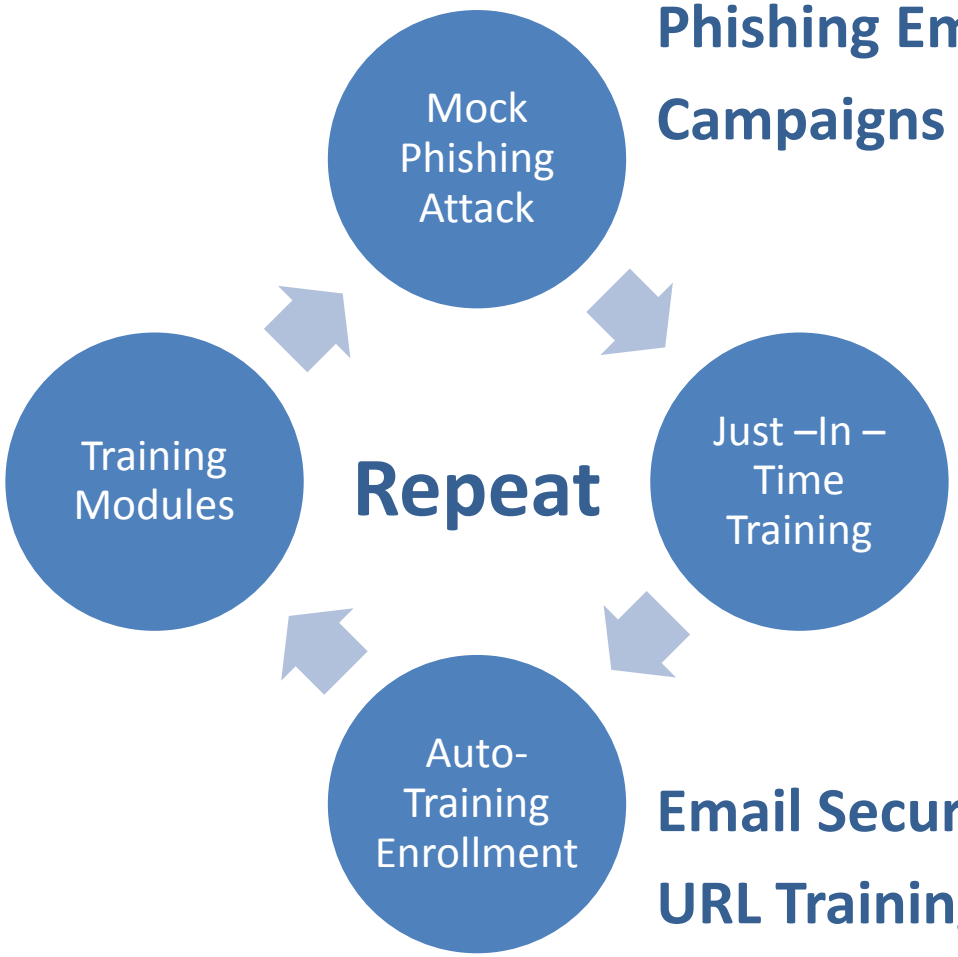
Collect valuable data

http://villageville.com@highscores.net/h37shgkldhs8

wombat technologies

Reduce Risk.

Results of Continuous Training



Phishing Email Campaigns

Email Security URL Training

Over 80% Reduction

35% Failure 1st Campaign

6% Failure 2nd Campaign

wombat security technologies

Change Behavior. Reduce Risk.

SECTF Winners

• Target Companies	10
• Number of Contestants	20
• Completed calls	51
• Possible flags	37
• Men vs Women	10/10
• Points for Men	2991
• Points for Women	3579

wombat security technologies

Change Behavior. Reduce Risk.

Conclusions

- Social engineering is a large & growing risk
- Your end users are the target
- Mitigation strategy is through policies and ongoing education & assessments

"There is a direct correlation between companies that provide frequent awareness training and the amount of information a company gives up."(1)

Change Behavior. Reduce Risk.

1 Social-Engineering.org, DEFCON 20 Social Engineering CTF 2012

wombat®
security technologies

Ralph Massaro
r.massaro@wombatsecurity.com