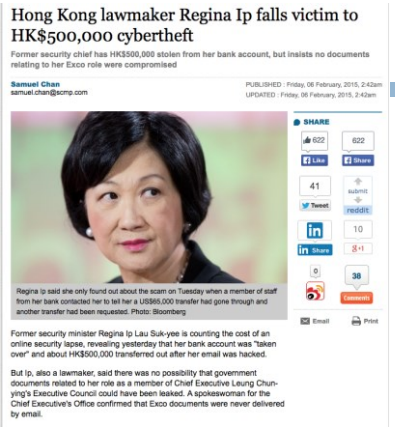
LECTURE 15:SOCIAL ENGINEERING AND HUMAN HACKING



Hong Kong lawmaker Regina Ip falls victim to HK$500,000 cybertheft

Former security chief has HK$500,000 stolen from her bank account, but insists no documents relating to her Exco role were compromised

Samuel Chan
samuel.chan@scmp.com

PUBLISHED : Friday, 06 February, 2015, 2:42am
UPDATED : Friday, 06 February, 2015, 2:42am

Regina Ip said she only found out about the scam on Tuesday when a member of staff from her bank contacted her to tell her a US$65,000 transfer had gone through and another transfer had been requested. Photo: Bloomberg

Former security minister Regina Ip Lau Suk-yee is counting the cost of an online security lapse, revealing yesterday that her bank account was "taken over" and about HK$500,000 transferred out after her email was hacked.

But Ip, also a lawmaker, said there was no possibility that government documents related to her role as a member of Chief Executive Leung Chun-ying's Executive Council could have been leaked. A spokeswoman for the Chief Executive's Office confirmed that Exco documents were never delivered by email.

Introduction

- If you know the enemy and know yourself you need not fear the results of a hundred battles.
  - Sun Tzu

  知己知彼百戰百勝
  - 孫子

- What is Social Engineering?
  - Manipulate people into doing something, rather than by breaking in using technical means
- Types of Social Engineering
  - Quid Pro Quo
  - Phishing
  - Baiting
  - Pretexting
  - Diversion Theft
- Ways to prevent Social Engineering

What is Social Engineering?

- Attacker uses **human interaction** to obtain or compromise information
- Attacker my appear **unassuming or respectable**
  - **Pretend** to be a new employee, repair man, ect
  - May even **offer credentials**
- By asking questions, the attacker may **piece enough information together** to infiltrate a companies network
  - May attempt to get information from many sources

Kevin Mitnick

Famous Social Engineer Hacker
- Went to prison for hacking
- Became ethical hacker

"People are generally helpful, especially to someone who is nice, knowledgeable or insistent."

Kevin Mitnick - *Art of Deception*:

- "*People inherently want to be helpful and therefore are easily duped*"
- "*They assume a level of trust in order to avoid conflict*"
- "*It's all about gaining access to information that people think is innocuous when it isn't*"
- Hear a nice voice on the phone, we tend to be helpful
- Social engineering cannot be blocked by technology alone

Examples of Social Engineering

- **Kevin Mitnick talks his way into central Telco office**
  - Tells guard he will get a new badge
  - Pretend to work there, give manager name from another branch
  - Fakes a phone conversation when caught
- **Free food at McDonalds**

Live Example

- Convinced friends that you would help fix their computers
- People inherently want to trust and will believe someone when they want to be helpful
- Fixed minor problems on the computer and secretly installed remote control software
- Now you have total access to their computer through ultravnc viewer

Types of Social Engineering

- **Quid Pro Quo**
  - Something for something
- **Phishing**
  - Fraudulently obtaining private information
- **Baiting**
  - Real world trojan horse
- **Pretexting**
  - Invented Scenario
- **Diversion Theft**
  - A con

Quid Pro Quo

- **Something for Something**
  - **Call random numbers** at a company, claiming to be from technical support.
  - Eventually, you will reach someone with a **legitimate problem**
  - Grateful you called them back, they will **follow your instructions**
  - The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to **install malware**

Phishing

- **Fraudulently obtaining private information**
  - **Send an email** that looks like it came from a legitimate business
  - **Request verification** of information and warn of some consequence if not provided
  - Usually contains link to a **fraudulent web page** that looks legitimate
  - User gives information to the social engineer
    - **Ex**: Ebay Scam

Phishing continued

- Spear Fishing
  - **Specific phishing**
    - **Ex**: email that makes claims using your name
- Vishing
  - **Phone phishing**
  - Rogue interactive voice system
    - **Ex**:call bank to verify information

Baiting

- **Real world Trojan horse**
  - **Uses physical media**
  - Relies on **greed/curiosity of victim**
  - Attacker leaves a **malware infected cd or usb drive** in a location sure to be found
  - Attacker puts a **legitimate or curious lable** to gain interest
  - **Ex**: "Company Earnings 2009" left at company elevator
    - **Curious employee/Good samaritan uses**
    - User inserts media and **unknowingly installs malware**

Pretexting

- **Invented Scenario**
  - **Prior Research/Setup** used to establish legitimacy
    - **Give** information that a user would normally not divulge
  - This technique is **used to impersonate**
    - **Authority** ect
      - Using **prepared answers** to victims questions
      - **Other gathered information**
  - **Ex**: Law Enforcement
    - **Threat of alleged infraction** to detain suspect and hold for questioning

Diversion Theft

- Persuade deliver person that **delivery is requested elsewhere** - "*Round the Corner*"
- When deliver is redirected, attacker persuades delivery driver to **unload delivery near address**
- **Ex**: Attacker parks **security van outside a bank**. **Victims going to deposit money** into a night safe are told that the **night safe is out of order**. **Victims then give money to attacker** to put in the fake security van
- Most companies do not prepare employees for this type of attack

Weakest Link?

- No matter how strong your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software
- You are the weakest link in computer security!
  - People are more vulnerable than computers
- "*The weakest link in the security chain is the human element*" -Kevin Mitnick

Ways to Prevent Social Engineering

Training

- User Awareness
  - User knows that **giving out certain information is bad**
- **Military** requires Cyber Transportation to hold
  - **Top Secret Security Clearance**
  - **Security Plus Certification**
- **Policies**
  - Employees are **not allowed to divulge private information**
  - **Prevents employees from being socially pressured or tricked**

Ways to Prevent Social Engineering Cont..

- 3rd Party test - **Ethical Hacker**
  - Have a third party come to your company and attempted to **hack into your network**
  - 3rd party will attempt to **glean information from employees using social engineering**
  - Helps **detect problems people have with security**
- **Be suspicious** of unsolicited phone calls, visits, or email messages from individuals asking about internal information
- **Do not provide personal information**, information about the company(such as internal network) unless authority of person is verified

General Saftey

- Before transmitting personal information over the Internet, check the **connection is secure** and check the **url is correct**
- If unsure if an email message is legitimate, **contact the person or company by another means** to verify
- Be **paranoid and aware** when interacting with anything that needs protected
  - The smallest information could compromise what you're protecting

Further Reading

- Art of Deception
  - Kevin Mitnick
- Social Engineering: The Art of Human Hacking
  - Christopher Hadnagy