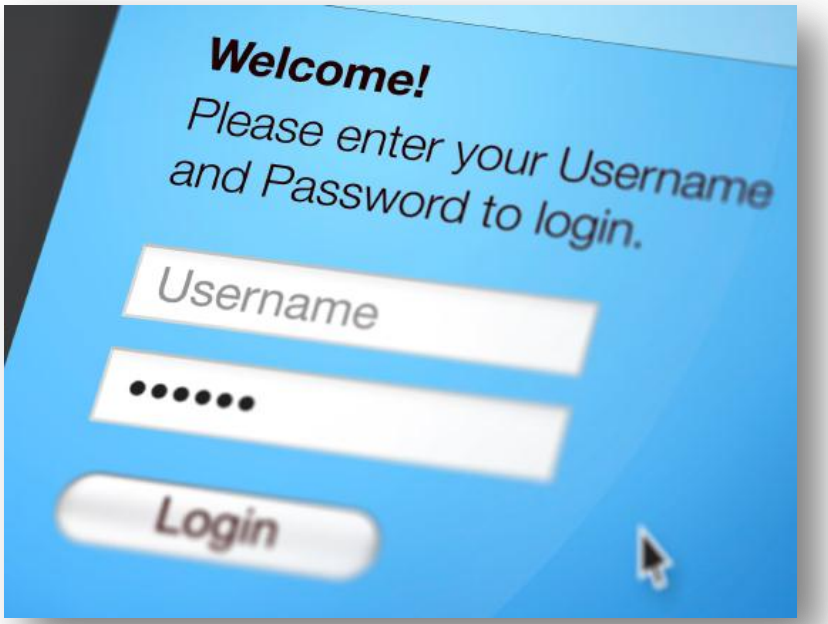
wombat®
security technologies

Social Engineering & How to Counteract Advanced Attacks

Joe Ferrara, President and CEO
Wombat Security Technologies, Inc.

Agenda

- Social Engineering
- DEFCON Competition
- Recent Examples
- Countermeasures



wombat security technologies
Change Behavior. Reduce Risk.

What is Social Engineering?

- The art of manipulating people into performing actions or divulging confidential information
- An act of psychological manipulation
- Originally was “engineering society to cause a favorable change”

wombat security technologies

Change Behavior. Reduce Risk.

How Large is the Problem?

- 91% of targeted attacks involve spear-phishing emails (1)
- 29% of breaches in 2012 leveraged social tactics (2)
- 31% of mobile users received a text from someone they didn't know requesting that they click a link or dial an unknown number (3)

wombat security technologies

Change Behavior. Reduce Risk.

1 Trend Micro, November 2012
2 Verizon Data Breach Investigations Report 2013
3 Cloudmark, September 2012

Social Engineering Scenarios

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

ombat®
urity technologies
vior. Reduce Risk.

DEFCON 20 Competition

- 20 social engineers
- 10 target companies
- Research & phone calls only
- Points for data captured
- Strict rules in place

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

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

Competition Process

- Target industries – freight, telecom, oil, retail & 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.

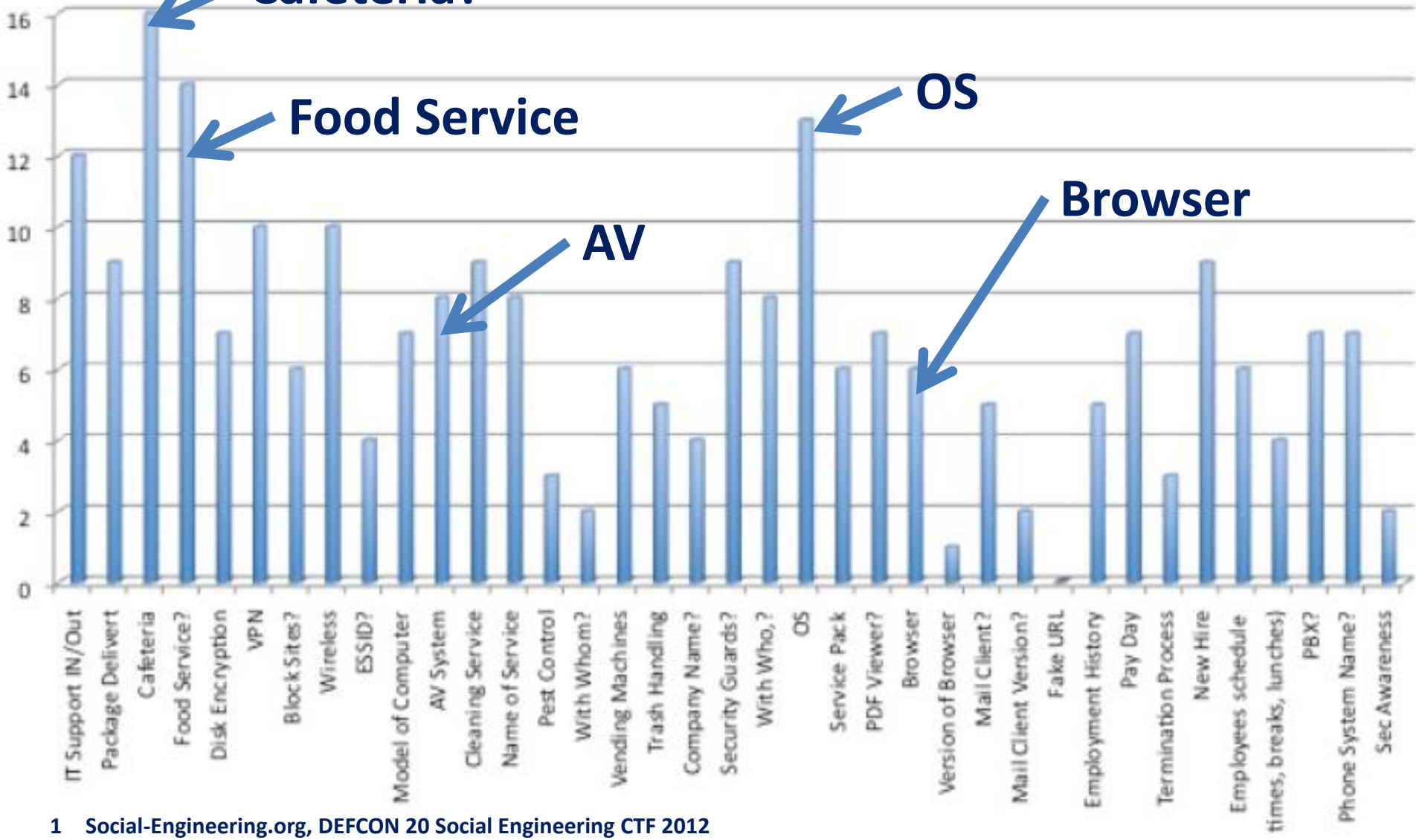
What were they looking for?

- 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

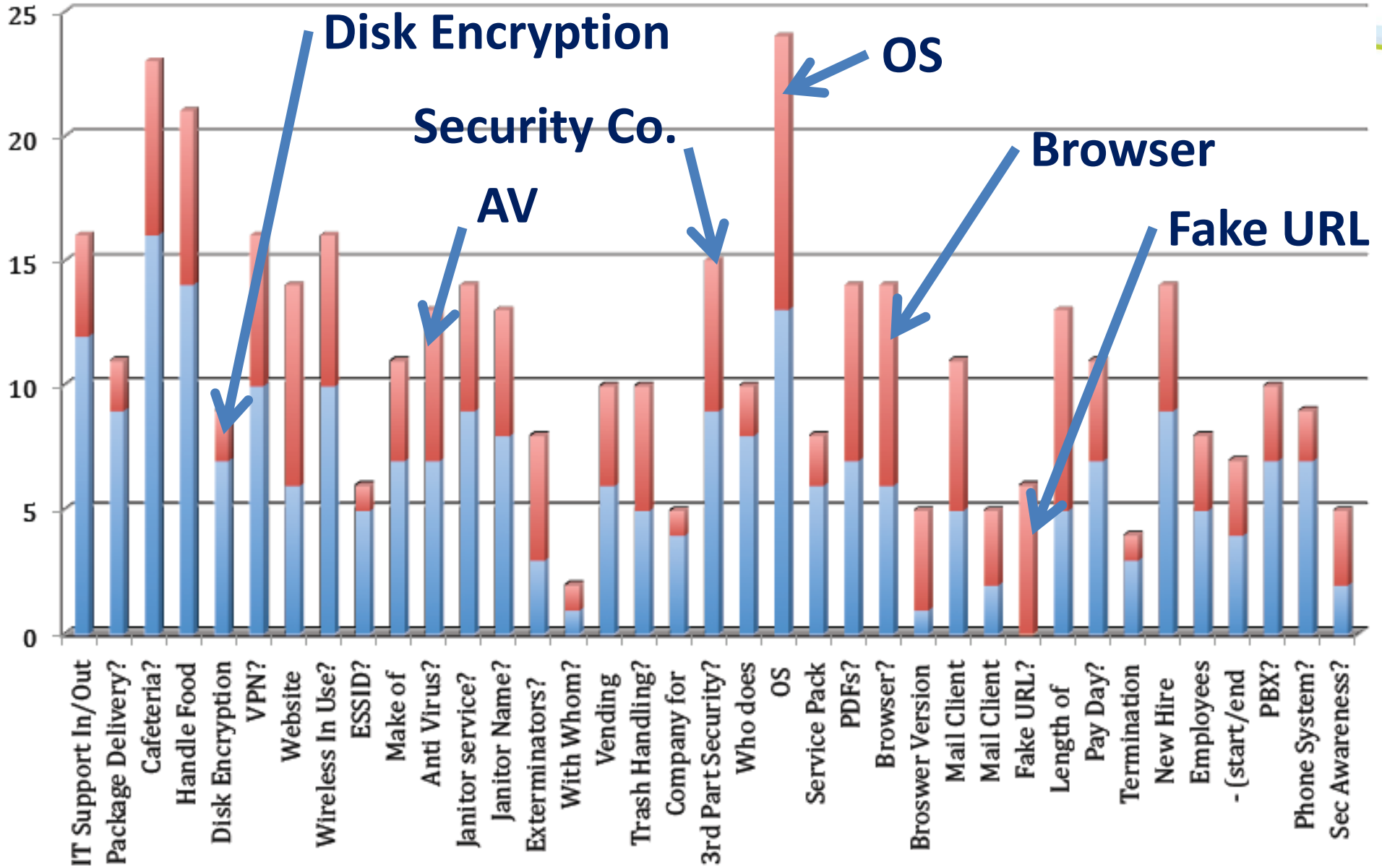
Change Behavior. Reduce Risk.

What did they find through research?



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

What else did they get on the phone?



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

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.

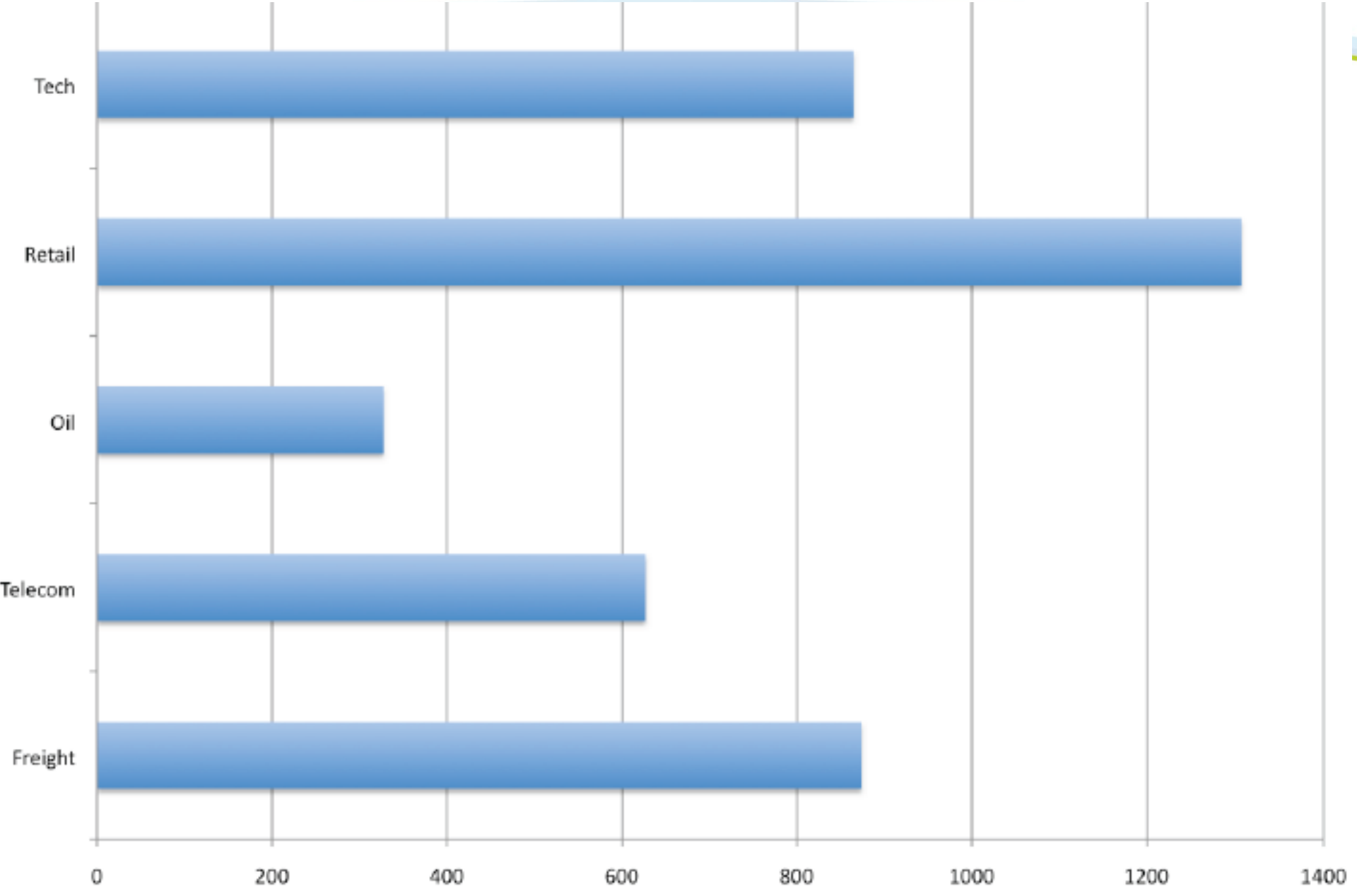
1 Social-Engineering.org, DEFCON 20 Social Engineering CTF 2012

Pretexts Used

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

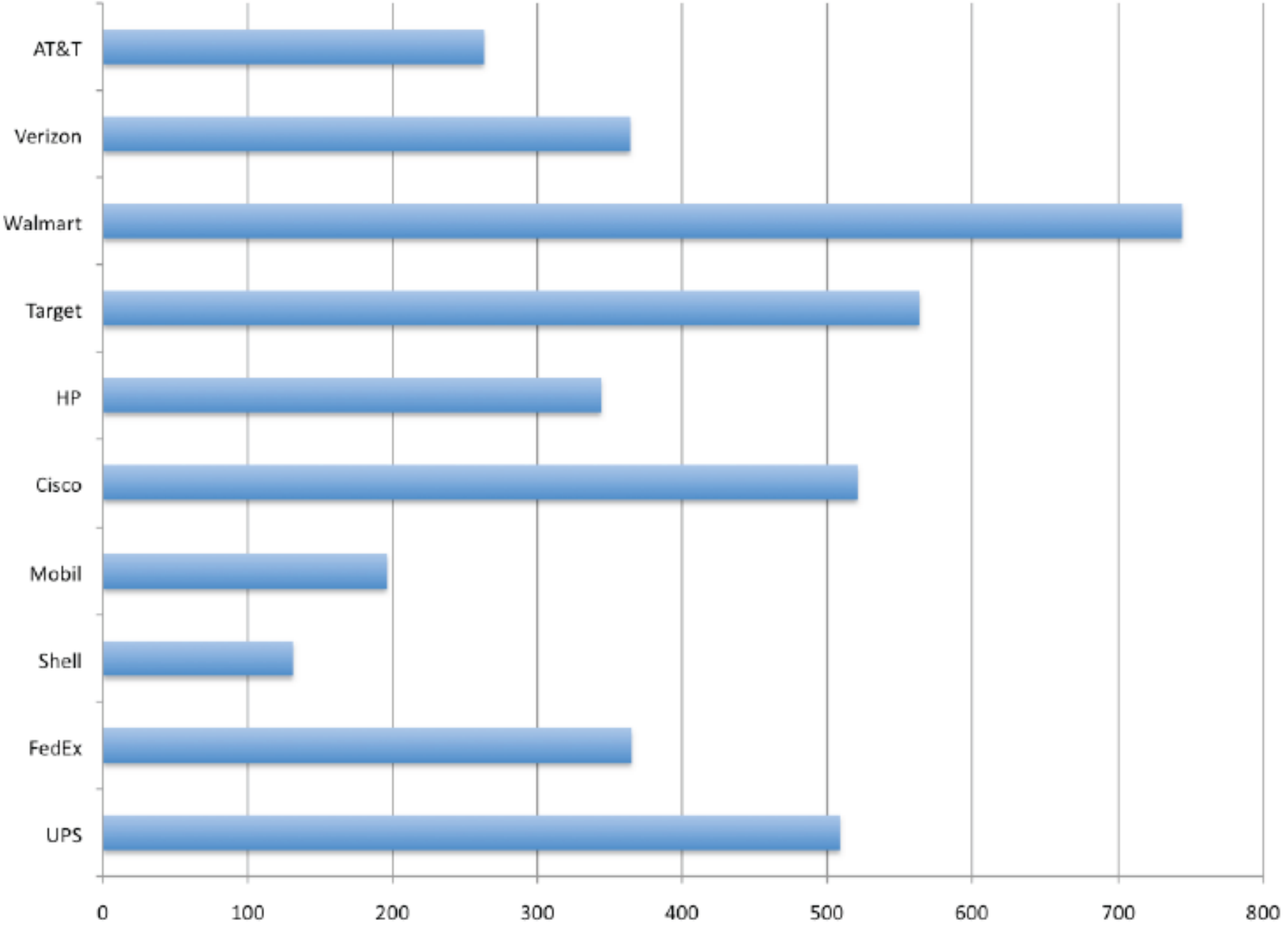
Scores by Industry

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



Scores by Company

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



Recent Attacks

- Email
- Smartphone
- Social networking

wombat security technologies

Change Behavior. Reduce Risk.

Would you fall for this?

Change Behavior. Reduce Risk.

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

Phishing led to AP Twitter Hack

- April 23rd Attack
- Phishing on corporate network first
- AP's Twitter & Mobile Twitter accounts compromised
- False tweet about White House attack (1pm)
- Dow immediately fell by 1%

wombat security technologies

Change Behavior. Reduce Risk.

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

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…

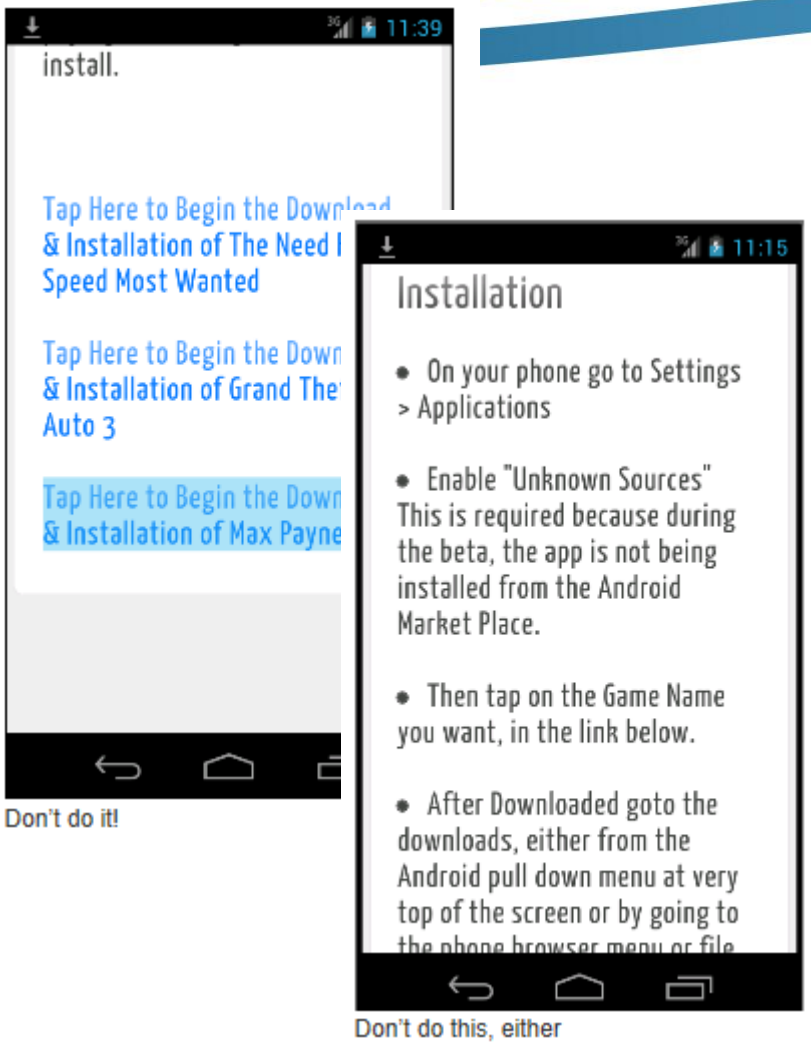
Mobility Adds New Challenges

- App downloads (1)
  - Lack of understanding of permissions
  - Relying on word of mouth and ratings
- Email Phishing (2)
  - Worse on mobile phones
  - Mobile phones first to arrive at phishing websites
  - 3x more likely to submit credentials
- SMS attacks
  - Smishing, links, calls

1 P. Gage Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone", USEC2012.
2 Trusteer, Jan. 2011 – similar

wombat security technologies
Change Behavior. Reduce Risk.

Android Trojan Creates SMS Botnet



Don't do it!

Don't do this, either

- Random SMS invitation to download a free Android game
- Unknowingly loading malicious software
- Turns handset into a simple botnet
- Sending SMS malware based on instructions from a command and control server

1 Cloudmark, December 2012

wombat security technologies

Change Behavior. Reduce Risk.

SMS/Text-based Attacks

- September 2012 - 913% increase in the volume of SMS phishing attempts
- Surge appears to be the result of a single set of attacks with over 500 unique phishing pitches
- Simplistic attack message:

  Fwd: Good Afternoon. Attention Required. Call (xxx)xxx-xxxx

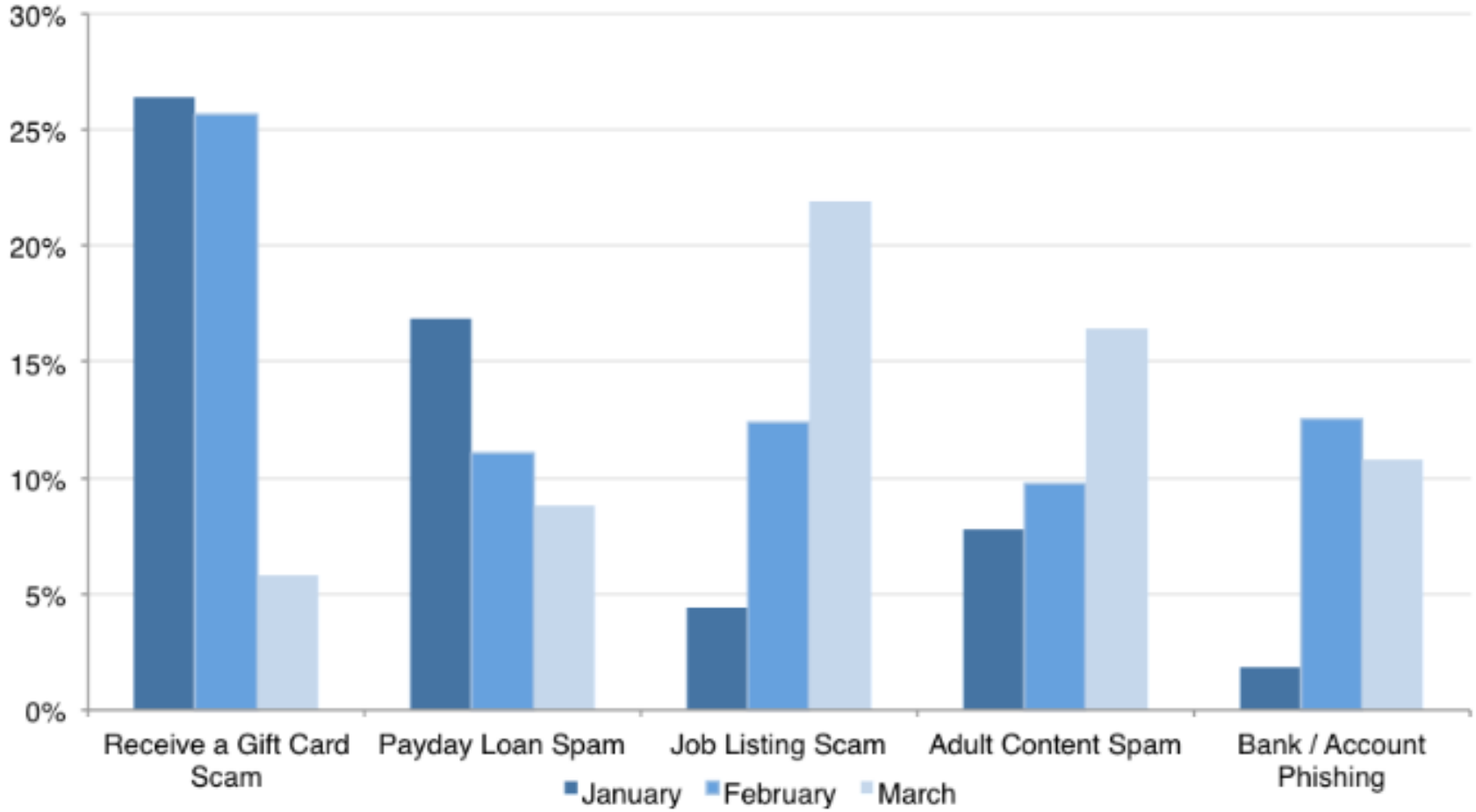
1 **Cloudmark, September 2012**

wombat security technologies

Change Behavior. Reduce Risk.

Q1 2013 Text-Based Attacks

Figure 2. Monthly Volumes of the Quarter's Top 5 Attack Types, 1Q13
Source: Cloudmark / GSMA



1 Cloudmark / GSMA, April 2013

Social Networking Attacks

- 15% users had profile hacked & impersonated (1)
- 10% of users fell victim to scam or fake link (1)
- Recent Login & Malware Scams:
  - Facebook – “You were violating policies”
  - Twitter – “Someone saying nasty things about you”
  - LinkedIn: “Fake employee event invitations”

wombat security technologies

Change Behavior. Reduce Risk.

1 **Norton, September 2012**

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

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.

Mitigation Recommendations

- **Social Media Policies**
  - If you don't have one, get one
  - Clear definitions of what is allowed and not allowed
  - Business use versus personal use
- **Consistent, Real World Education**
  - Quality, meaningful, security awareness education
  - Consistent & frequent to keep topics top of mind
- **Regular Risk Assessments and Penetration Tests**
  - Social engineering risk assessments & penetration tests
  - Results to develop & target training and prepare for attacks

wombat security technologies

Change Behavior. Reduce Risk.

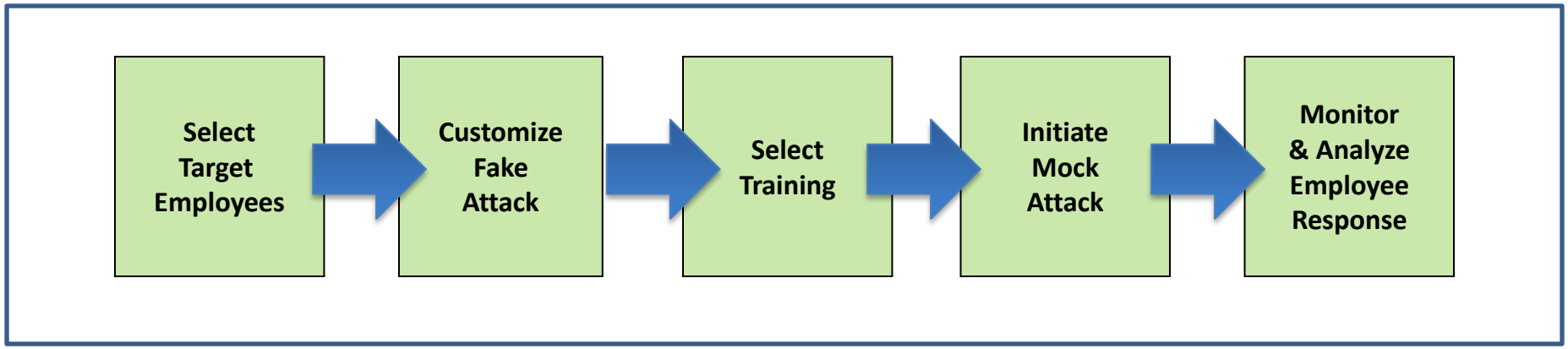
Mitigation Steps

- **Social Media Policies**
  - Research, create & distribute new policy
- **What if you combine education & assessments?**
  - Security consulting companies
  - Vendor solutions

wombat security technologies
Change Behavior. Reduce Risk.

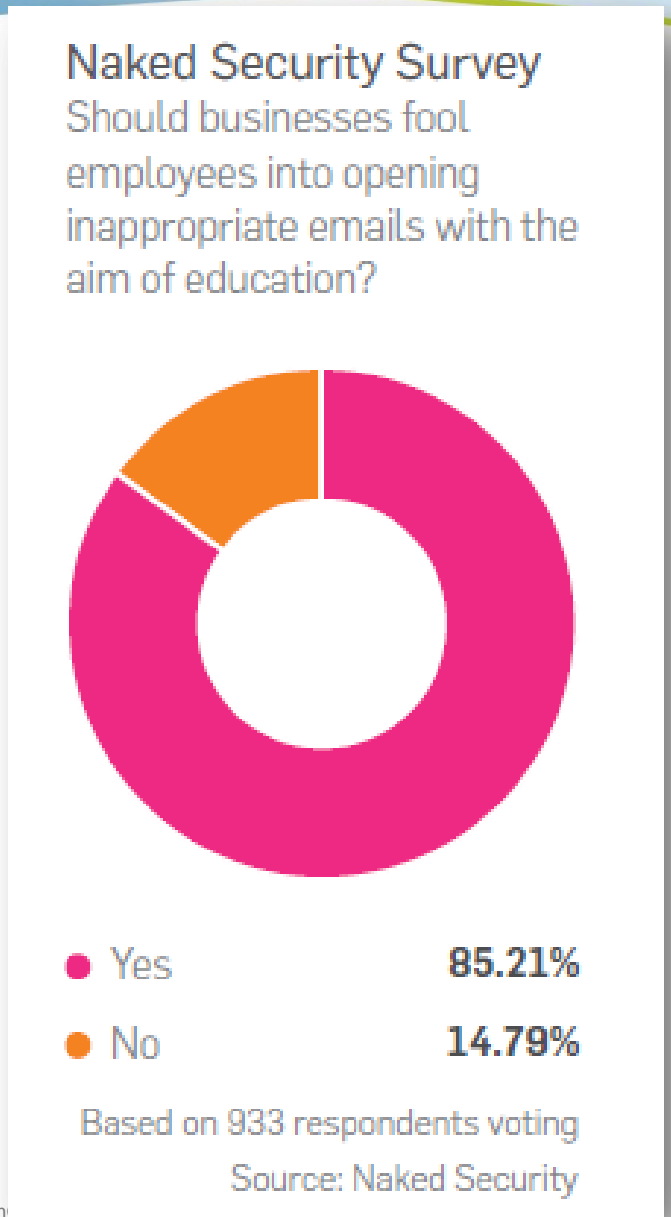
Training via Simulated Attacks

- Training as part of daily routine
- Just-in-time training for those that fall for attack
- Creates a unique “teachable moment”
- Significantly increases training penetration
- Provides detailed reporting & metrics

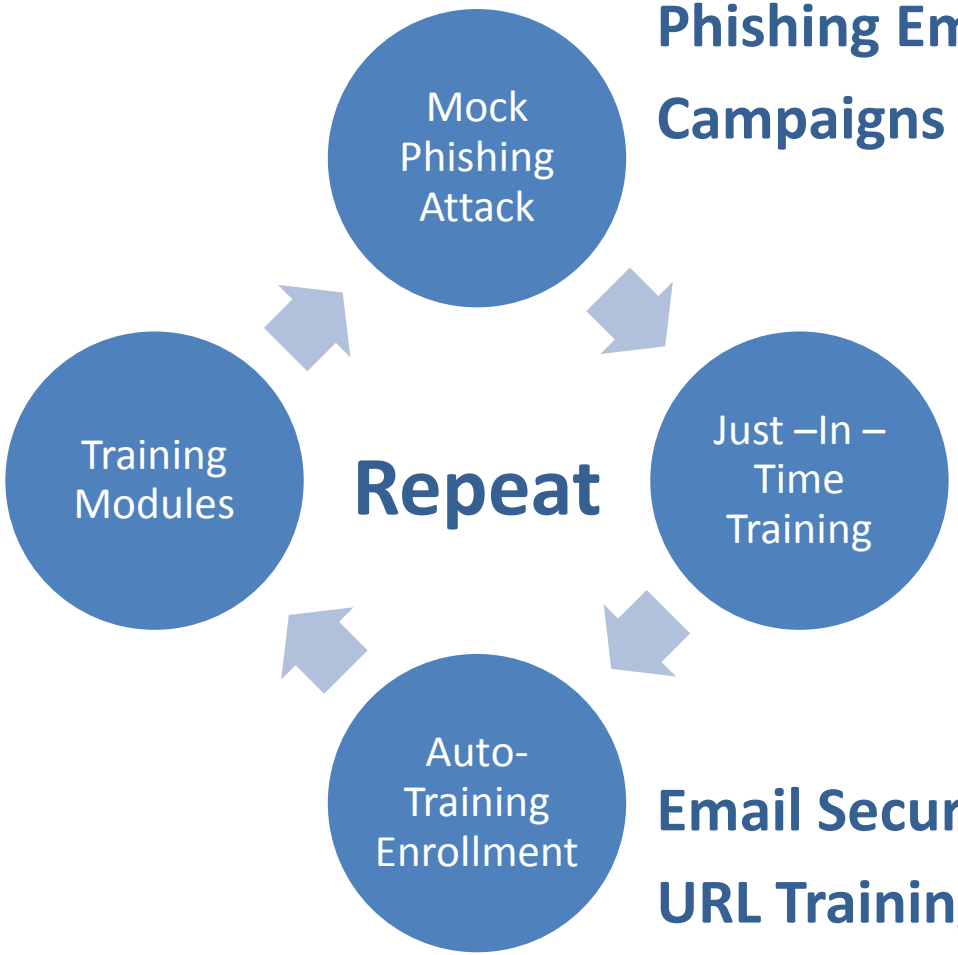


Social Engineering Assessments

- **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



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.

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