



DATAOMBUDSMANNENS BYRÅ

HOAX, VAD ÄR DET?

Uppdaterad 15.9.2010

www.tietosuoja.fi

VAD ÄR ETT HOAX?

DU HAR MEJL FRÅN EN BEDRAGARE!

- vad innebär phishing?

Du har fått ett e-postmeddelande från din bank om att någon har försökt använda dina bankkoder. Banken ber dig byta till en säkrare kod. Dessutom ombeds du uppge såväl din nuvarande som din nya kod samt de fem följande engångslösenorden, så att bankens säkerhetsenhet kan testa om den nya koden är tillräckligt säker. Det känns tryggt att veta att de övervakar kundernas konton och meddelar om eventuella säkerhetsluckor så här snabbt per e-post. Banken ber dig fylla i uppgifterna via en länk i meddelandet. När du klickar på länken kommer du in på nätbankens välbekanta webbsidor.

Ett par veckor senare får du ett nytt meddelande från banken, denna gång per brev, och nu handlar det om att man misstänker att någon missbrukat ditt konto. Det visar sig att du har fått ett meddelande av en bedragare och besökt en falsk webbplats där du avslöjat dina bankkoder. Med hjälp av koderna har bedragaren kommit åt ditt konto under de senaste dagarna. Du har blivit utsatt för phishing, dvs. olovligt fiskande efter uppgifter.

Hur kan man bli lurad att lämna ut uppgifter över internet?

Bedragare har många olika knep för att lura alla som använder internet och olika nättjänster. Någon kan sända dig meddelanden där han eller hon ger sig ut för att vara någon annan och be dig skicka konfidentiella och sekretessbelagda uppgifter. Bedragaren kanske har byggt upp en webbplats som påminner om en webbank och begär där att få dina bankkoder. Bedrägeriförsöken blir allt mer avancerade och de falska webbplatserna allt mer trovärdiga. Förutom bankuppgifter kan en bedragare också fiska efter dina användarnamn och lösenord till olika datasystem och tjänster på internet genom att låtsas representera en enhet som ansvarar för databehandlingen i en viss organisation. Den här typen av bedrägeri betraktas så gott som alltid som ett brott.

Du kan åsamkas stor skada om en bedragare lyckas fiska fram sekretessbelagda uppgifter av dig och utnyttja dessa. Förutom att du kan förlora pengar och att någon kan komma åt att missbruka dina personliga rättigheter och förmåner, kan du framför allt förlora din tillförlitlighet. Uppgifter om dig kan hamna till exempel i register över betalningsstörningar på fel grunder, och då blir du även ofta bedömd på basis av denna information. I värsta fall kan dina uppgifter hamna i straffregistret. Det kan visa sig vara ytterst jobbigt och tidskrävande att korrigera felaktiga uppgifter; du vet ju inte ens vilka alla register som innehåller felaktiga uppgifter om dig.

Det är dock ganska enkelt att undvika "phishing" på internet. Du behöver bara tillägna dig några smarta vanor. För att kunna undvika att dina uppgifter hamnar i fel händer måste du lära dig vilka knep bedragare brukar använda. Dessutom bör du känna till hur till exempel banker eller databehandlingsenheter går till väga när de meddelar sina kunder om oklarheter. Du gör också klokt i att på förhand fundera ut vad du ska göra om du misstänker att du blivit utsatt för bedrägeri.

AGERA SMART OCH SNABBT

Här får du några råd om hur du kan minska riskerna för att bli offer för bedrägeri, hur du kan avslöja eventuella bedrägeriförsök samt vad du ska göra om du misstänker att du blivit utsatt för ett sådant:

1) Ta reda på enligt vilka principer de instanser som erbjuder nättjänster agerar

- Ta reda på hur de instanser som erbjuder dig tjänster, t.ex. bankerna, gör för att garantera säkerheten i sina nättjänster. Är till exempel kommunikationen till och från nättjänsten krypterad? En pålitlig tillhandahållare redogör för dessa åtgärder på sin webbplats.
- Ta reda på hur man kontaktar dig till exempel om det blir aktuellt att byta lösenord eller dylikt; ingen pålitlig instans begär eller skickar sekretessbelagda uppgifter per e-post.
- Ta reda på hur dina uppgifter behandlas i allmänhet. Bästa sättet att få reda på detta är att läsa instansernas dataskyddsprinciper och -policy. En pålitlig tillhandahållare berättar om dessa på sin webbplats, men kom ihåg att också bedragare kan redogöra för sina tillvägagångssätt på ett till synes tillförlitligt sätt.

2) Följ själv principerna om säker och tillförlitlig användning av e-post och internet för övrigt

- Det är lätt att förfalska uppgifterna om avsändaren av ett e-postmeddelande; besvara inte meddelanden från okända avsändare eller meddelanden som verkar opålitliga.
- Skicka inte sekretessbelagda uppgifter om dig själv per e-post, om du inte har skyddat kommunikationen till exempel genom att kryptera uppgifterna. Överlag bör du aldrig avslöja känsliga uppgifter om dig själv över internet, om du inte har förvissat dig om att motparten är tillförlitlig.
- Ta till vana att alltid efter bästa förmåga förvissa dig om att en instans som skickat dig e-post har ärliga avsikter eller att webbplatsen för en instans som tillhandahåller nättjänster är autentisk.

3) Agera snabbt om du misstänker att du blivit utsatt för bedrägeri eller bedrägeriförsök

- Du kan till exempel kontakta den instans som avsändaren av e-postmeddelandet ger sig ut för att representera och fråga vad saken gäller.
- Om du misstänker att du blivit utsatt för bedrägeri eller bedrägeriförsök bör du meddela den involverade instansen, till exempel din bank, att den kanske utnyttjas av bedragare.
- Spärra konton som blivit eller riskerar att bli missbrukade.
- Byt koder och lösenord som kan ha hamnat i händerna på en bedragare.
- Kontakta polisen om det är fråga om ett uppenbart brott.
- Kontakta också polisen i det fall att dina personuppgifter har missbrukats.
- Om du stöter på oklarheter angående behandlingen och användningen av dina personuppgifter ska du kontakta den instans som behandlar uppgifterna. Du kan också vända dig till dataskyddsmyndigheterna.