Social Engineering

by Patrick Robertshaw and
Michael Yousef

What is social engineering?

- Psychological manipulation of people to divulge sensitive information
- Doesn’t rely on software vulnerabilities
- Defense is heavily dependant on users

Why Social Engineer?

- It is often easier to trick someone into giving you their information than hacking them
- Systems can be secure, but the users may not be
- Cheap and easy
- It is not inherently illegal

Types of Social Engineering

- Pretexting
- Phishing
- Baiting
- Quid Pro Quo
- Tailgating
- Shoulder Surfing

Pretexting

- Targeted attack
- Requires some knowledge about the victim to lure them into a false sense of security
- Attacker may investigate further to maintain false security

Phishing

- Attacker sends a fraudulent email that appears to be legitimate
- Attacker hopes the victim provides them with more information
- Directed phishing attacks are known as spear phishing and rely on pretexting

Nice to Know You

Naomi Surugaba [azlin@moa.gov.my]

Actions

Inbox

Monday, March 10, 2014 1:18 PM

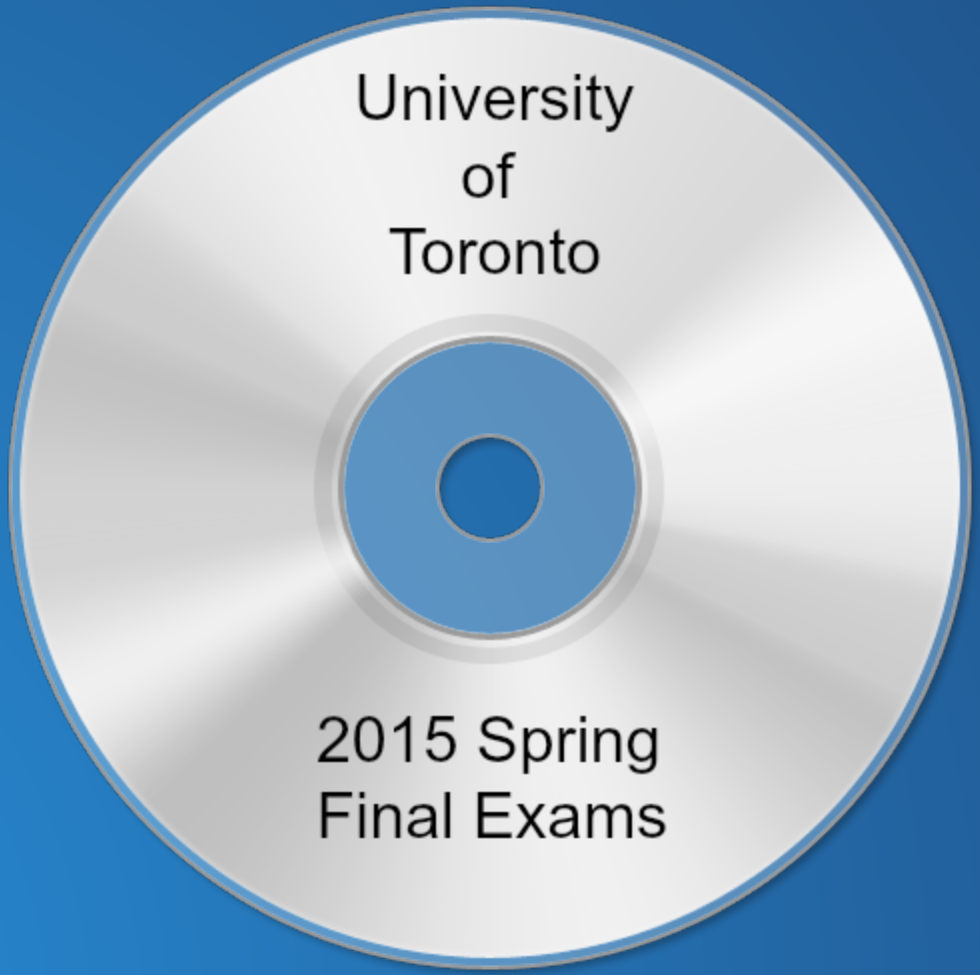
Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Emails from Friends

- A friend that is compromised might send you fraudulent emails
- You would trust this email because it came from a friend
- It might contain a link or download that would compromise your system

Baiting

- Uses physical media to scam the victim
- Attacker places a CD in a place they know the victim will see
- CD would be labeled in a way that the victim would be curious to look
- CD could contain malicious code when run


University
of
Toronto
2015 Spring
Final Exams

Quid Pro Quo

- Means “something for something”
- This attack attempts to offer the victim something in an attempt to gain confidential information

Quid Pro Quo Example

Attacker calls pretending to be IT support
“Hi, this is Bob from IT, I’m calling in regards to your support ticket”
“Finally, someone’s calling.”
“If I could just get your username and password, I can log into the system and see what the problem is”

Tailgating

- Getting access to restricted areas
- Simply walk behind someone, who would hold the door open for you
- Have you ever held the door open for someone at an apartment?

Shoulder Surfing

- Observing the victim’s private information over their shoulder
- Common in public places such as airports and coffee shops

Social Engineering and the Law

- Social engineering is by and large legal
- Using data from social engineering in malicious ways is illegal
- Pretexting for phone numbers or bank accounts is illegal

Rogers Communication Social Engineering Hack

- Attacker called support and got an employee's ID and answers to their security questions
- Reached company's internal network
- Ransomed Rogers for 70 bitcoins
- Dumped private data online

Twitter Hijacking of @N

- @N a sought after Twitter handle
- Attacker called PayPal and claimed to be an employee, and got the last 4 digits of @N's credit card
- Attacker used this to gain access to a GoDaddy account, and threatened to delete data or give up @N

Chase Bank Bad Advice

- Sent emails to customers to tell them how to avoid being hacked
- Emails told customers to call the number on their credit card or click a link for more details
- Normal advice to prevent social engineering says not to click links

Social Engineering leads to Social Engineering

- Social engineering preys on pretexting
- Gaining knowledge of users from one attack may lead to future attacks, and better attacks
- eBay was hit in 2014 and attackers got access to sensitive information including physical addresses and birthdays

How to Prevent Social Engineering

- Educate yourself on social engineering
- Do not give out sensitive information
- Do not click on links to secure sites from emails - go there directly instead
- Be wary of unsolicited messages
- Ensure websites are who they claim to be
- Discard sensitive information properly
- Test employees

What If I Am A Victim?

- Report it to the company or website
- Change any passwords that may be compromised
- Contact your bank
- Watch for signs of other identity theft
- Report it to the police


JIMMY
Kimmel
LIVE!