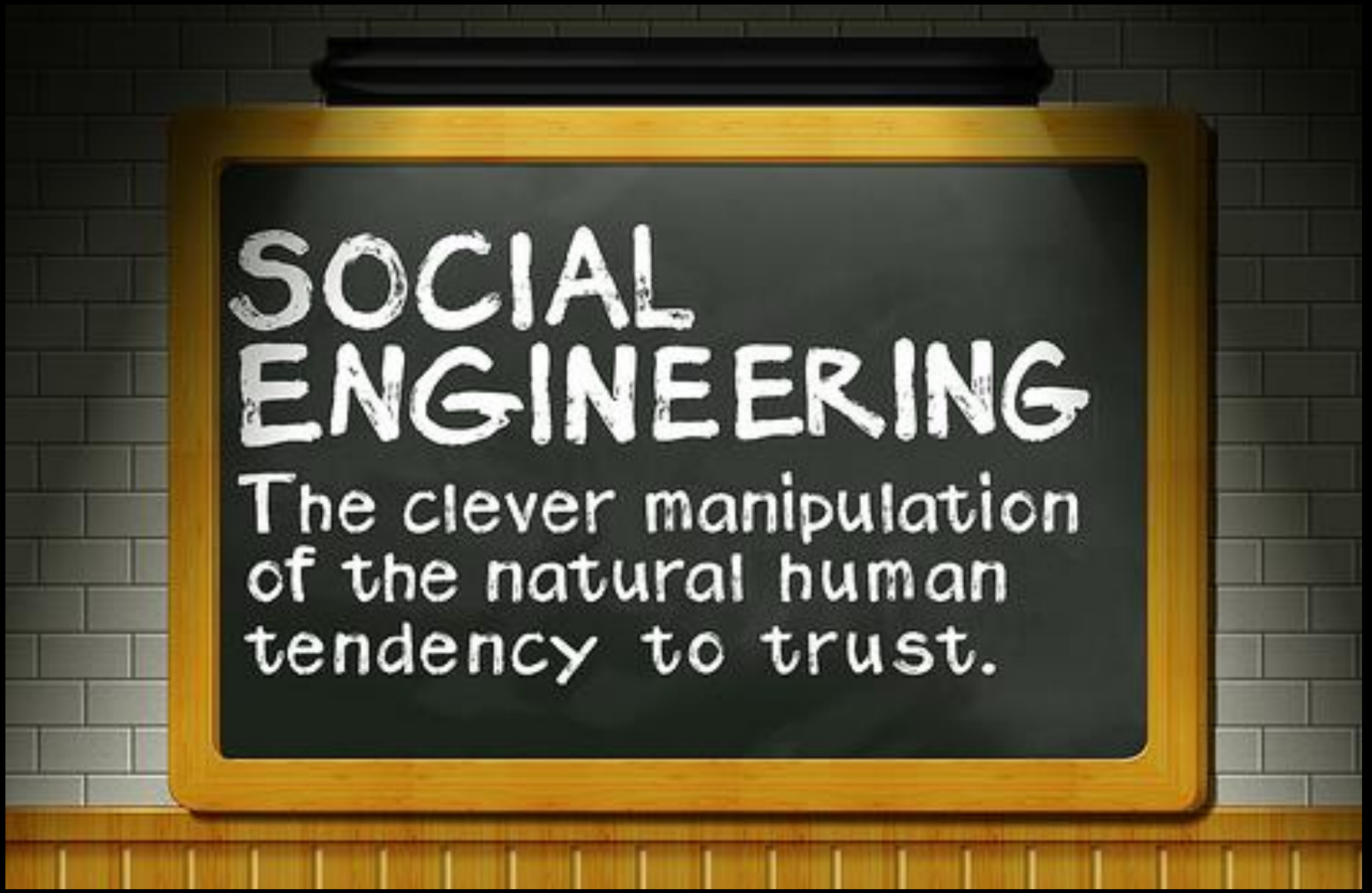
Info Security Technology

Topic 2
Client Security
(Social Engineering)


SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.

Statistics

- 60% of enterprises were victims of social engineering attacks in 2016
- Read more
- Read more

Social Engineering Attacks

- Directly gathering information from individuals
- Relies on trusting nature of individuals
- Psychological approaches to persuade the victim to provide information or take action.
  - Flattery or flirtation
  - Conformity
  - Friendliness

Social Engineering

- One attacker called human resources office
  - Asked for and got names of key employees
- Small group of attackers approached door to building
  - Pretended to have lost key code; let in by friendly employee
- Group had learned CFO was out of town
  - Because of his voicemail greeting message
- Group entered CFO's office
  - Gathered information from unprotected computer
  - Dug through trash to retrieve useful documents
- One member called help desk from CFO's office
  - Pretended to be CFO; asked for password urgently
  - Help desk gave password
- Group left building with complete network access

Social Engineering by Phone

- 'I m calling from xyz credit card company… May I speak to Mr. abc…..' 'Have you been using your credit card in Malaysia for the last six hours?'
- 'No'
- 'Well, we have a card charged that's actually active just now, it's on your credit card and it's to Malaysia and as a matter of fact, you've got about $2,000 worth of charges from somebody using your card. You're responsible for the $2,000, you have to pay that... but we suspected that it is a credit card fraud '
- 'I did not use the card, can you help me to undo the changes'
- '**O.K. first I must verify your card details, start with your full name… card no.? credit limit ? PIN no ? payment method ? mother's name ? Company ? E-mail address ? Mobile tel ?** …..

31 Oct 2017 09:46PM
(Updated: 31 Oct 2017 09:50PM)

33,008 shares

Bookmark

Singapore

IKEA Singapore warns of scam messages offering free vouchers

SINGAPORE: IKEA Singapore is warning customers of messages circulating online and through messaging apps purportedly offering free vouchers from the Swedish furniture giant.

http://www.channelnewsasia.com/news/singapore/ikea-singapore-warns-of-scam-messages-offering-free-vouchers-9362542

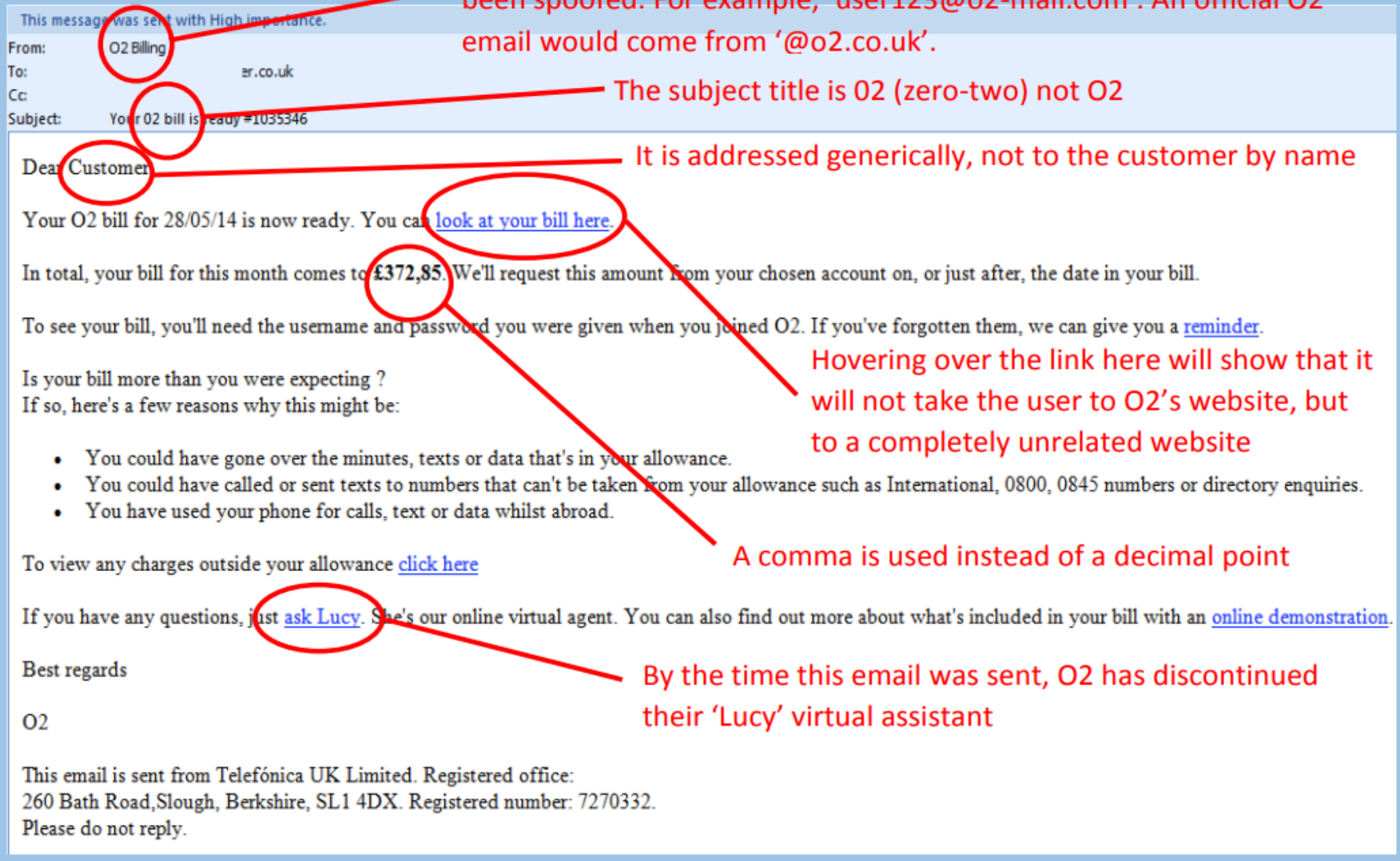
A screenshot of a scam message making its rounds on the Internet and through messaging apps.

Ikea – how to spot a phishing scam

http://www.ikea.com/gb/en/customer-service/how-to-spot-a-phishing-scam/

Social Engineering by Email

Example 1 – A phishing email[iii]



This message was sent with High importance.

From: O2 Billing

To: er.co.uk

Cc:

Subject: Your 02 bill is ready #1055346

Dear Customer

Your O2 bill for 28/05/14 is now ready. You can look at your bill here.

In total, your bill for this month comes to **£372,85**. We'll request this amount from your chosen account on, or just after, the date in your bill.

To see your bill, you'll need the username and password you were given when you joined O2. If you've forgotten them, we can give you a reminder.

Is your bill more than you were expecting ?
If so, here's a few reasons why this might be:

- You could have gone over the minutes, texts or data that's in your allowance.
- You could have called or sent texts to numbers that can't be taken from your allowance such as International, 0800, 0845 numbers or directory enquiries.
- You have used your phone for calls, text or data whilst abroad.

To view any charges outside your allowance click here

If you have any questions, just ask Lucy. She's our online virtual agent. You can also find out more about what's included in your bill with an online demonstration.

Best regards

O2

This email is sent from Telefónica UK Limited. Registered office:
260 Bath Road,Slough, Berkshire, SL1 4DX. Registered number: 7270332.
Please do not reply.

Although it appears to be from O2, closer inspection, by right clicking or hovering over the name, shows the email address has been spoofed. For example, 'user123@o2-mail.com'. An official O2 email would come from '@o2.co.uk'.

The subject title is 02 (zero-two) not O2

It is addressed generically, not to the customer by name

Hovering over the link here will show that it will not take the user to O2's website, but to a completely unrelated website

A comma is used instead of a decimal point

By the time this email was sent, O2 has discontinued their 'Lucy' virtual assistant

Psychological Approaches

Many social engineering attacks rely on psychology, which is the mental and emotional approach rather than the physical. At its core, social engineering relies on an attacker's clever manipulation of human nature in order to persuade the victim to provide information or take actions.

Principle	Description	Example
Authority	Directed by someone impersonating authority figure or falsely citing their authority	"I'm the CEO calling."
Intimidation	To frighten and coerce by threat	"If you don't reset my password, I will call your supervisor."
Consensus/social proof	Influenced by what others do	"I called last week and your colleague reset my password."
Scarcity	Something is in short supply	"I can't waste time here."
Urgency	Immediate action is needed	"My meeting with the board starts in 5 minutes."
Familiarity/liking	Victim is well-known and well-received	"I remember reading a good evaluation on you."
Trust	Confidence	"You know who I am."

Social engineering psychological approaches

- … fften involve impersonation, phishing, spam, hoaxes, typo squatting, and watering hole attacks.

Impersonation

- … to masquerade as a real or fictitious character and then play out the role of that person on a victim.
- For example, an attacker could impersonate a help desk support technician who calls the victim, pretends that there is a problem with the network, and asks her for her user name and password to reset the account.
- Common roles that are often impersonated include a repairperson, IT support, a manager, a trusted third party, or a fellow employee.
- Often attackers will impersonate individuals whose roles are authoritative because victims generally resist saying "no" to anyone in power.

Phishing

- … most common forms of social engineering.
- **Phishing** is sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information.
- Users are asked to respond to an email or are directed to a website where they are requested to update personal information, such as passwords, credit card numbers etc.

Social Engineering by Phishing

- Variations of phishing
  - Pharming
    - Automatically redirects user to fraudulent Web site
  - Spear phishing
    - Email messages target specific users
  - Whaling
    - Going after the "big fish"; targeting wealthy individuals
  - Vishing (phishing by phone)
    - Victim calls attacker's number and enters private information

Hoaxes

- Attackers can use hoaxes as a first step in an attack.
- A **hoax** is a false warning, often contained in an email message claiming to come from the IT department.
- E.g report a "deadly virus" circulating through the Internet and that the recipient should erase specific files or change security configurations, and then forward the message to other users.
- Performing the above will allow an attacker to compromise the system.

Typo Squatting

- What happens when a user makes a typing error when entering a uniform resource locator (URL) address in a web browser, such as typing *goggle.com* (a misspelling) or *google.net* (incorrect domain) instead of the correct *google.com*?
- Most often today the user will be directed to a fake look-alike site. These fake sites exist because attackers purchase the domain names of sites that are spelled similarly to actual sites.
- This is called **typo squatting** or **URL hijacking**.
- A well-known site like *google.com* may have to deal with more than 1000 typo squatting domains. Over 62 percent of the active domain names based on common misspellings of *facebook.com* are typo squatting sites.

Watering Hole Attack

- In many regions similar types of animals are known to congregate around a pool of water for refreshment.
- In a similar manner a watering hole attack is directed toward a smaller group of specific individuals, such as the major executives working for a manufacturing company.
- These executives all tend to visit a common website.
- An attacker who wants to target this group of executives will attempt to determine the common website that they frequent and then infect it with malware that will make its way onto the group's computers.

Class Assignment

- Form into your groups of 2 students
- Using the knowledge of "social engineering attack', describe 2 such attack scenarios.
- Provide ways to mitigate (prevent) such attack from happening.
- Submit to "week 3 submission"

30 mins