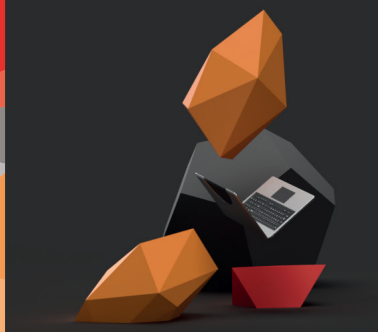


SE UPP FÖR Bedrägerier SOM PÅGÅR I DIN inkorg

Vad snackar vi om egentligen?

Phishing (nätfiske)

Bedragaren försöker komma åt pengar eller andra känsliga uppgifter om dig eller ditt företag. Oftast via mailutskick till stort antal mottagare. Men nu har trenden vänt och bedragarna vänder sig till specifika personer. En skrämmande utveckling eftersom attacken är mer utstuderad.

Spoofing

Hjälp! Någon skickar mail från min mailadress. Det kan innebära att du fått virus på dator eller att din mail är hackad. Men vanligast är att du blivit ”spoofad”. Någon använder dina uppgifter genom förfalskning. Det finns fortfarande inte så många kontroller av mailtrafik och mailservrar. Det har i princip varit fritt fram för bedragare att skriva in vilka mailadresser som helst. Men utvecklingen går snabbt framåt.

Ransomware

Är ett typ av virus som ofta sprids via email. Avsändaren är inte vem den utger sig för att vara och ber dig klicka på länkar eller ladda ner dokument. När man klickar på länken laddas viruset ner och låser alla dina filer på datorn. Det sprider sig via nätverket till server, program och dina kollegors datorer. I samband med detta får man ett meddelande om en lösensumma för att få tillbaka filerna som nu hålls om gisslan.

Bedragarens tillvägagångssätt

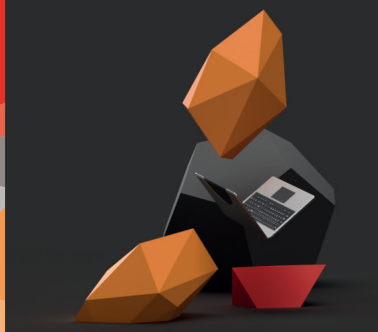
De tar reda på information om er och om företaget. Genom att surfa på er hemsida får bedragaren reda på namn och mailadresser och rikta personliga mail. Du kan också blivit lurad tidigare och klickat på en länk utan att det just då hände något. Vad som skett är att hackarna nu har full tillgång till din mail och kan lära sig exakt hur du skriver och hur din mailsignatur ser ut. Dessutom får de tillgång till alla dina kontakter och är bara ett stenkast ifrån att lura dem också.

Viktigt med säkra lösenord och multifaktorsinloggning

För att minska risken för intrång är det viktigt att inte använda samma lösenord på mer än ett ställe. Skilj alltid på jobbkonton och på privata konton. Använd alltid två-stegs-inlogg där det är möjligt detta kallas ofta MFA och 2FA och innebär ofta att man använder en autentiseringsapp eller sms.

Vad är ett säkert lösenord?
För att ingen ska kunna gissa lösenordet ska man inte använda namn eller siffror med kopplingar till dig eller företaget. Undvik enkla ord, som ”password” eller ”123456,” och vanliga lösenord som ”hejhej.” Använd minst 12 tecken. Blanda bokstäver i VERSALER och gemener, siffror och specialtecken som #@|∞&% och även mellanslag går ibland bra att använda. Att skapa en mening kan hjälpa dig att komma ihåg lösenordet.

netmine
PERSONLIG IT :)



03 enkla sätt ATT inte BLI DEN SOM klickade

Att-göra i mailkorgen

Virusen och hackare är smarta. Du måste bli smartare.
Du kan alltid öppna dina mail - MEN låt dig inte luras att klicka vidare i länkar och bilagor förrän du gjort följande:

01 Kolla e-postadressen & länken!

Vanligtvis kan du se på mailadressen att något är fel. Dubbelkolla länkar genom att föra muspekaren till länken utan att klicka. Kan du avgöra vart länken tar dig? Kolla efter konstiga tecken, namn, domännamn och ändelser. Kolla supernoga! Att göra pyttesmå tillägg är mycket vanligt.

02 Läs noga!

Ofta är mailen nu helt språkligt korrekta. Hackarna har koll på hur du skriver och vem du skriver till. Har man bråttom kan man därför lätt missta sig. Tänk efter två gånger!

03 Var misstänksam!

Det kommer ständigt nya avsändare och nya sätt att försöka lurar dig. Därför är det viktigt att du alltid är misstänksam. Och lämna aldrig ifrån dig dina inloggningsuppgifter. På senare tid ombeds du att logga in på ditt Microsoftkonto, och vips har du delat med dig av dina uppgifter. Fundera på om denna person verkligen vill dela en fil med mig?

Stora företag imiteras flitigt, dessa kan ni vara extra uppmärksamma mot:
PostNord, Microsoft, FedEx, Viasat, Spotify, DHL, Telia

”Oj, nu klickade jag ändå”

Pinsamt? Ja, kanske det men du måste agera snabbt!

01 Koppla ner dig från internet!

Stäng av ditt WIFI om du kör trådlöst, och annars drar du helt enkelt ut din nätverkssladd.

02 Stäng av datorn

Viruset jobbar på så länge det kan men om du stänger av dess möjligheter minimerar du skadan.

03 Kontakta Netmine - NU!

Ring direkt! Vänta inte. Alla tycker det är pinsamt. Ring. **Nu.** Växelnummer till Netmine: **0370-15590.**

04 Ha tålamod

Beroende på hur omfattande skadan blivit kommer det krävas olika mycket tid. Vi måste återläsa datan från den senaste backupen. Det tar sin tid.

De flesta som har klickat har snabbt kommit på vad de gjort. Det viktiga då är att följa punkterna och be om hjälp **DIREKT** för att minimera konsekvenserna!