A Brief Introduction to Phishing, Whaling & Social Engineering

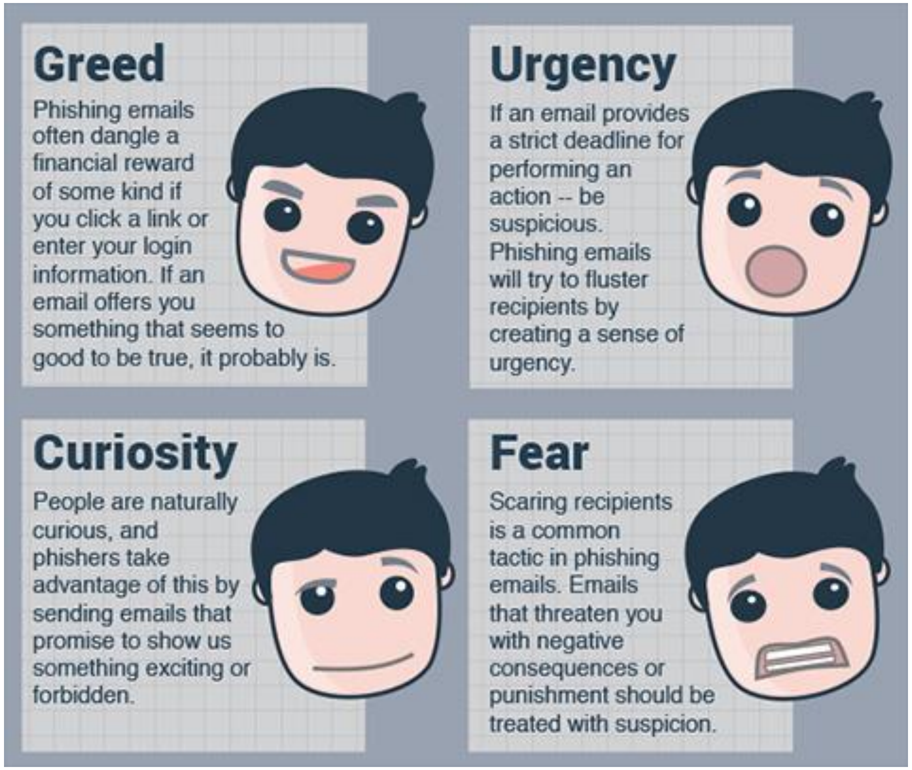
William Favre Slater, III
M.S., MBA, PMP, CISSP, SSCP, CISA, ITIL, IPv6
Senior IT Consultant in Cybersecurity
Chicago, Illinois
United States of America
slater@billslater.com
http://billslater.com/interview

Agenda

- What Is Phishing?
- What is Spear Phishing?
- What Is Whaling?
- What Social Engineering?
- Why Does Social Engineering Work?
- Recent Whaling Attack Examples
- How and Why Did the Recent Whaling Attack Work?
- How Does Can Your Security Staff Try to Protect Employees and Contractors?
- How to Protect Yourself and Your Company
- Conclusion
- Final Thoughts
- Questions

What Is Phishing?

- The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.



Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems to good to be true, it probably is.

Urgency

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.

Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.

Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

Source: http://www.wikipedia.org

What Is Spear Phishing?

- Phishing attacks directed at specific individuals, roles, or organizations are referred to as "spear phishing". Since these attacks are so pointed, attackers may go to great lengths to gather specific personal or institutional information in the hope of making the attack more believable and increasing the likelihood of its success.

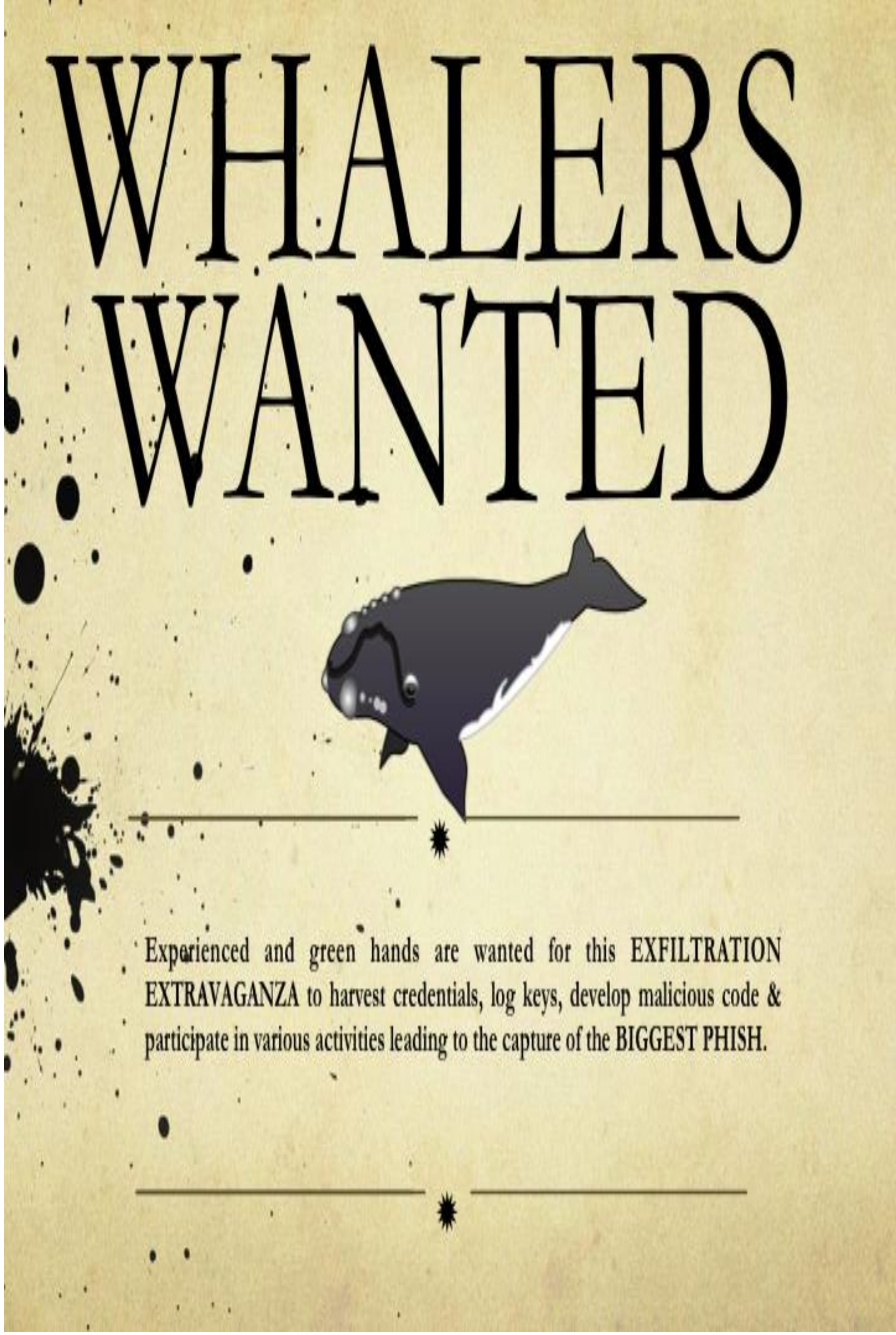
- The best defense against spear phishing is to carefully, securely discard information (i.e., using a cross-cut shredder) that could be used in such an attack. Further, be aware of data that may be relatively easily obtainable (e.g., your title at work, your favorite places, or where you bank), and think before acting on seemingly random requests via e-mail or phone.

Source: https://kb.iu.edu/d/arsf

What Is Whaling?

- The term "whaling" is used to describe phishing attacks (usually spear phishing) directed specifically at executive officers or other high-profile targets within a business, government, or other organization.

- A whaling attack is also known as a C-level fraud and BEC (business e-mail scam) and involves targeting high level executives with forged e-mails asking for urgent payments. Usually they are spoofed to appear to come from a trusted colleague or business partner.



Experienced and green hands are wanted for this EXFILTRATION EXTRAVAGANZA to harvest credentials, log keys, develop malicious code & participate in various activities leading to the capture of the BIGGEST PHISH.

Source: https://kb.iu.edu/d/arsf

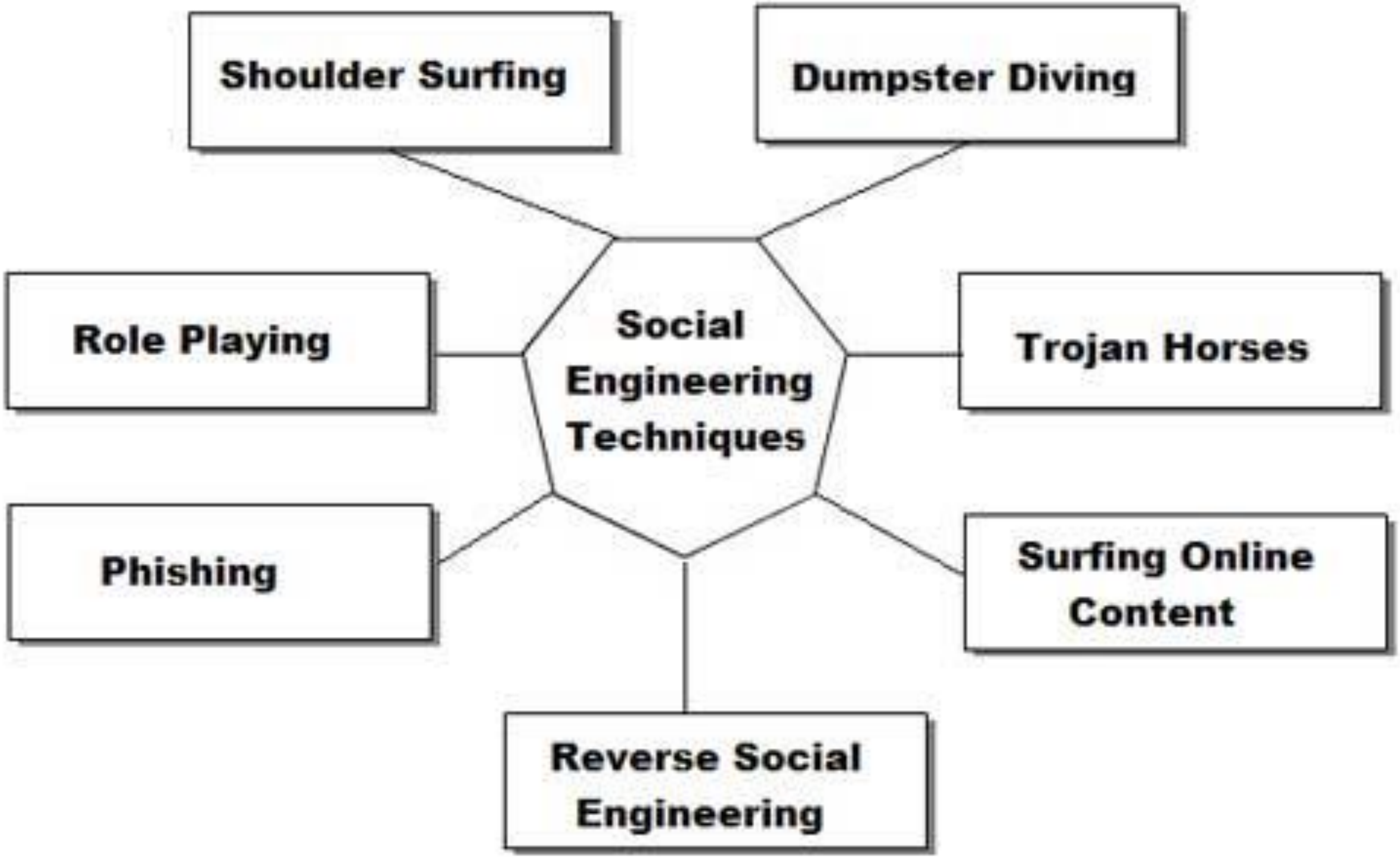
What Social Engineering?

- Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

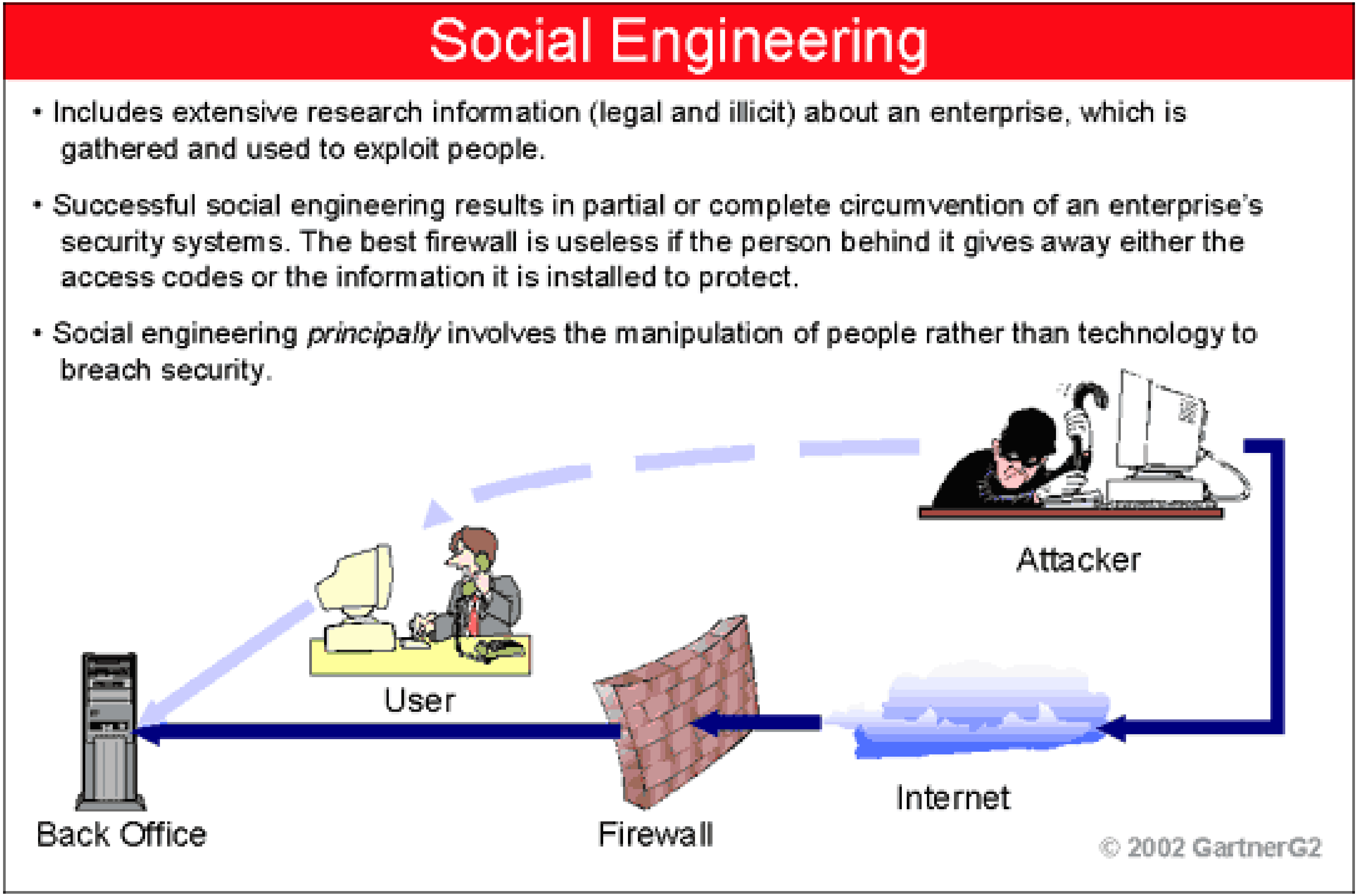
- Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Source: http://bit.ly/1U1cXFq

Social Engineering Techniques



Why Does Social Engineering Work?



Social Engineering

- Includes extensive research information (legal and illicit) about an enterprise, which is gathered and used to exploit people.
- Successful social engineering results in partial or complete circumvention of an enterprise's security systems. The best firewall is useless if the person behind it gives away either the access codes or the information it is installed to protect.
- Social engineering *principally* involves the manipulation of people rather than technology to breach security.

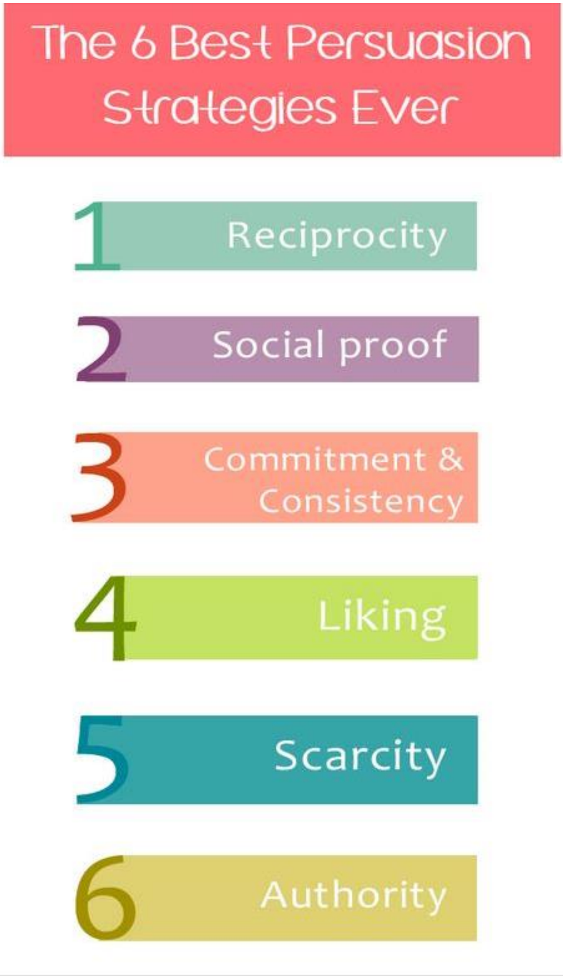
© 2002 GartnerG2

Why Does Social Engineering Work?

- **Pretexting:**
  - Much of the information required by Social Engineers to plan and launch a successful attack is easily available from:
    - Web Searches
    - Social networks and media
    - Loose documents carelessly left unprotected on your desk or in the open
    - Publically filed documents (Annual Reports, 10K statements, news releases, etc.)
    - Business cards
    - Dumpster diving
    - Shoulder surfing
    - Eavesdropping
    - Lost or misplaced documents

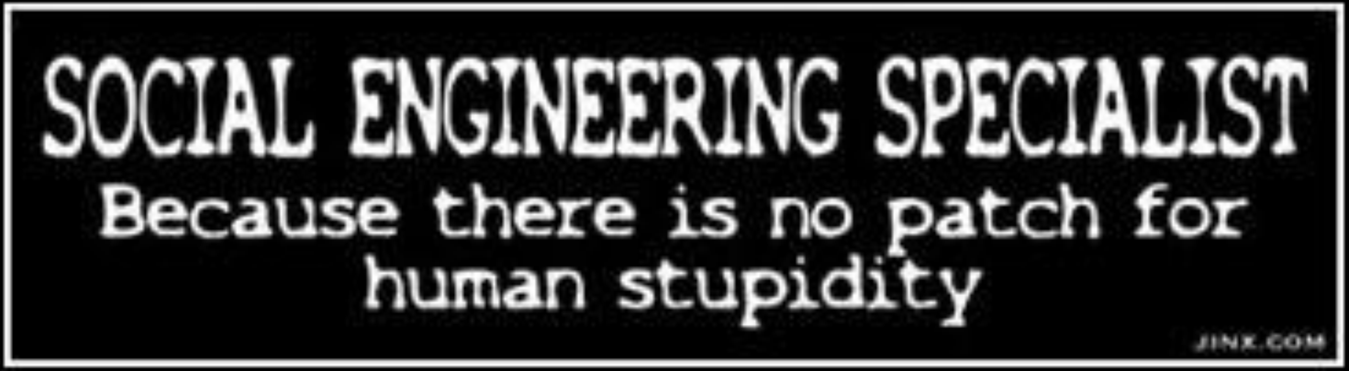
Why Does Social Engineering Work?

- **Humans *are* hackable**



The 6 Best Persuasion Strategies Ever

1. Reciprocity
2. Social proof
3. Commitment & Consistency
4. Liking
5. Scarcity
6. Authority



SOCIAL ENGINEERING SPECIALIST

Because there is no patch for
human stupidity

JINX.COM

Recent Whaling Attack Examples

Year of Attack	Year Detected	Company	Location	The Victims	Financial Impact(s)
2015	2016	Unknown	U.S. (Most likely NYC)	CEO	$98.9 million
2015	2016	FACC	Ried im Innkreis, Austria	CEO & CFO (both were later fired by the Board of Directors)	$46.5 million, AND 17% loss of stock value
2016	2016	Unnamed Company	Chicago, IL	Director & Manager	$14,500

Note: Each of these examples are valuable and "teachable moments" because by nature, they are rare and seldom, if ever, disclosed.

Recent Whaling Attack Example – Unknown American Company

- An unnamed American company fell victim to $98.9 million in CEO E-mail Fraud
- First discovered by a Bank in Cyprus
- $74 million was recovered
- This scam only surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover about $25 million held in at least 20 bank accounts around the world.

Source:
https://blog.knowbe4.com/us-company-falls-victim-to-100-million-ceo-e-mail-fraud

Recent Whaling Attack Example - FACC

- At FACC, an Austrian-based aircraft manufacturing company, both the CFO and the CEO, Walter Stephan, were fired after a successful whaling attack cost FACC € 40.9 million ($46.5 million) and wiped out the company’s annual profits.

- The fraud was discovered in January 2016.

- This publicly traded company also lost 17% of its market value.

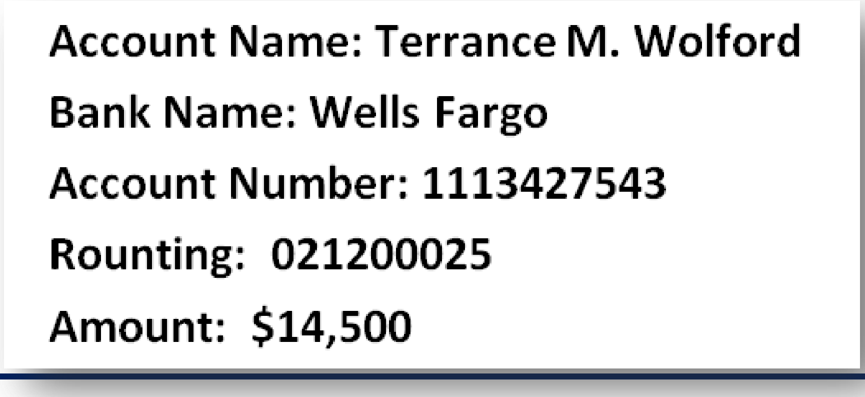
Source: SC Magazine
http://www.scmagazine.com/ceo-sacked-after-aircraft-company-grounded-by-whaling-attack/article/499258/

Recent Example – Unnamed Company in Chicago

- In May 2016, a manager at an unnamed company was contacted by an authentic looking e-mail from what was believed to be his boss, a Director.
- The e-mail was sent from the Director’s e-mail account, looked completely authentic, with an e-mail signature, and came from **INSIDE the unnamed company’s Infrastructure**.
- It directed an electronic funds transfer in the amount of $14,500 to a bank account at Wells Fargo.
- The manager unwittingly responded because the requester appeared to be a Director that he knew and worked with
- Earlier in that week, the Director’s login credentials were compromised because the Director had responded to a phishing e-mail.
- The entire series of events in this whaling incident has been investigated by IT Security, Corporate Investigations, and even the CFO was later involved.

Actual funds transfer specification from the Director’s e-mail account.

Note the misspelled word: “**Rounting**”.



Account Name: Terrance M. Wolford

Bank Name: Wells Fargo

Account Number: 1113427543

Rounting: 021200025

Amount: $14,500

How and Why Did the Recent JLL Whaling Attack Work?

- **How? Five-stage attack**
  1. Identification and Reconnaissance from outside
  2. Spear Phishing to get Executive credentials, Director was tricked into providing user credentials
  3. Reconnaissance and Research from the inside about the employees the Director would normally interact with
  4. Attack execution, ordering an unsuspecting manager to electronically transfer money
  5. Successful wire transfer of $14,500 to a Wells Fargo account

- **Why?**
  - The attacker did their homework
  - Launched the attack from inside the company network using compromised user credentials
  - The manager believed the attacker was a real Director and responded to his authority
  - The manager was worried about the consequences of not following orders

How Can Your IT Security Staff Try to Protect Employees and Contractors?

- Information Security Awareness Training
- Phishing Campaigns commissioned by your IT Security and conducted by Third Party vendors to understand user behaviors and susceptibility to Phishing and the need for additional training and/or coaching

PHISHME

How to Protect Yourself and Your Organization

- Your company and other reputable organizations will never use e-mail to request that you reply with your passphrase, Social Security number, or confidential personal information.

- Be suspicious of any e-mail message that asks you to enter or verify personal information, through a website or by replying to the message itself.

- Never reply to or click the links in a message.

- When you recognize a phishing message, delete the e-mail message from your Inbox, and then empty it from the deleted items folder to avoid accidentally accessing the websites it points to.

More on Protecting Yourself and Your Organization

- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages. If the e-mail looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it's a scam.
- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it.
- **Don't let a link be in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in e-mail will show the actual URL at the bottom, but a good fake can still steer you wrong.

Source:
http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

Conclusion

- People execute Social Engineering attacks because they know they have a high probability of success.

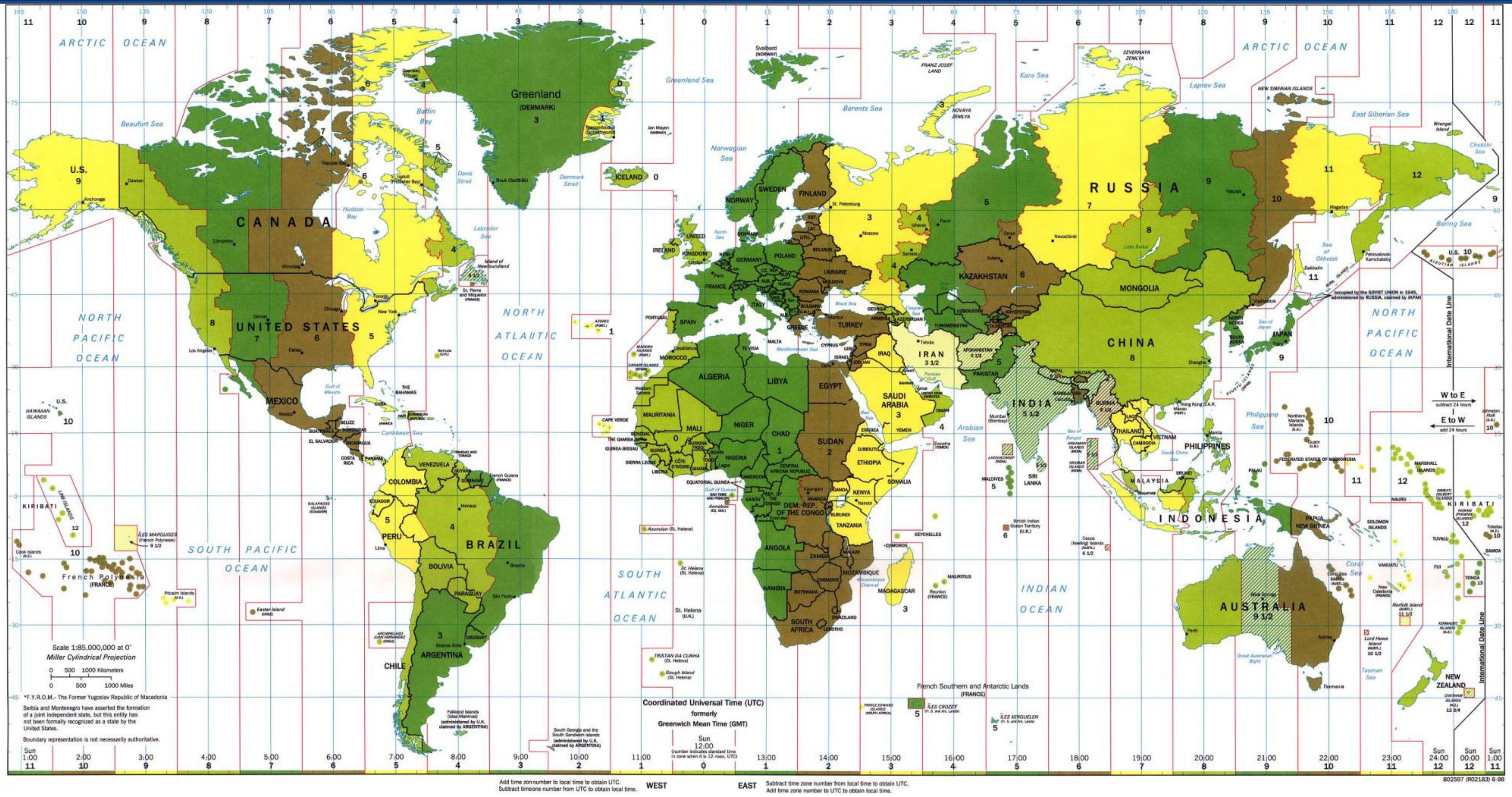
- If humans are unaware of social engineering techniques, they are vulnerable.

- Successful social engineering attacks will easily cause other security controls, such as firewalls, and access control lists (ACLs), etc., to fail.

- Social engineering attacks such as ***phishing, spear phishing and whaling*** are extremely dangerous because when they succeed, other security controls fail, they can lead to theft, espionage, and in some cases, threats and/or violence.

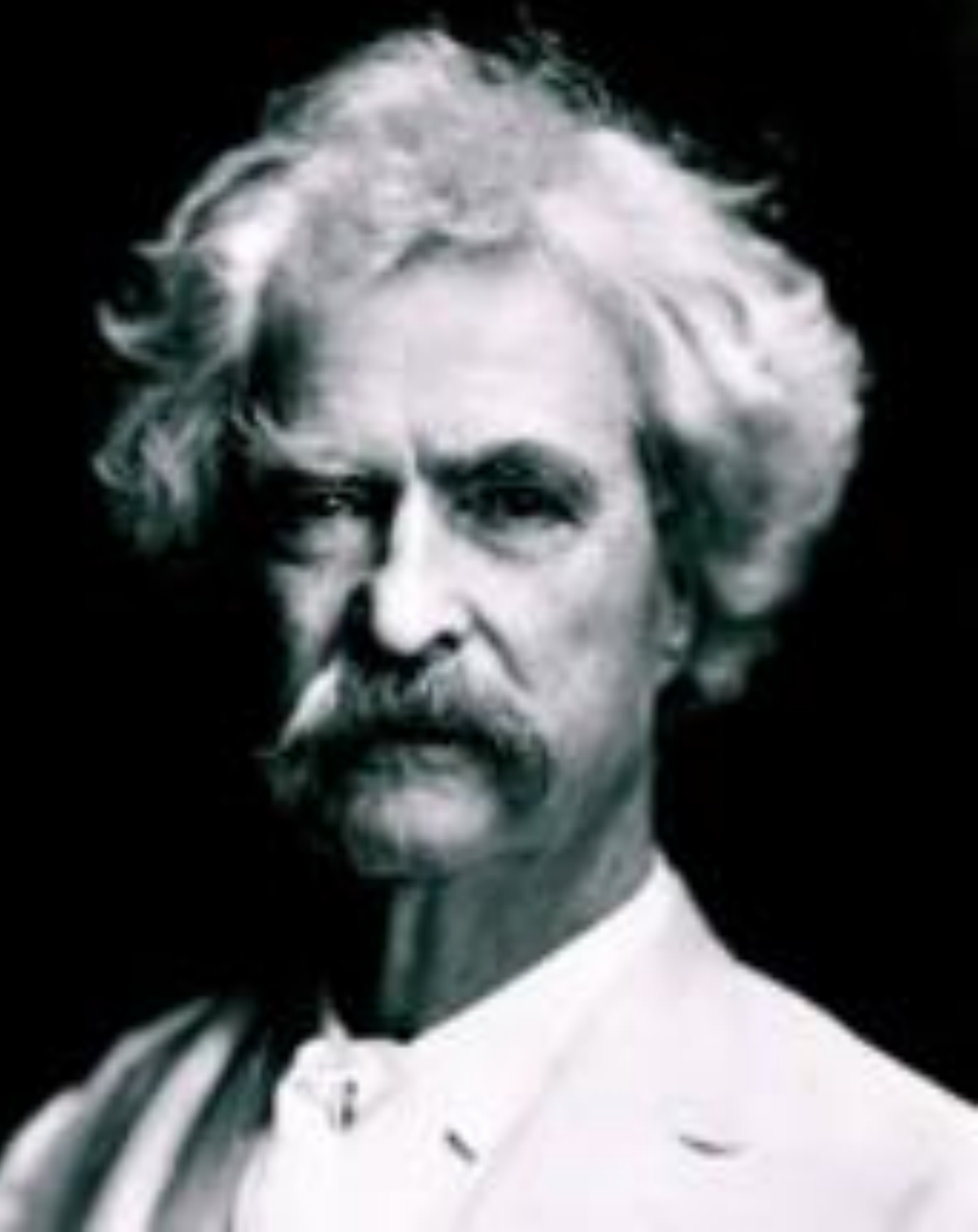
- Through education, training, application of Social Engineering Defenses, and diligence, JLL Employees and Contractors can minimize vulnerabilities to Social Engineering attacks.

Questions?


ARCTIC OCEAN
NORTH PACIFIC OCEAN
SOUTH PACIFIC OCEAN
NORTH ATLANTIC OCEAN
SOUTH ATLANTIC OCEAN
INDIAN OCEAN
Greenland (DENMARK) 3
CANADA
UNITED STATES
U.S. 9
MEXICO
BRAZIL
ARGENTINA
CHILE
PERU
COLOMBIA
VENEZUELA
BOLIVIA
ICELAND 0
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA 8
INDIA 5 1/2
IRAN 3 1/2
JAPAN 9
SAUDI ARABIA 3
ALGERIA
LIBYA
EGYPT
SUDAN 2
NIGER
CHAD
MALI
ETHIOPIA
KENYA
TANZANIA
ANGOLA
SOUTH AFRICA
MADAGASCAR
INDONESIA
PHILIPPINES
AUSTRALIA 9 1/2
NEW ZEALAND
French Polynesia (FRANCE)
KIRIBATI
International Date Line
W to E subtract 24 hours
E to W add 24 hours
Scale 1:85,000,000 at 0°
Miller Cylindrical Projection
Coordinated Universal Time (UTC) formerly Greenwich Mean Time (GMT)
Sun 12:00
WEST
EAST
Add time zone number to local time to obtain UTC. Subtract timezone number from UTC to obtain local time.
Subtract time zone number from local time to obtain UTC. Add time zone number to UTC to obtain local time.
Sun 1:00 11
2:00 10
3:00 9
4:00 8
5:00 7
6:00 6
7:00 5
8:00 4
9:00 3
10:00 2
11:00 1
12:00 0
13:00 1
14:00 2
15:00 3
16:00 4
17:00 5
18:00 6
19:00 7
20:00 8
21:00 9
22:00 10
23:00 11
Sun 24:00 12
Sun 00:00 12
Sun 1:00 11
802597 (R02183) 6-98

"It's easier to
fool people than
to convince them
that they have
been fooled."

- Mark Twain -



William F. Slater, III

- **Current Positions –**

Information Security Engineer at a Chicago-based FinTech Company, Project Manager / Sr. IT Consultant, President & CEO of Slater Technologies, Inc., and Adjunct Professor at the Illinois Institute of Technology - Working on projects related to

- Subject Matter Expert in Risk Management and Cybersecurity
- Security reviews and auditing
- Writing a Security Certification Book for a Major U.S. Publisher
- ISO 27001 Project Implementations
- Software Development
- Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
- Providing subject matter expert services to Data Center product vendors and other local businesses.
- Also Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.
- Developing and delivering Cybersecurity Classes for Triton College in River Grove, IL.

Contact Information & Other Information

http://billslater.com/career

http://billslater.com/certifications

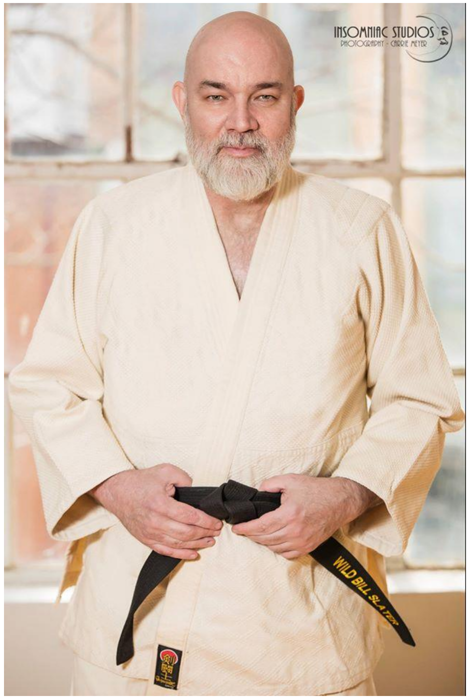
http://billslater.com/interview

http://billslater.com/writing

http://billslater.com/datacentermanager

http://billslater.com/iso27001

William Favre Slater, III
MBA, M.S., PMP, CISSP, SSCP, CISA, ISO 27002, ISO 20000, ITIL v3, IP v6
Project Manager / Program Manager
slater@billslater.com
williamslater@gmail.com
Career Page: http://billslater.com/career
LinkedIn: https://www.linkedin.com/profile/in/billslater
Twitter: @billslater
SKYPE: billslater (by pre-arrangement reservation)
773 - 235 - 3080 - Home Office
312 - 758 - 0307 - Mobile
312 - 275 - 5757 - FAX
1337 N. Ashland Ave. No. 2
Chicago, IL 60622
United States of America



William Favre Slater, III
Black belt and Certified Instructor in Kodokan Judo