Kan vi känna oss säkra på nätet?

SPF Maria Högalid den 7 mars 2022

Bakgrund

- 20 år inom polisen
- IT-forensiker
- Dataintrångsutredare
- Nationell samordnare mot immaterialrättsliga brott
- Rådgivare mot digitala brott hos SSF (nuvarande)

Förklaringar

Bedrägeri:

En person lurar en annan, för att sedan tjäna pengar på den man lurar.

Phishing (Nätfiske):

Bedrägeri genom att skicka mail, eller använda falska hemsidor.

Vishing (Röstfiske):

Bedrägeri genom att via telefonsamtal lura någon.

Smishing (Smsfiske):

Bedrägeri genom att via sms lura någon.

Social manipulation:

När man manipulerar någon för att göra något.

SSF

Olika bedrägerier på nätet

Romansbedrägeri – Kärlek över sociala nätverk

Investeringsbedrägeri – Bli rik fort med Bitcoin

Befogenhetsbedrägeri – Förtroende som brottsmetod

Annonsbedrägeri – För bra erbjudande

Fakturabedrägeri – Betalat en okänd faktura

Kortbedrägeri (med eller utan kort) – Är kontot tomt

Identitetsbedrägeri – Är det jag som köpt denna vara

SSF

Phishing

- Falska hemsidor, mail med länkar till skadlig kod.
- Lurar av folk på personliga uppgifter, ex. kontokortsinformation.

SSF råd

- Klicka aldrig på okända länkar.
- Lämna aldrig ut privat information.
- Logga aldrig in på BankID på uppmaning från någon okänd.
- Gör en polisanmälan.

SSF

Exempel phishing

Vishing

- Uppringd av personer som inger förtoende, ex. från bank, 1177.
- Lurar av folk på personliga uppgifter, ex. kontokortsinformation.

SSF råd

- Ring själv upp och kontrollera.
- Lämna aldrig ut privat information.
- Logga aldrig in på BankID på uppmaning från någon okänd.
- Gör en polisanmälan.

SSF

Exempel vishing

Carin, 100, utsattes för bedrägeri: ”Skurkfasoner”

En av alla drabbade är Carin, 100, bosatt i södra Sverige. Hon berättar i ”Efterlyst” hur en man som utgav sig komma från hennes bank tog kontakt över telefon för att meddela att hennes konto blivit kapat och att banken skulle hjälpa henne.

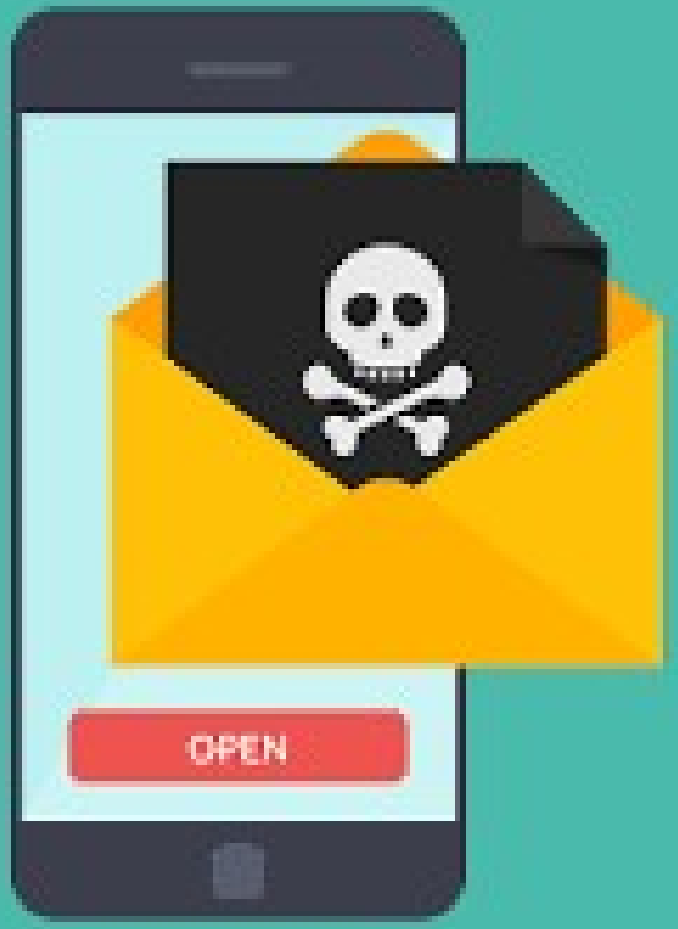
Carin var först skeptisk och bad att få tala med sin kontaktperson på banken. Då blev svaret att hon gått för dagen.

– Jag visste att hon hade haft lite glesa tjänstgöringsdagar så jag reagerade inte, säger Carin.

Mannen i telefonen berättade att en kollega till honom var på väg till henne för att stoppa kapningen genom att hämta hennes kontokort.

– Jag hade ingenting att sätta emot. Det lät lite övertygande alltihop, säger Carin.

Mannen som ringde bad henne stanna kvar i telefonen tills hans påstådda bankkollega kommit. Ett tillvägagångssätt som är vanligt, enligt polisen.



Smishing

- Sms som innehåller länkar till falska hemsidor eller skadlig kod.
- Lurar av folk på personliga uppgifter, ex. kontokortsinformation.

SSF råd

- Klicka aldrig på okända länkar
- Lämna aldrig ut privat information
- Logga aldrig in på BankID på uppmaning från okänd
- Gör en polisanmälan

SSF

Exempel smishing

Övriga tips och råd

- Om något verkar för bra att vara sant så är det nog inte sant.
- Var alltid kritisk när du får meddelande från någon okänd.
- Om osäker, så släng mail, radera sms direkt eller lägg på luren på en gång.

För fler råd, tips eller tricks gå in på:

sakerhetskollen.se

Säkerhetskollen
En tjänst från SSF

SSF

Frågor?

Paul Pintér

Rådgivare mot digitala brott

Mail: sakerhetskollen@stoldskyddsforeningen.se

Telefon: 08-783 74 00

Chatta med oss på sakerhetskollen.se