Social Engineering: How do you like your Phish?

ISSA-COS Mini Seminar 14 May 2016

Agenda

Social Engineering

Phishing

State of Phish 2016

Crime Files

Prevention

Questions

Credits

Hello!

I am Debi Caldwell

I'm a Hacker – A People Hacker.

You can find me at:
Debi.Caldwell@gmail.com

Your smile will give you a positive countenance that will make people feel comfortable around you.

Les Brown

Social Engineering

Science
Art
Psychology

ISSA-COS Mini Seminar 14 May 2016

Social Engineering

Any act that influences a person to take an action that may or may not be in their best interest.

Who are the Social Engineers in your life?

To have influence, you really don't need to have power. But what you need more than anything else is to have that almost uncanny understanding of what matters to people.

Anne Sweeney

Influence

The capacity to have an effect on the character, development, or behavior or someone or something, or the effect itself.

Who influences you?

Paths of Influence:

- Authority
- Commitment and consistency
- Concession
- Obligation
- Reciprocity
- Scarcity
- Social proof


Teach a
Man to
Phish
ISSA-COS Mini Seminar 14 May 2016

Phishing

To acquire sensitive information
(passwords, usernames, credit card details)
For malicious reasons
By masquerading as a trustworthy entity
In electronic communication
(email, IM or other communication channels)

Bigger Phish

Spear-Phishing
Whaling
Pharming
Vishing
Smishing

Wombat Security Technologies
2016 State of Phish

87% were victims of phishing (up 13% from last year)

67% experienced spear phishing (up 22%)

60% increase in phishing attacks

Wombat Security Technologies
2016 State of Phish

Malware infections (42%)

Compromised accounts (22%)

Lost data (4%)

Wombat Security Technologies
2016 State of Phish

44% lost employee productivity

36% faced consequences resulting from loss of propriety information

20% dealt with damage to reputation

A few more interesting facts:

- Emails that included users' first names had a 19% higher average click rate than messages with no personalization.
- Organizations used corporate-style templates in 56% of their mock attacks. Consumer-style templates were used in 29% of simulated messages.
- Employees were most likely to click on emails that they expected to see in their business inboxes, including HR documents and shipping confirmations. They were more cautious with "consumer-oriented" emails like gift card offers and social networking notifications.

Just a couple more:

- The most popular attack template in 2015 was an electronic fax notification message. It had an average click rate of more than 15%.
- Another popular attack was an Urgent Email Password Change request, which had an average failure rate of 28%.

Be a little suspicious … Ask yourself next time you receive an e-mail claiming you have won an iPad or received a FedEx package — is this probably real? Would it happen to me walking down the street?

James Lynne

Bad Boys,
Bad Boys

ISSA-COS Mini Seminar 14 May 2016

Ryan Collins: Guilty of Hacking iCloud & Google storage

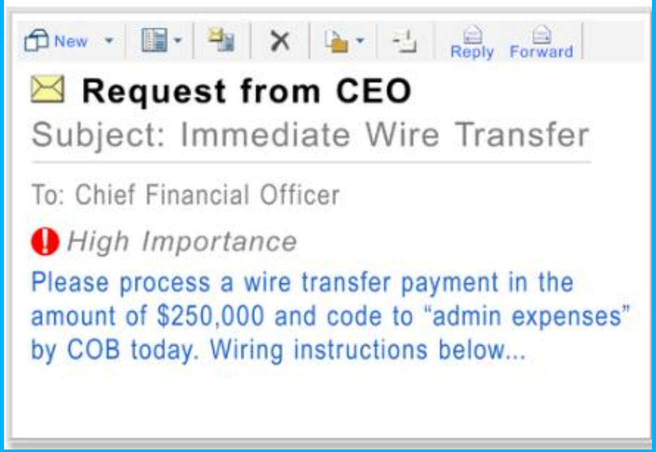

Ryan Collins, Google+

- Hacked more than 100 accounts – including celebrities from November 2012-September 2014
- Sent email pretending to be from Apple & Google
- Stole pictures, videos, even full backups
- No evidence that he leaked anything he stole
- 18-month sentence as a result of plea deal
- Expected to name other hackers

Charles Harvey Eccleston:
Plead Guilty to Attempted Spear-Phishing Attack

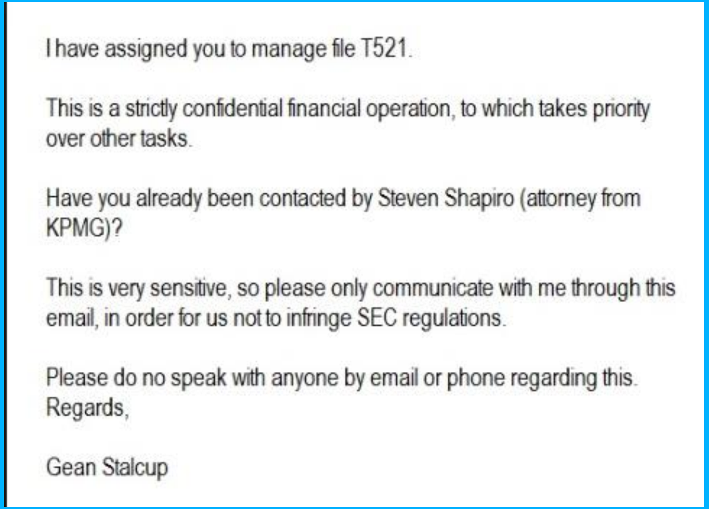
- Employed by Department of Energy & Nuclear Regulatory Commission
- Terminated from NRC when he failed to meet requirements of 2-year probation
- Attempted to launch spear-phishing campaign against 80 DoE employees
- Caught in FBI sting
- Prepared a list of email addresses and the text of the email
- Sentenced to 18 months in prison

“Business Email Compromise” costs $2.3 BLN 10/13-2/16



- 17,642 businesses in 79 countries
- 270% increase
- Spoofed email to trick employees into believing it is money transfer for CEO

http://www.reuters.com/article/cyber-fraud-email-idUSL2N17B0I2



I have assigned you to manage file T521.

This is a strictly confidential financial operation, to which takes priority over other tasks.

Have you already been contacted by Steven Shapiro (attorney from KPMG)?

This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations.

Please do no speak with anyone by email or phone regarding this.
Regards,

Gean Stalcup

- BEC is 4% of total scams (Zapfraud)
- Average loss is $130,000

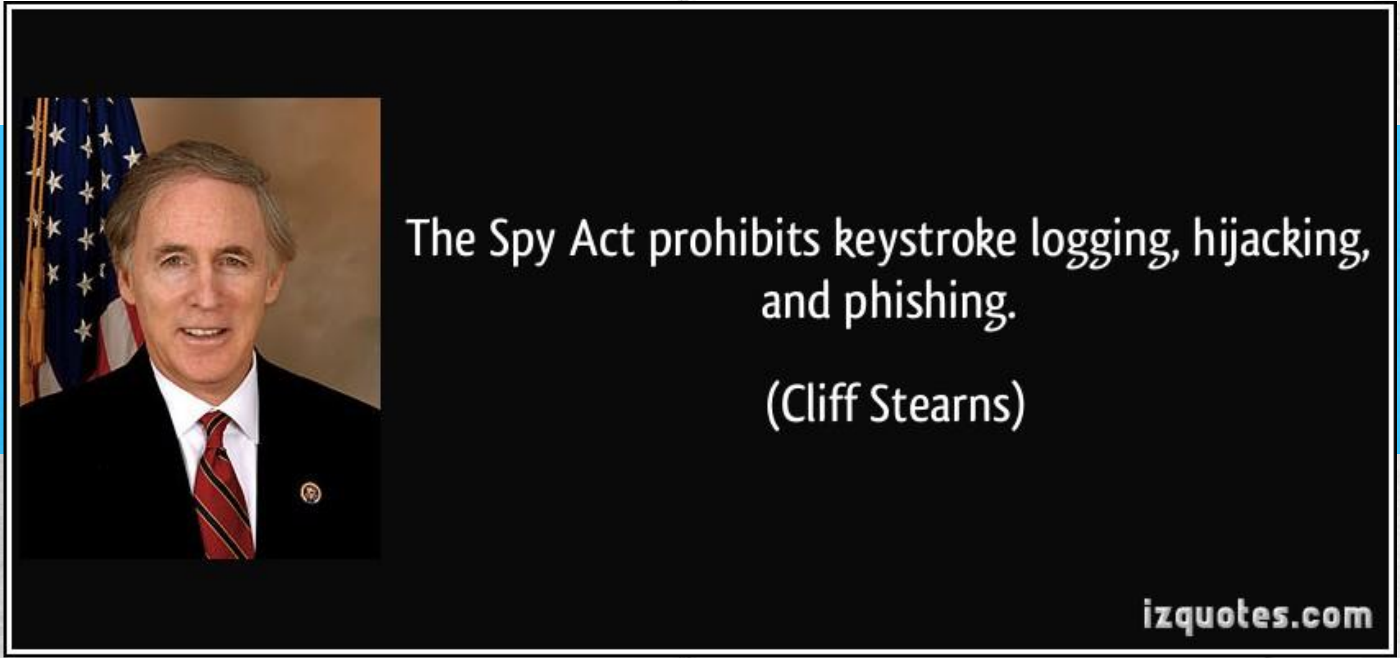
http://www.csoonline.com/article/3044070/social-engineering/business-email-compromise-fraud-rising-fast-hard-to-fight.html

Yet while millions of dollars are spent in trying to beef up IT, very few organizations realize that the best defense against corporate espionage begins with an attitudinal change among its people. Most continue to invest in expensive firewalls when they could be building efficient 'humanwalls'.

Captain Raghu Raman, Mahindra Special Services Group

Defense against the Dark Arts

ISSA-COS Mini Seminar 14 May 2016


The Spy Act prohibits keystroke logging, hijacking, and phishing.
(Cliff Stearns)
izquotes.com

Technology is not enough …

- People want to be helpful. Whether it is the bedraggled guy running late for his interview, or the woman on the phone who cant access her networked documents, people want to be helpful
- Educate employees regarding social engineering attacks and especially email fraud.
- People are the greatest weakness in the security posture.
- People are greatest strength in the security posture.

This cyberattack surely serves as a bucket of ice water to the face.
Sen. Chuck Schumer, D-N.Y., as quoted by The Hill

Thanks!

Any questions?

You can find me at:
Debi.Caldwell@gmail.com

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by [SlidesCarnival]
- Photographs by [Death to the Stock Photo] ([license])
- Wombat Security Technologies 2016 State of the Phish https://info.wombatsecurity.com/blog/wombats-2016-state-of-the-phish-report-shows-double-digit-increases-in-phishing-threats
- CICentre, SpyPedia.net at http://www.cicentre.com/default.asp?