SOCIAL ENGINEERING

Grant Thornton

An instinct for growth™

anaplan

Jake Johnson

Sixto Bernal

AGENDA

What is social engineering?

Current events

Social engineering risks

Mitigation Strategies

Q&A

WHAT IS SOCIAL ENGINEERING?

- The Art of Deception, Kevin Mitnick:

  "Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."

- Wikipedia:

  "refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

EARLY EXAMPLES OF SOCIAL ENGINEERING

- Used everyday by everyday people in everyday situations.

  Promotion, Free Pizza, Dating

- The Trojan Horse
- Steve Wozniak and Steve Jobs - Blue Box

  1960s and 1970s – generates same tones as operator's dialing console to make long distance calls

- Kevin Mitnick – Phone Phreaking

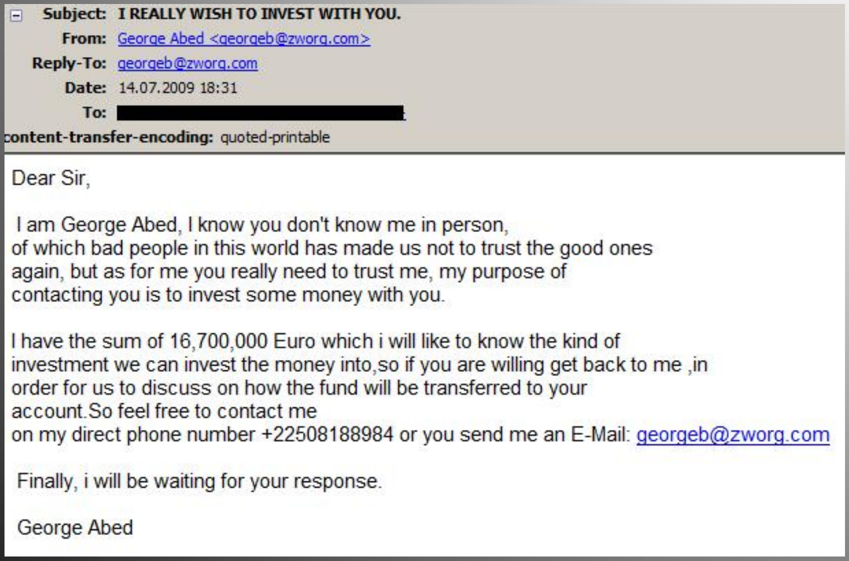
  Using "lingo" or "talk the talk" to exploit the phone systems and phone company employees

GREATEST THREATS

- 1 out of every 500 emails contain confidential data.
- 66% say co-workers, not hackers, pose the greatest risk to consumer privacy.
- 46% say it would be "easy" to "extremely easy" for workers to remove sensitive data from the corporate database.
- 32% are unaware of internal company policies to protect customer data.

http://financialservices.house.gove/media/pdf/062403ja.pdf – http://go.Symantec.com/vontu/

CURRENT EVENTS – EMAIL SCAMS



Subject: I REALLY WISH TO INVEST WITH YOU.
From: George Abed <georgeb@zworg.com>
Reply-To: georgeb@zworg.com
Date: 14.07.2009 18:31
To: [redacted]
content-transfer-encoding: quoted-printable

Dear Sir,

I am George Abed, I know you don't know me in person,
of which bad people in this world has made us not to trust the good ones
again, but as for me you really need to trust me, my purpose of
contacting you is to invest some money with you.

I have the sum of 16,700,000 Euro which i will like to know the kind of
investment we can invest the money into,so if you are willing get back to me ,in
order for us to discuss on how the fund will be transferred to your
account.So feel free to contact me
on my direct phone number +22508188984 or you send me an E-Mail: georgeb@zworg.com

Finally, i will be waiting for your response.

George Abed

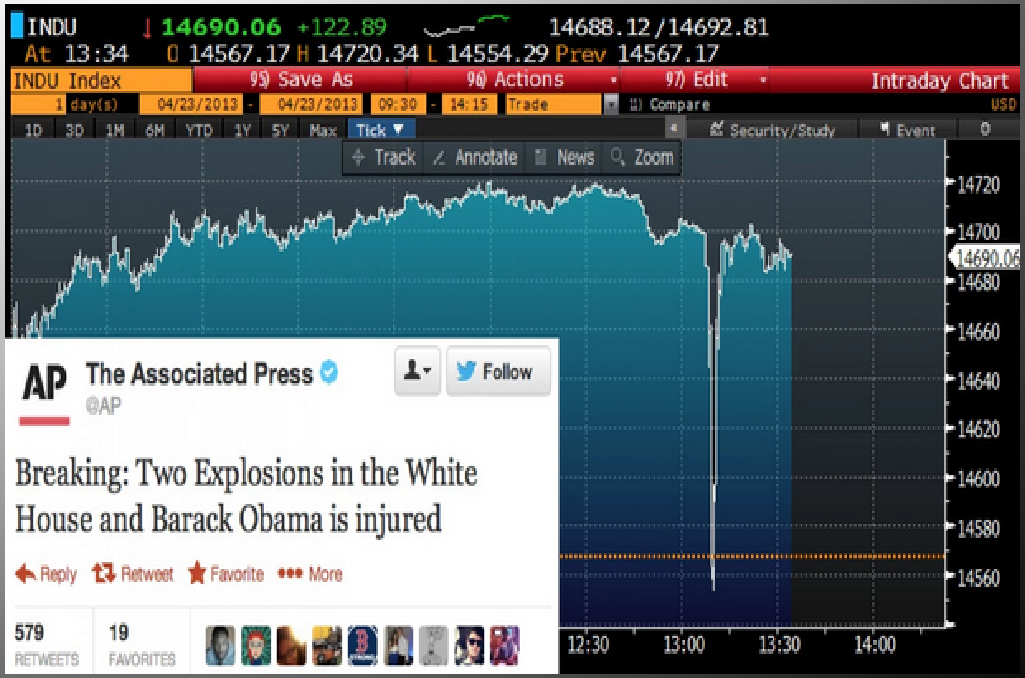
- The 419 Scam or Nigerian Scam
  - Losses from totaled $12.7 billion in 2013
    - $82 Billion in Losses to Date
  - 800,000 Organized Perpetrators
    - Growing 5% Annually
  - 2013: people in the U.S., the U.K., and India fell for the most scams
  - Scam range from $200 to $12 Million

http://www.geektime.com/2014/07/21/millions-of-victims-lost-12-7b-last-year-falling-for-nigerian-scams/

CURRENT EVENTS (CONT'D)

Associated Press Twitter Hijack

- 2013, Twitter Account Hacked by Syrian Electronic Army
- Within 3 minutes, the fake tweet erased $136 billion in equity market value
  - Tweet sent at 1:07 p.m.
  - 1:08 p.m. the Dow started the nosedive
  - Dropped 150 points before 1:10 p.m.



The Associated Press
@AP

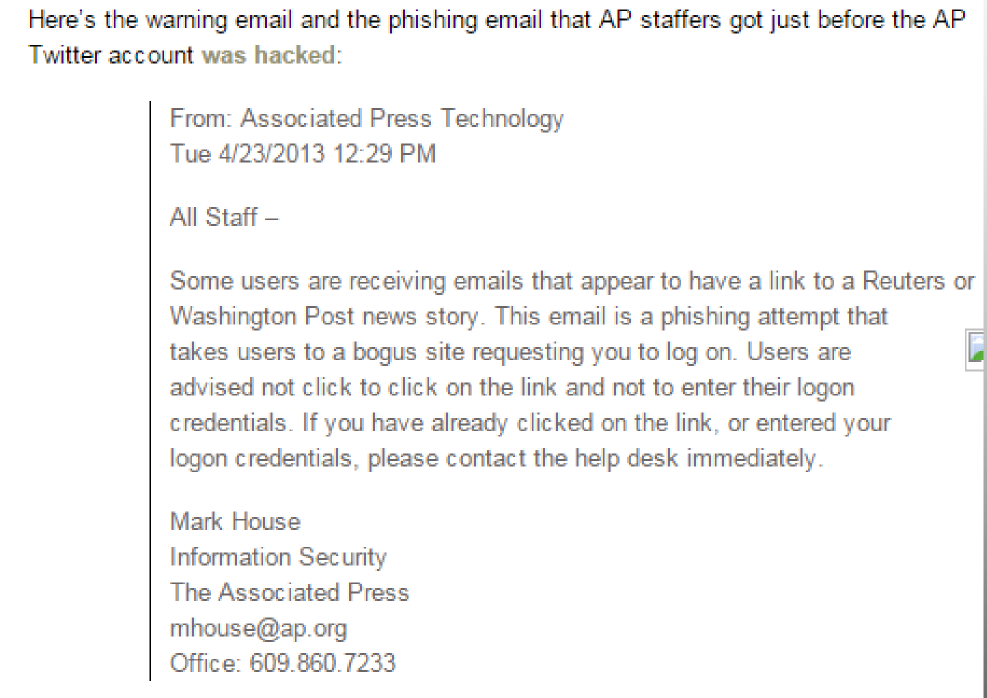
Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

579 RETWEETS 19 FAVORITES

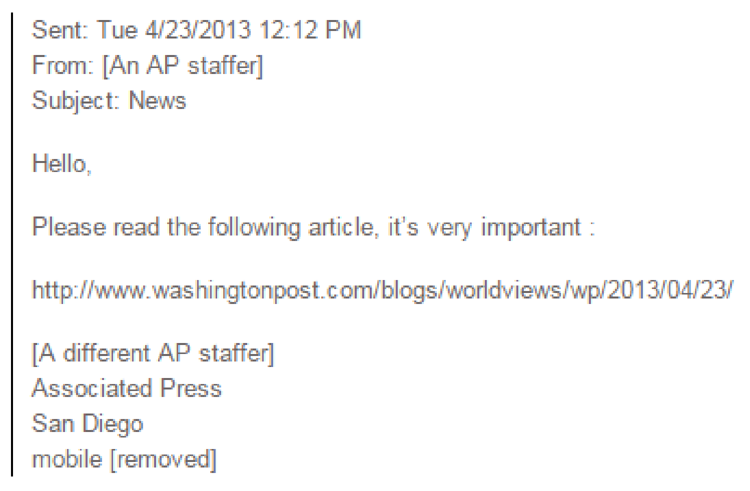
https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Associated Press Twitter Hijack



Here's the warning email and the phishing email that AP staffers got just before the AP Twitter account was hacked:

> From: Associated Press Technology
> Tue 4/23/2013 12:29 PM
>
> All Staff –
>
> Some users are receiving emails that appear to have a link to a Reuters or Washington Post news story. This email is a phishing attempt that takes users to a bogus site requesting you to log on. Users are advised not click to click on the link and not to enter their logon credentials. If you have already clicked on the link, or entered your logon credentials, please contact the help desk immediately.
>
> Mark House
> Information Security
> The Associated Press
> mhouse@ap.org
> Office: 609.860.7233



> 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]

http://jimromenesko.com/2013/04/23/ap-warned-staffers-just-before-ap-was-hacked/

CURRENT EVENTS (CONT'D)

RSA SecurID Breach

- Phishing email contained an excel sheet with a zero-day exploit
- RSA's parent company, EMC, spent $66 million recovering from the attack
- Information regarding their Two-factor authentication mechanism was compromised.

CURRENT EVENTS – USB DRIVES

- USB Drives
  - Can emulate a keyboard and issue commands on behalf of the logged-in user
  - Can spoof a network card and change the computer's DNS setting to redirect traffic
  - Can boot a small virus, which infects the computer's operating system prior to boot.

http://www.tripwire.com/state-of-security/security-data-protection/danger-usb/

CURRENT EVENTS – SOCIAL MEDIA

10/8/2015: SecureWorks Reports: Suspected Iran-Based Hacker Group Creates Network of Fake LinkedIN Profiles

- 204 Legitimate Accounts were associated with the fake accounts.
- The CTU believes that TG-2889's LinkedIN activity is the initial stage of the Op CLEAVER's fake resume submitter malware operation.

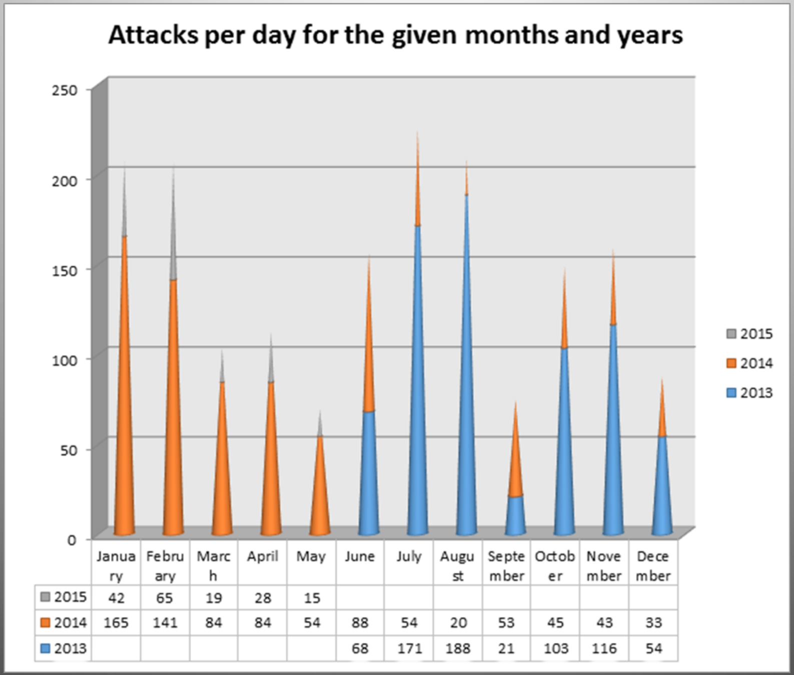
http://www.darkreading.com/vulnerabilities---threats/secureworks-reports-suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles-/d/d-id/1322553

SOCIAL ENGINEERING RISKS

- Cost of Breaches
  - 3.8 million victims attacked in 2014
  - $3.5 million is the average cost incurred by large companies in the wake of a cyber-attack in 2013
  - Average data breach costs about $145 per compromised record
  - mean time to identify a breach was 206 days
- Spear-phishing
  - 91% of cyberattacks and the resulting data breach begin with a spear phishing email in 2012
  - 94% of targeted emails use malicious file attachments

http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-reports-finance-related-malware-attacks-rose-28-m
http://www.darkreading.com/attacks-breaches/ponemon-cost-of-a-data-breach-rose-to-$35m-in-2013/d/d-id/1251019

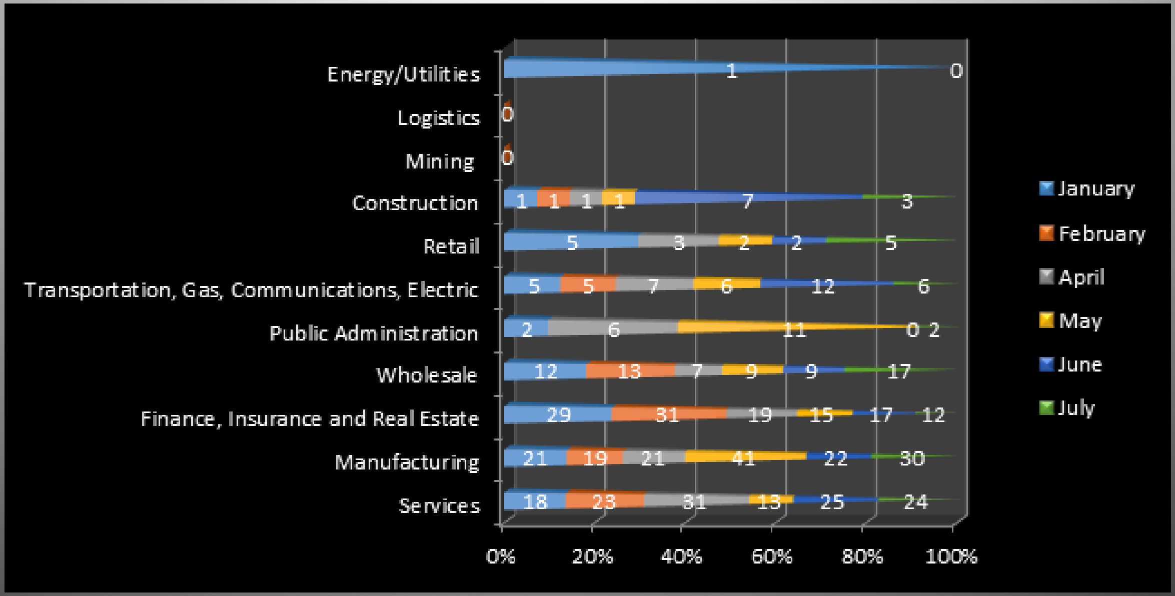
HOW WIDESPREAD IS SPEAR-PHISHING AND WHAT ARE THE ATTACK VOLUME TRENDS?



	January	February	March	April	May	June	July	August	September	October	November	December
■ 2015	42	65	19	28	15							
■ 2014	165	141	84	84	54	88	54	20	53	45	43	33
■ 2013						68	171	188	21	103	116	54

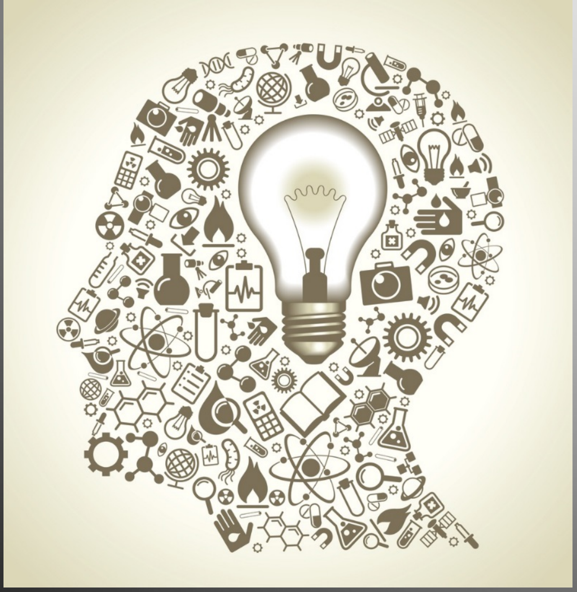
http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/

TOP TEN INDUSTRIES TARGETED BY SPEAR-PHISHING IN 2015



http://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/

MITIGATION STRATEGIES



- Knowledge is Power
- Realize we are all targets at all times
- Change your point of view
- Commitments from IT
- Train, Train, Train

REDUCE RISK

Creating and Maintaining a Security-Aware Culture

- Password Management
- Two-Factor Authentication
- Anti-Virus/Anti-phishing Defenses
- Change Management
- Information Classification
- Document Handling and Destruction
- Physical Security

http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html

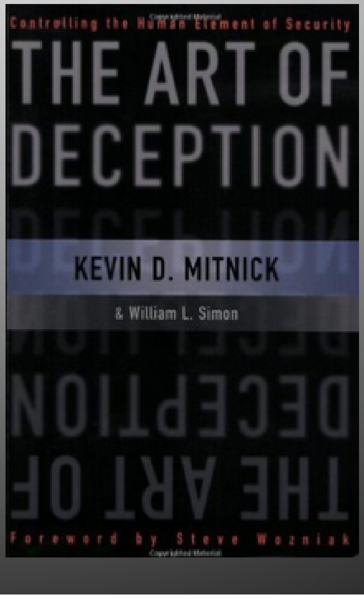
RESOURCES

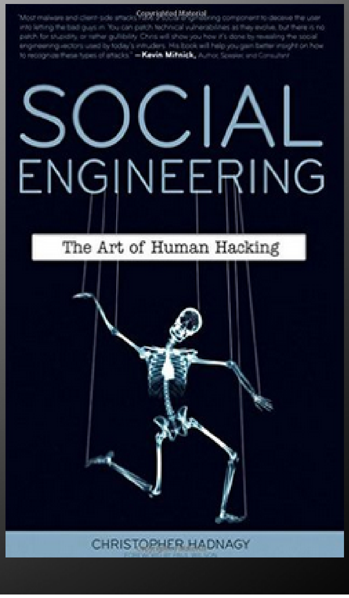
Mitnick, Kevin. The Art of Deception

Hadnagy, Christopher & Wilson, Paul. Social Engineering: The Art of Human Hacking

www.social-engineer.org

www.offensive-security.com


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak



QUESTIONS