SOCIAL ENGINEERING

DARSHAN & RAJ

AGENDA

- What is it?
- The Past
- The Present
  - How to attack?
  - How to defend?
- The Future

SOCIAL ENGINEERING

The art of manipulating people so they give up confidential information.

TYPES OF ATTACKS

Phishing
Vishing / Smishing
Content Injection
Link Manipulation
Keyloggers
Malvertising

Ransomware
Baiting
Quid Pro Quo
Piggybacking
Pretexting
Tailgating

HISTORY OF ATTACKS

Playing with someone's trust

Baiting using Trojan Horse (& USBs)

Pretexting in Catch Me If You Can

If a social engineer looks, acts and sounds the part, people will take the attacker at face value and not question the pretext any further.

LATE 20TH CENTURY

Vishing 

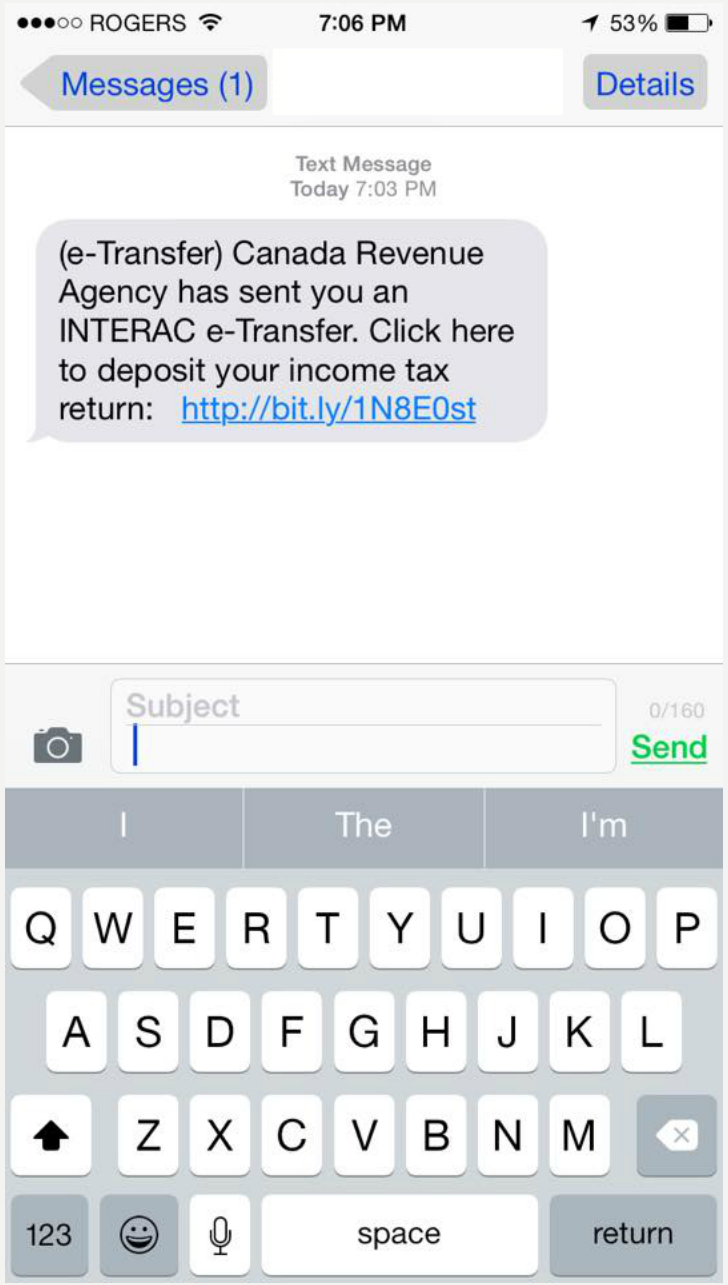
Faxing 

Emails 

1 in every 131 emails were unsolicited and contained malware attachments (2016)

Cellphones numbers targeted (Kijiji - data being sold)

Email filters by providers



PHISHING

PHISHING

- Tricking someone into sharing passwords, credit card numbers, and other sensitive information by posing as a trusted institution.

- Vishing - phishing through phone calls.
- Smishing - phishing through SMS.

HISTORY OF PHISHING

- Early 1990s, the warez community used AOL.
- Random credit card number generator.
- 1995, the warez group began imitating AOL employees.
- Finally, emails became popular:
  - yahoo-billing.com
  - ebay-fulfillment.com

CURRENT STATISTICS

- 156 million phishing emails are sent worldwide
  - 80,000 clicks — PER DAY (Government of Canada)
- The typical 10,000-employee company spends $3.7 million annually (Ponemon Institute)

HOW TO PHISH

Gather Information.

Identify method of phishing.

Look, sound, and feel like the real deal. Walk and talk the act and the victim won't second guess.

Release the hounds! … & wait.

GATHERING INFORMATION

- Telephone
- Social Network Sites
- Intrusion/Role Play
- Shoulder Surfing
- Tailgating

Free Tools and APIs:

Open Source Intelligence Framework

Industry Used Tool:

Maltego Tool

HOW TO PHISH

Gather Information.

Identify method of phishing.

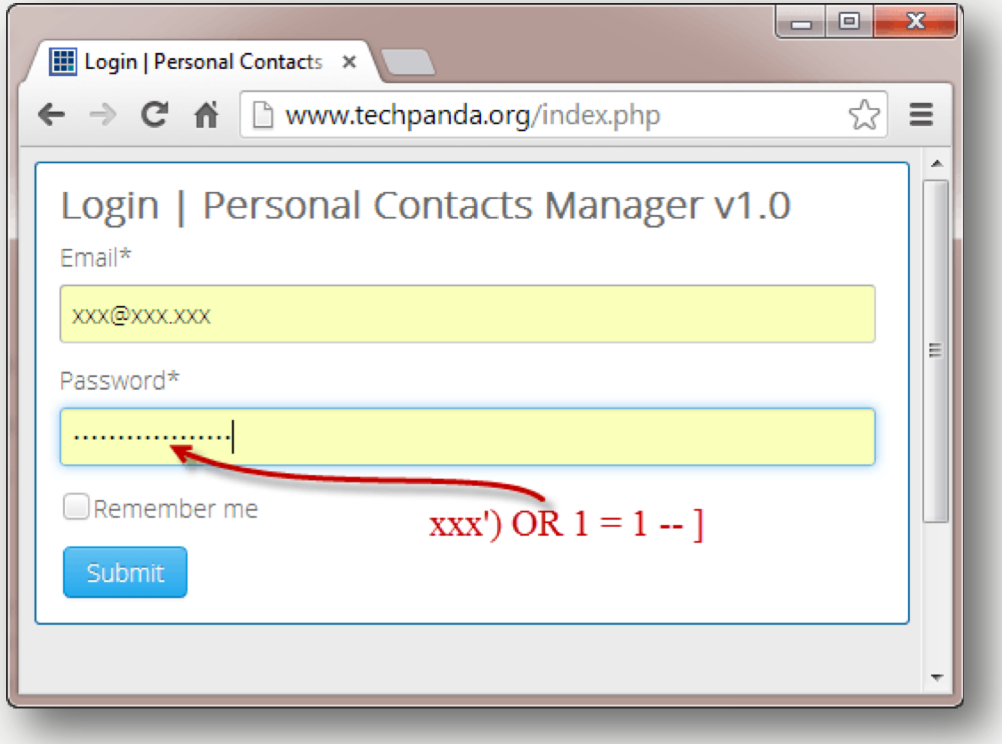
Look, sound, and feel like the real deal. Walk and talk the act and the victim won't second guess.

Release the hounds! … & wait.

OTHER SOCIAL ENGINEERING ATTACKS

CONTENT INJECTION

Vulnerability in a web application – does not properly handle user-supplied data.



RANSOMWARE

Threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

QUID PRO QUO

Promise a benefit in exchange for information. This benefit usually assumes the form of a service.

PIGGYBACKING

A person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. Also known as tailgating.

LINK MANIPULATION

LINK MANIPULATION

- ***Unsubscribe*** or ***Click to access your account*** in emails
- Editing the link www.youtube.com
- URL Shorteners
  - https://bit.ly/2T5jLGT points to our class website. Trust me!

NETFLIX

Please Update Your Payment Method

Hello,

Sorry for the interruption, but we are having trouble authorising your Credit Card. Please visit www.netflix.com/youraccountpayment to enter your payment information again or to use a different payment method. When you have finished, we will try to verify your account again. If it still does not work, you will want to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 0800 096 6380.

-The Netflix Team

Paul Moore

@Paul_Reviews

Follow

Can you spot the difference?

lloydsbank.co.uk

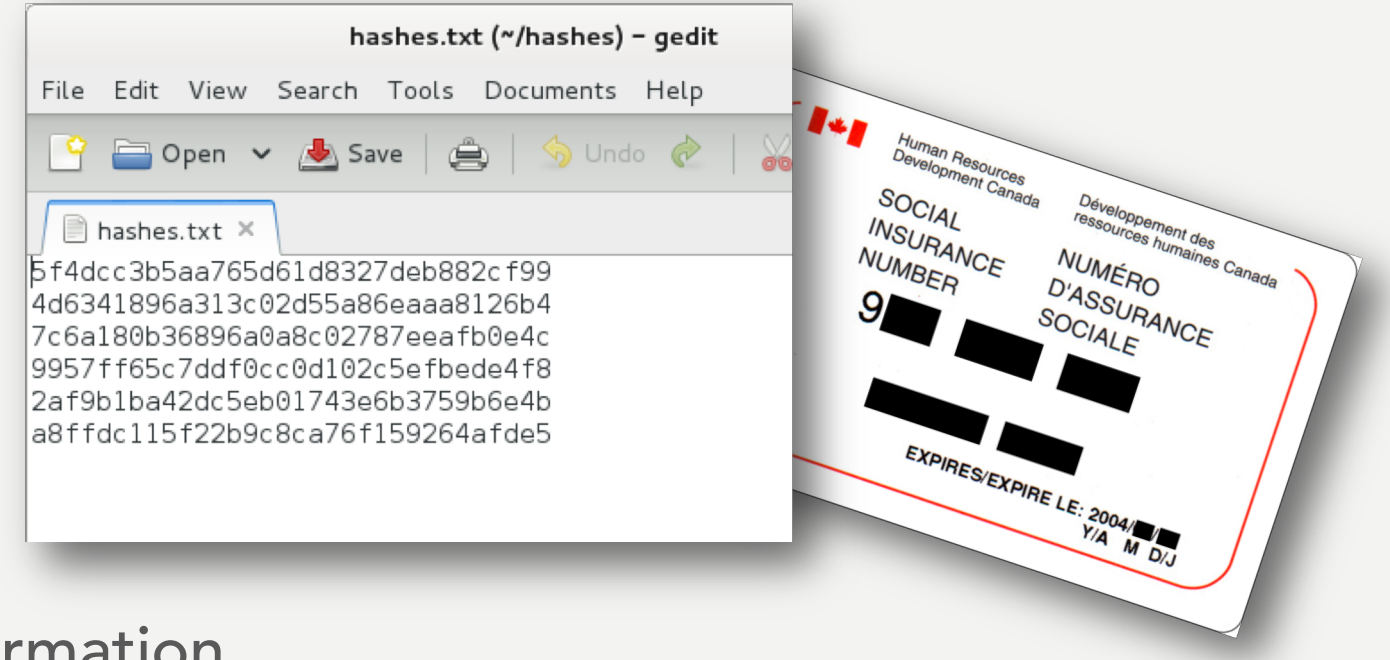
lloydsbank.co.uk

#phishing #scam #caseSensitive #security

VIDEO BREAKDOWN

- Phone number indicates he’s internal.
- Praises the other person.
- Request sounds important.
- Polite and kind, more likely to receive help.

STOLEN DATA



- Personally identifiable information.
- Financial, healthcare and education information.
- Credit and debit card information, bank account numbers, sort code numbers.
- Other ID credentials like passport numbers, driving licence details.

USES OF DATA

- Sold on black market for cash.
  - Use credentials to gain immigration status, buy and re-sell expensive equipment
  - Claim medical insurance
  - Black market has no borders — hard to trace
- Used to spear-phish
- Blackmail or expose individuals

- www.haveibeenpwned.com
- www.dehashed.com

MAJOR EVENTS

2013 YAHOO CUSTOMER ACCOUNT COMPROMISE

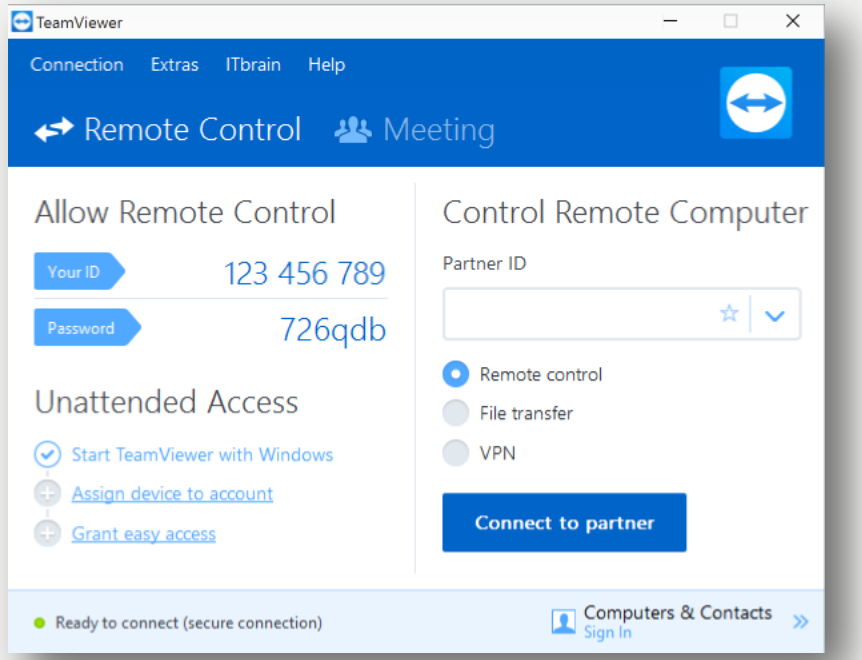
- A semi-privileged engineer at the company made the mistake of falling for a spear-phishing message.
- Hackers compromised every single customer account at the company—more than 3 billion accounts.
- The data promptly went up for sale on the dark web.

2014 SONY PICTURES HACK

- North Korean vs The Interview
- Sony released the movie for free
  - Substantial financial loss
  - Employee data leaked online

2013 DEPARTMENT OF LABOR WATERING HOLE ATTACK

- A server at the U.S. Department of Labor was hacked and used to host malware.
- It redirected certain visitors to another site installed a remote access Trojan named Poison Ivy.



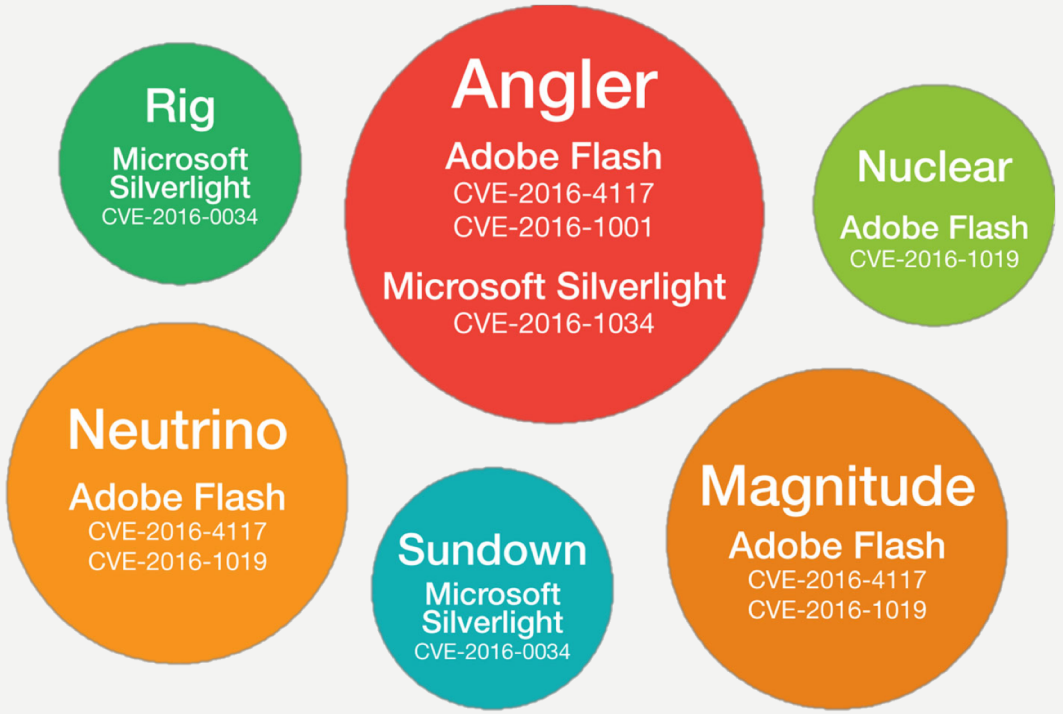
MALVERTISING

- Placement of malicious code in ads.
- Difficult to track.
- Third party ad companies manage ads.

- Ad is clicked.
- Victim is redirected to a compromised server or host.
- Exploit kit is launched and it evaluates the users system for vulnerabilities.
- Malware is installed using a security bypass in the exploit kit.

EXPLOIT KITS

- Automated threats that utilize compromised websites:
  - divert web traffic,
  - scan for vulnerable browser-based applications,
  - and run malware.
- Sold on underground criminal markets as a service.



HOW TO DEFEND?

Security Planet: No matter how much expertise and money you put into your network security and preventing data theft — firewalls, security appliances, encryption, etc. — the human element remains vulnerable to hackers who apply social engineering techniques.

TIPS FOR YOU!

- Know the accounts you own
- Limit your public profile info
- Secure security questions
- Continual education, training & reminders
- 2FA everything you can
- Setup alerts for unauthorized or unknown logins, get notifications of withdrawals, deposits, transactions
- Updates are good (most of the time)

FUTURE OF SOCIAL ENGINEERING

- More blackmail/spear-phishing attacks
- Continuous use of emails, phone calls on landlines and now cellphones
- Google things, check their ratings
  - read reviews (adblockers with malware)
- Explain IT (Social Engineering) Podcast by Softcat

SOURCES

- https://www.webroot.com/ie/en/resources/tips-articles/what-is-social-engineering
- http://www.phishing.org/phishing-techniques
- https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks#
- https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/#gref
- https://osintframework.com
- Link Manipulation and Vishing - https://www.youtube.com/watch?v=PWVN3Rq4gzw
- Defcon Vishing - https://www.youtube.com/watch?v=F78UdORll-Q
- https://www.bullguard.com/blog/2018/02/what-happens-to-stolen-data
- https://www.social-engineer.org/framework/
- http://datasploit.info

THE END

QUIZ TIME!

View slides at: https://cs.utm.utoronto.ca/~pandyara/