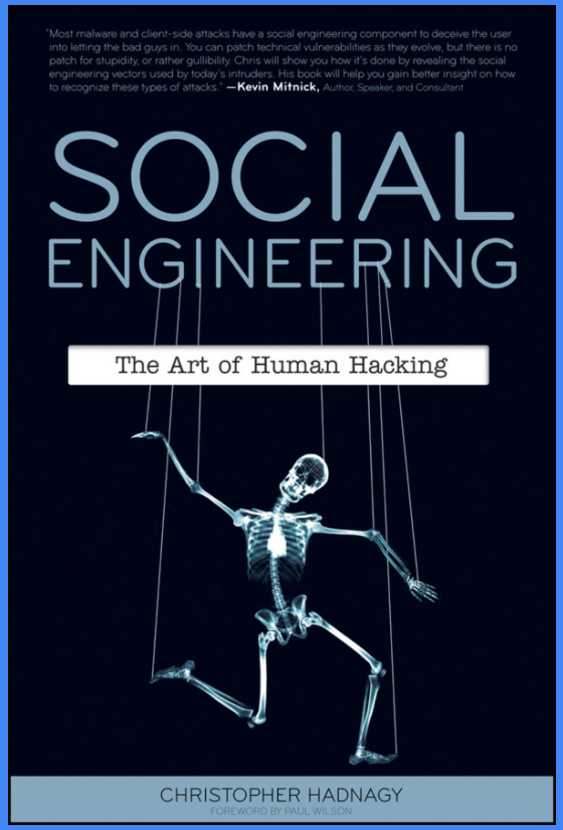
Social Engineering

UDLS
September 11, 2015
Neil Newman



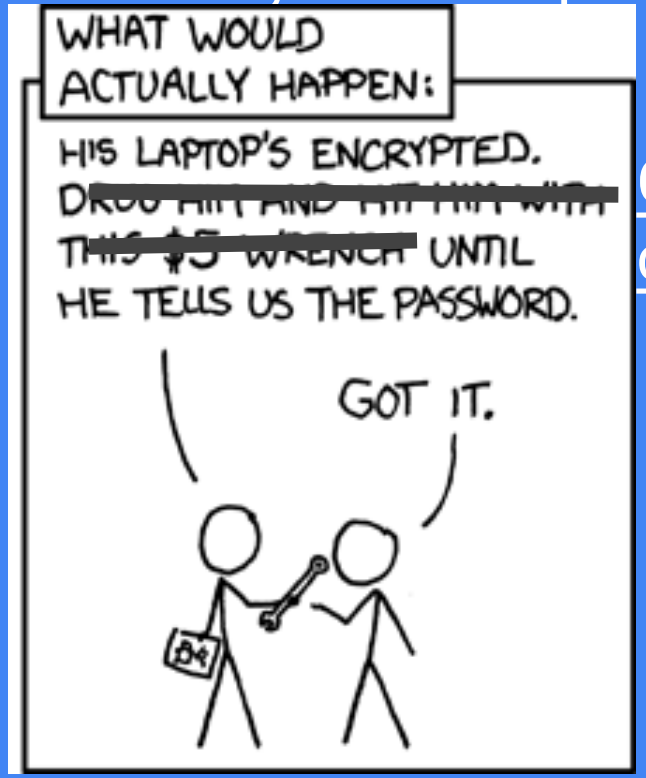
"Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures."

- SearchSecurity

Why Social Engineering?

It can be hard to break cryptographic algorithms...

...but it is often easy to break people



Offer chocolate

Confidence man

“Have you confidence in me to trust me with your watch until tomorrow?”

Why Social Engineering Works

You are NOT unique or special. You are like one of huge groups of people who all act the same way and fall for the same things. You are screwed.

- You: For Sale: Protecting Your Personal Data and Privacy Online

Methods

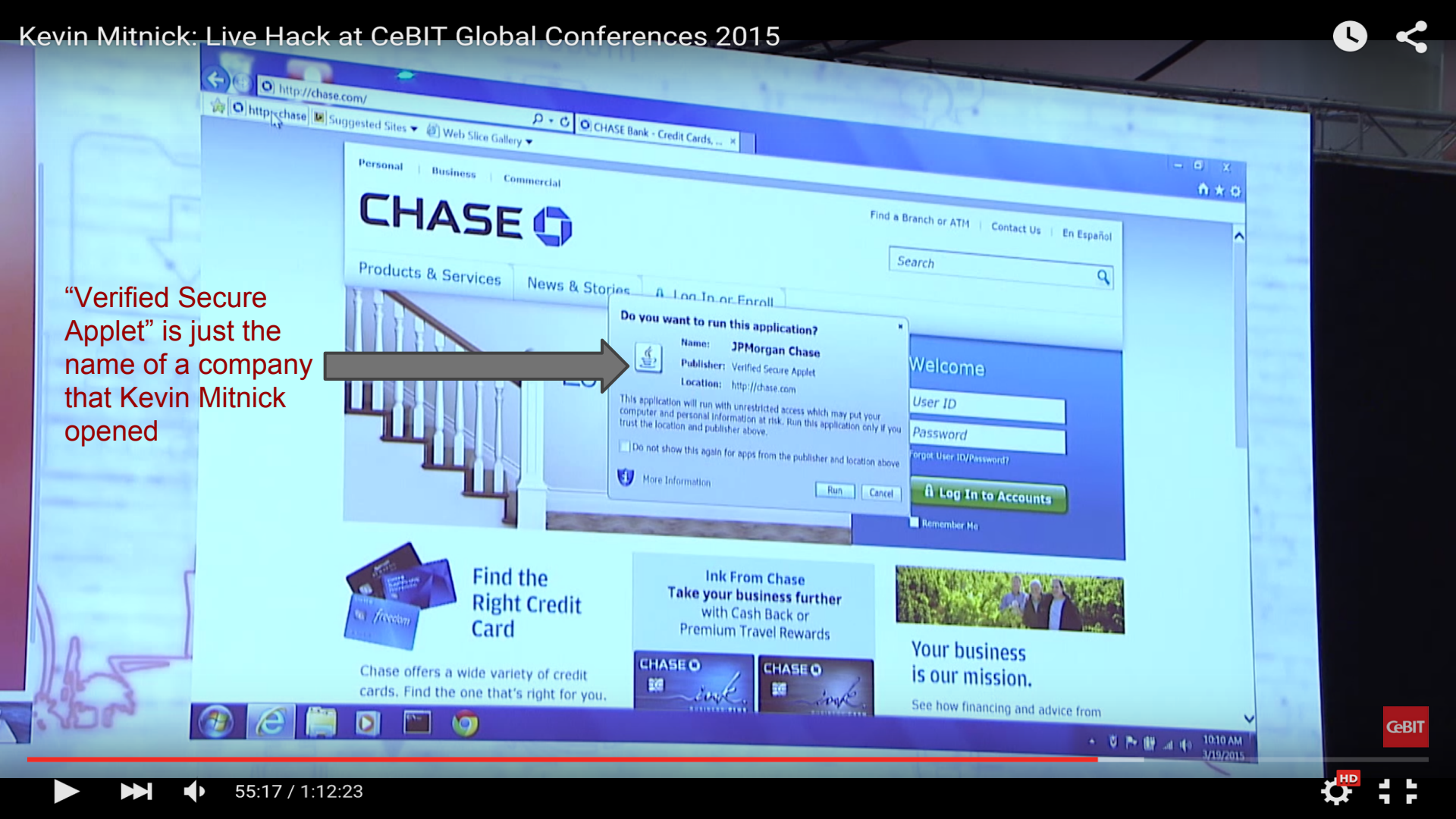
Pretexting

- Creating a scenario to engage the victim in which they are more likely to divulge information
- It helps to have information you shouldn't have without the authority you are claiming (can come from research, dumpster diving, social networks, etc.)
- Unshredder
- Examples: posing as janitors, exterminators, TV technicians to gain entry and go unnoticed

Phishing

- Attempt to gain sensitive information by masquerading as a trustworthy entity electronically
- Send an e-mail that seems to come from a legitimate source requesting sensitive information and with negative consequences if it is not provided (e.g. your account will be deleted if you do not confirm your PIN)
- It's pretty easy to mimick the look of HTML
- IVR phising - mimick a phone system (can collect PINs, transfer to a "customer service" agent)

Kevin Mitnick: Live Hack at CeBIT Global Conferences 2015



55:17 / 1:12:23

Baiting

- Trojan horse - rely on curiosity and greed to get someone to execute your malware on a trusted machine
- Leave a malware infected media device (e.g. USB drive) in a location where it will be found (e.g. bathroom, an elevator, parking lot), and give it an irresistible label (e.g. Executive Salary Summary Q2 2012)

Quid pro quo

- Request information for compensation
- If you call random phone numbers at a company and claim to be tech support, eventually you will find someone who was waiting for tech support to call back and will be grateful for your call. You then help them, and then also have them install malware.

Tailgating

- To get into an unrestricted area, simply walk behind someone with access
- People might even hold the door open for you
- Think about flashing your U-Pass (back in the day) - sometimes IDs are not checked thoroughly
- If you are distracted / angry, you are less likely to be stopped. For example, pretend you are yelling at your wife on your cell phone. No one wants to deal with an angry person if they can help it.

Examples

Tourist Scams

CASHIER ON THE PHONE

A cashier in a shop will pretend to be on the phone while serving you. What she's actually doing though, is taking a photo of your credit card so it can be replicated later.

THE FAKE TAKEAWAY MENU

Scam artists will slide fake takeaway menus under your hotel door, in the hope that you order from them on an evening where you don't feel like going out. You won't receive any food though, just a frightening bank statement after they have used your card details to make their own copy.

THE FLIRT

An attractive woman will approach a lone male traveller, and start to flirt with him. She will ask him if he would like to go to a bar or nightclub with her, and the bill will be extortionate at the end of the night!

DEFCON Social Capture the Flag

- Contestants are given three weeks to research their targets and gather any information they can get online passively (without hacking) e.g. using Google, Facebook, WhoIs
- Contestants have 30 minutes to perform phone calls to get sensitive corporate details like what email software they use and the name of the outside contractor that cleans their office

Example

Detailed multi-stage example scenario

Thank you for listening