IN5290 Ethical Hacking
Lecture 10: Social Engineering

Universitetet i Oslo

Laszlo Erdödi

Lecture Overview

- What is social engineering and how it works
- What are the techniques that are used
- Analysis of specific computer based social engineering attacks

What is Social Engineering?

Social Engineering is the manipulation of people to perform actions that lead to compromisation such as revealing confidential information.

- information gathering
- fraud
- system access
- physical access

Basis of Social Engineering

- Human nature of trust

People are usually positive to each other. If there’s no negative indication (suspicious signs, bad previous experience) people prefer to suppose the best.

  – Can you open that door for me? I left my card at home.
  – Please log in here using the link below.

- Trust based on the information provided

Trust can be achieved by the information that is provided. If the attacker mentions «accidently» something that refers to something that is only known by privileged persons it can trigger the trust.

  – Hi Jane, this is John from the admin. Your boss George (known from website) asked me to update your profile while you’re on holiday (known from facebook). It’s kinda urgent, because …Ignorance

Basis of Social Engineering

- Moral obligation

To serve moral obligations can overwrite security policies. Personal interest (not to be rude to someone) can be more important than the company's interest even if it's mixed with the nature of trust.

  - Open the door for someone carrying heavy boxes

- Something promising

By providing something promising can turn people to be less cautious.

  - Win a new Iphone X, just click the link below
  - Cheaper prices in a web shop

- Confusement

Providing misleading infomation. People feel stupid and think it's their fault. They try to solve the situation to be in balance again that makes them less cautious

Basis of Social Engineering

- Hurry

Hurry makes people disposed to overlook details or make them less cautious.

- Ignorance

Ignorant users easily overlook details or don't care about security at all

- Fear

Fear has also negative effective on the security. It hardens to make reliable decisions that helps attackers

- Combinations of the previous ones

Example: Trust based on the provided info + hurry + fear

The CIO (name from info gathering) is furious about the …..(private story revealed from info gathering) you should immediately provide your credentials to check if it was you or not. If we can't check it the CIO will …

Social Engineering techniques

Impersonate someone

- Posing as a legitimate user
- Posing as priviliged user
- Posing as technical support
- Posing as Repeairman, Cleaning service, Pizza delivery, etc.

- Eavesdropping

Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent.

- Shoulder surfing

It is used to obtain personal information (e.g. passwords) and other confidential data by looking over the victim's shoulder. This attack can be performed either at close range (by directly looking over the victim's shoulder) or from a longer range, for example by using telescope.

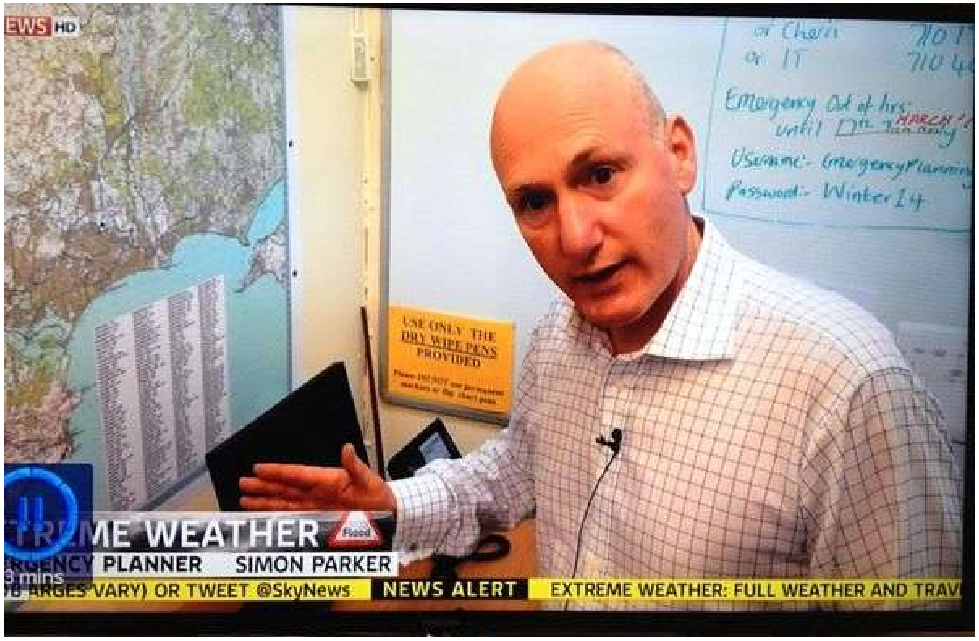
Social Engineering techniques

- Dumpster diving

Looking for teasures in someone’s trash ☺ (calendar entries, passwords in post-it, phone numbers, emails, operation manuals)

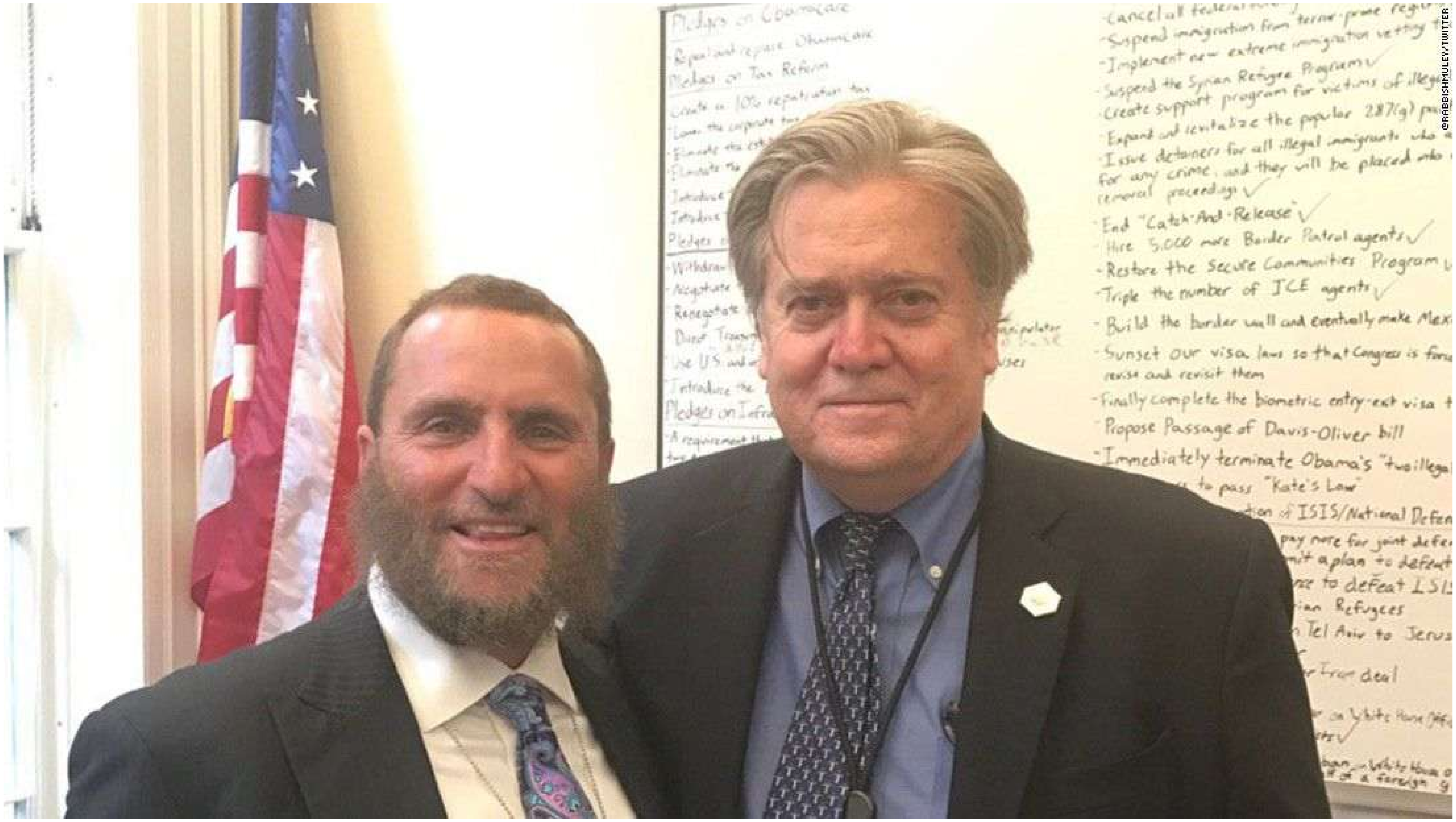
- Piggybacking/Tailgating

A person goes through a checkpoint (physical access) with another person who is authorized.


EWS HD
or Chem
or IT
710
710 4
Emergency Out of hrs:
until 1st MARCH January
Username:- EmergencyPlanning
Password:- Winter14
USE ONLY THE DRY WIPE PENS PROVIDED
ME WEATHER
RGENCY PLANNER SIMON PARKER
3 mins
ARGES VARY) OR TWEET @SkyNews
NEWS ALERT
EXTREME WEATHER: FULL WEATHER AND TRAV

Social Engineering techniques

Picture from the White House in the Social Media


Pledges on Obamacare
Repeal and replace Obamacare
Pledges on Tax Reform
Create a 10% repatriation tax
-Suspend immigration from terror-prone regi
-Implement new extreme immigration vetting
-Suspend the Syrian Refugee Program ✓
Create support program for victims of illeg
-Expand and revitalize the popular 287(g) pa
-Issue detainers for all illegal immigrants who
for any crime, and they will be placed into
removal proceedings ✓
-End "Catch-And-Release" ✓
-Hire 5,000 more Border Patrol agents ✓
-Restore the Secure Communities Program
-Triple the number of ICE agents ✓
-Build the border wall and eventually make Mex
-Sunset our visa laws so that Congress is forc
revise and revisit them
-Finally complete the biometric entry-exit visa
-Propose Passage of Davis-Oliver bill
-Immediately terminate Obama's "two illegal
to pass "Kate's Law"
of ISIS/National Defen
pay more for joint defe
a plan to defeat
to defeat ISIS
Refugees
Tel Aviv to Jeru
deal

@RABBISHMULEY/TWITTER

Computer based Social Engineering techniques

Computer based

- Phising
- Spear phising
- Fake software
  - Tool that has hidden function
  - Modified legitimate tool
  - Fake AV

Phising attacks

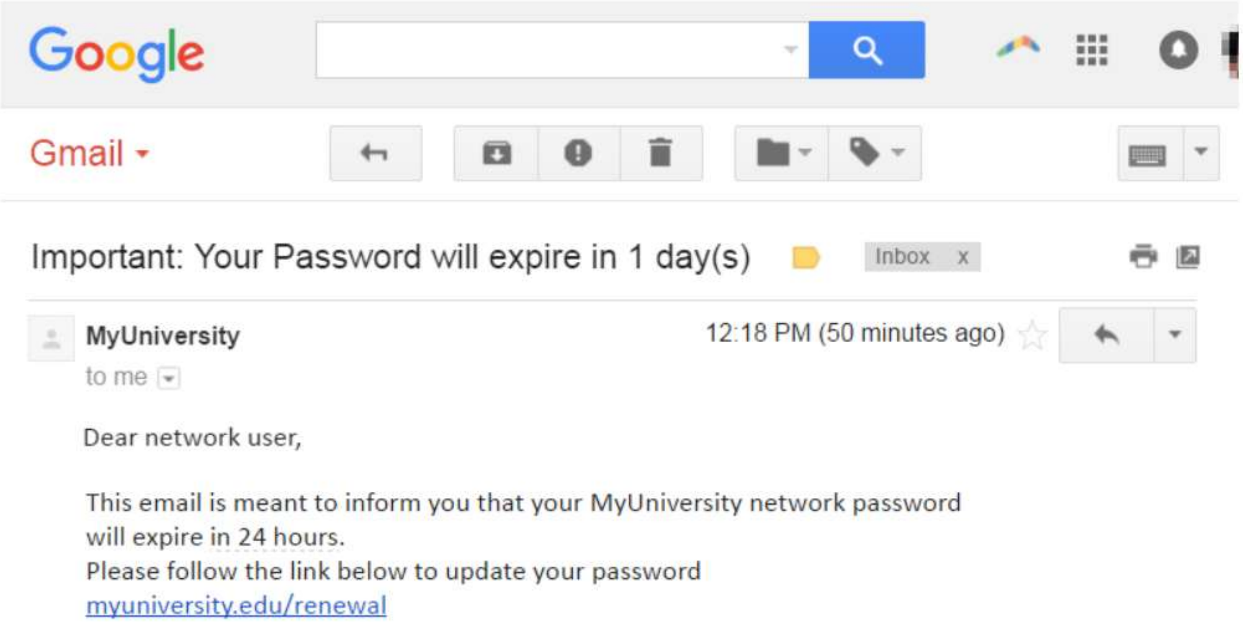
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

https://www.incapsula.com/web-application-security/phishing-attack-scam.html

Phising attack examples



Important: Your Password will expire in 1 day(s)

MyUniversity
to me

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

The link redirects to myuniversity.edurenewal.com which is an attacker controlled fake renewal page, but it looks like the same as the original.

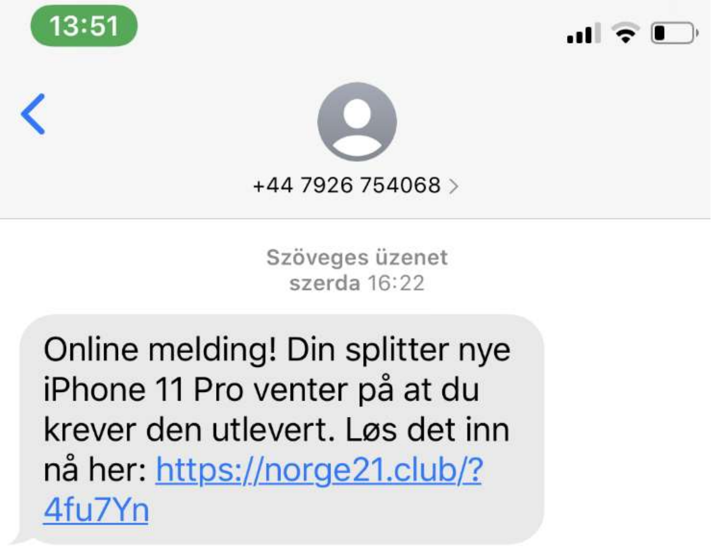
If the renewal page has XSS vulnerability then the attacker can redirect the victim to the real renewal page, but steal the session variables with XSS script.

https://www.incapsula.com/web-application-security/phishing-attack-scam.html

Spare phising attack examples

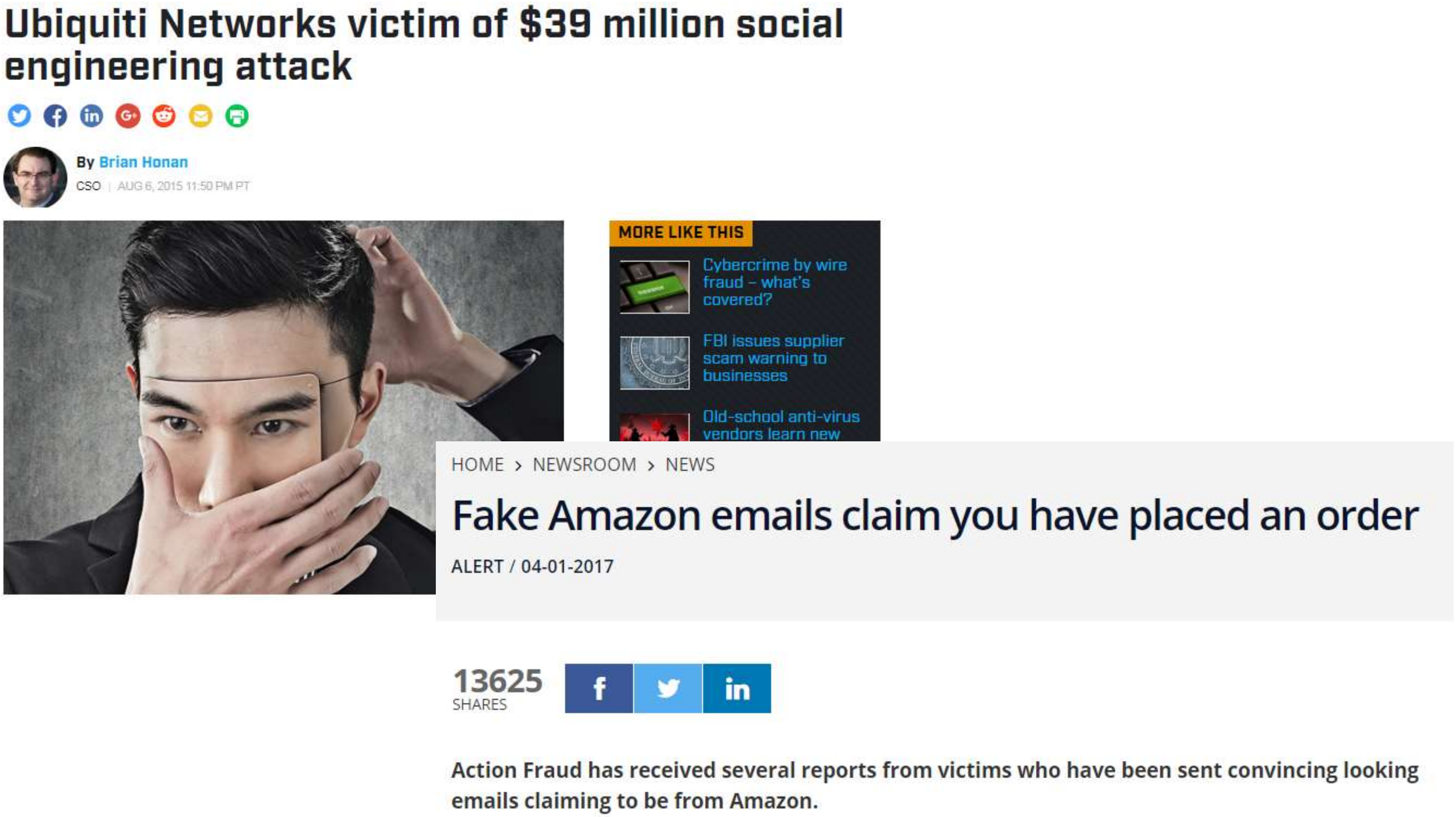
Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in depth version of phishing that requires special knowledge about an organization, including its power structure.

The attacker can use personal information obtained from information gathering (e.g. social media) to customize the story.



Online melding! Din splitter nye iPhone 11 Pro venter på at du krever den utlevert. Løs det inn nå her: https://norge21.club/?4fu7Yn

Spare phising attack examples



Ubiquiti Networks victim of $39 million social engineering attack

By Brian Honan

CSO | AUG 6, 2015 11:50 PM PT

MORE LIKE THIS

- Cybercrime by wire fraud – what's covered?
- FBI issues supplier scam warning to businesses
- Old-school anti-virus vendors learn new

HOME › NEWSROOM › NEWS

Fake Amazon emails claim you have placed an order

ALERT / 04-01-2017

13625 SHARES

Action Fraud has received several reports from victims who have been sent convincing looking emails claiming to be from Amazon.

End of lecture