# TSIT01 Datasäkerhetsmetoder

Föreläsning 10: Social engineering
Lite återkoppling på utkasten

Ingemar Ragnemalm

01001001 01000011 01000111

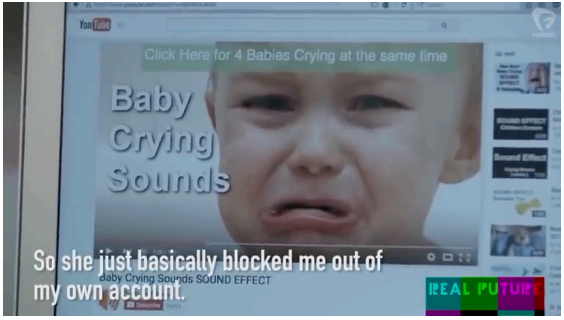
## Social engineering

Socialt samspel handlar om känslor, sedvänjor, kultur och tradition

Man kan utnyttja detta genom så kallad *Social Engineering*

Människan bakom maskinen attackeras

https://www.youtube.com/watch?v=lc7scxvKQOo



## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

Avsändaren låter pålitlig, känd

2. Moraliskt ansvar

3. Skuld

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

Offret känner att det är "rätt" åtgärd
Handlingen kanske fixar ett påhittat problem

3. Skuld

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

Offret övertygas om att det gjort något fel
och handlingen rättar till felet

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

*Man vill vara hjälpsam*

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Personliga mål:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Personliga mål:

1. Otydligt ansvar

"Detta är redan godkänt av någon annan, släpp in mig"

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

Offret tror sig få en fördel av hanteringen
"Du har vunnit 1000 kronor"

3. Rädsla

4. Annan emotionell manipulation

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

"Någon drar pengar från ditt konto"

4. Annan emotionell manipulation

## Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

"Jag tycker du är jättefin. Kom och bli medlem i klubben och chatta med mig"

## Vilka sociala “svagheter” utnyttjar Filer mot Kam?

Hjälpsamhet (och viss pliktkänsla?)

Upplevda fördelar

Maskerad till äldre man = ser ofarlig ut


01001001 01000011 01000111

## Social engineering: Sikta mot toppen!

Jan-Åke (ISYs prefekt) var på konferens

Då kom E-post till vår administratör

```
Från: Jan-Åke Larsson [mailto:jan-ake.larsson@liu.se]
Ämne: SV: omedelbar betalning(13:12:16)

Hej,

Kan du göra en banköverföring till Storbritannien idag?

Best Regards...
Jan-Åke Larsson
```

Brevet innehöll LiUs logga och bild på Jan-Åke

Adminstratören gör forward till fakturahanterare och till Jan-Åke

## Whaling

Meddelandet var "whaling" eller "CEO fraud"

Kallas ibland "spear phishing"

Riktas mot högsta ledningen (i detta fallet ISYs prefekt) men målet är ekonomiavdelningen

Dessa attacker har enligt FBI orsakat mer än 2.3 miljarder dollar i förluster sedan 2013

## Detta slutade väl

Det fanns en "reply-to" till en falsk adress men administratören gjorde ett "forward"

Upptäcktes därför inom 20 minuter och Jan-Åke kontaktade adminstratören och ekonomen samt även LiUs Incident Response Team.

Bra rutiner hade antagligen stoppat betalningen i alla fall.

## Phishing

En form av social engineering där personliga meddelanden används för att få fram personlig information som kan användas för intrång.

Kan vara E-post, genom meddelandesystem men även på socala media.

## Phishing-attacken via LiU IT

Meddelande som sade sig ha svar på supportfråga, med länk. Målet var våra lösenord. Angreppstyp: Tillit.

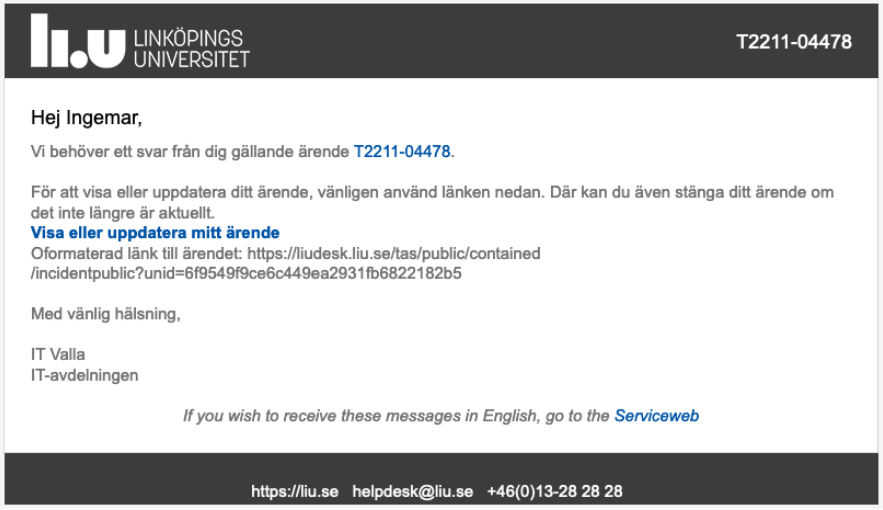
Meddelandet var exakt LiU ITs normala meddelanden! Ingen information om vad saken gäller, bara en länk, logga in här!

Den falska länken var lätt att se genom att hovra över den, MEN de som läser på mobilen ser inte detta. Många blev lurade och fick sina lösenord läckta!

Även idag har LiU IT samma system men med en ärenderad. Bra nog?

# Phishing-attacken via LiU IT

Så här ser ett vanligt meddelande ut:



LINKÖPINGS UNIVERSITET

T2211-04478

Hej Ingemar,

Vi behöver ett svar från dig gällande ärende T2211-04478.

För att visa eller uppdatera ditt ärende, vänligen använd länken nedan. Där kan du även stänga ditt ärende om det inte längre är aktuellt.
**Visa eller uppdatera mitt ärende**
Oformaterad länk till ärendet: https://liudesk.liu.se/tas/public/contained
/incidentpublic?unid=6f9549f9ce6c449ea2931fb6822182b5

Med vänlig hälsning,

IT Valla
IT-avdelningen

*If you wish to receive these messages in English, go to the Serviceweb*

https://liu.se helpdesk@liu.se +46(0)13-28 28 28

Ospecifikt! Klicka på länken... Bluffvänligt system!

01001001 01000011 01000111

## Rektors julgåva

Detta kom lagom före jul härom året:

# JULHÄLSNING FRÅN REKTOR

**BÄSTA LIU-MEDARBETARE!**

Året som snart lider mot sitt slut har minst sagt varit ett annorlunda år och inneburit en stor uppoffring för oss alla. Jag vill framföra ett stort tack från universitetsledningen för ditt tålamod och engagemang. För att visa vår uppskattning till alla medarbetare kommer här en julgåva. Förhoppningsvis är vi snart ute ur pandemin och kan ta nya tag för att driva vårt universitet framåt.

Låt oss nu ta en välbehövlig ledighet och önska varandra en God Jul och ett Gott Nytt År!

Med vänlig hälsning,

*Jan-Ingvar Jönsson*
*Rektor*

01001001 01000011 01000111

# Phishing-larmet slog till direkt hos oss!

Vackra ord

Lovar ekonomisk fördel

Extern, okänd länk

Vi klickade INTE på den!

**BÄSTA LIU-MEDARBETARE!**

Året som snart lider mot sitt slut har minst sagt varit ett annorlunda år och inneburit en stor uppoffring för oss alla. Jag vill framföra ett stort tack från universitetsledningen för ditt tålamod och engagemang. För att visa vår uppskattning till alla medarbetare kommer här en julgåva. Förhoppningsvis är vi snart ute ur pandemin och kan ta nya tag för att driva vårt universitet framåt.

Låt oss nu ta en välbehövlig ledighet och önska varandra en God Jul och ett Gott Nytt År!

Med vänlig hälsning,

*Jan-Ingvar Jönsson*
*Rektor*

*Hämta din julgåva värd 1000 kr*

- Gå till webbsidan www.gogift.com
- Klicka på "Lös in Superpresentkortet" och använd den här koden: POR-DBYY93Y7
- Välj de gåvor du önskar, och ange mottagare
- Gåvorna skickas via leverantören Gogift

01001001 01000011 01000111

## Falskt alarm!

...förrän vi fick veta att det var äkta...

Falskt alarm... vilket tyvärr också gör skada genom förlorad tid och blir man inte avtrubbad av att det "ropas varg" för ofta?

*Har du hört den förut?*

## Fiske efter säkerhetsfrågor

En form av phishing på sociala media.

INGEN bryr sig om vad din hund hette - utom informationsfiskaren!

Ändå får varje sådan postning *tusentals* svar - på grund av kärleken till hunden och att man spontant vill svara på en personlig fråga.


01001001 01000011 01000111

## Telefonbedrägerier

*Har du hört den förut?*

Rädsla kombinerat med tillit.

Telefonsamtal, det är från banken. "Det pågår en attack mot ditt konto!" Men det är bedragaren som ringer!

Spelar på din panikkänsla.

En annan form:

"Vi are kallink from Vindoze! Dere is a problem vid your komputter."

Typiskt kommer de att vilja att du installerar skadlig programvara eller liknande. Även detta bygger på att skrämma dig.

## Falska fakturor

*Se goddag gamle vän, tack för sist!*

Mest en fråga om tillit samt dåliga rutiner.

Antingen är fakturan påhittad, men ser äkta ut, eller så är det ett erbjudande som maskeras som faktura.

Går igenom om fakturor hanteras utan verifiering.

## Nigeriabrev

En klassiker. Baseras på personliga fördelar eventuellt kombinerat med moralskt ansvar. Effektivt när det når chefsnivå.

## Motåtgärder: Policy/Rutiner

LiU: Fakturor skall attesteras av två olika personer

Företagsexempel: Låna aldrig ut ditt lösenord

Fungerande infrastuktur behövs

## Motåtgärder: Medvetenhet

Man måste veta om att social engineering förekommer

Man bör känna till hur vanliga attacker fungerar

Alla i organisationen måste känna till det

**Lär dig och andra känna igen social engineering.**

## Motåtgärder: Teknologi

E-post-signaturer

Autentisering

## Social engineering

Går alltid ut på att få ett offer (inte alltid den som skadas) att göra något olämpligt.

Detta kan öppna för intrång eller direkt skapa en betalning.

Kräver, tyvärr, att vi är misstänksamma, känner igen bluffar och har rutiner för att täppa till våra egna svagheter.

Tyvärr behövs alla de där dubbelkollarna och verifieringarna.