VÄSTERVIKS KOMMUN

Socialförvaltningen

11 januari 2023

Lathund om bedrägeri

Bli inte lurad och skydda dig med svåra lösenord

Malin Ekdahl

VÄSTERVIKS KOMMUN

Innehåll

VÄSTERVIKS KOMMUN

Vad är bedrägeri?

”Bedrägeri innebär att en gärningsperson lurar någon att göra något, eller att inte göra något som denne annars skulle ha gjort. Det medför att gärningspersonen tjänar ekonomiskt på det och att det leder till ekonomisk skada för den som blir lurad.” (www.polisen.se)

Olika former av bedrägeri

Phising – nätfiske

En person försöker skada dig som person genom att komma åt dina bankuppgifter, känslig information eller dina inloggningsuppgifter genom att försöka komma in på din dator. De kan skicka in trojaner, virus eller installera spionprogram på din dator för att se vad du gör.

Se upp med misstänkta e-post som exempelvis att:

- Ber dig att lämna ifrån dig kort- eller kontonummer.
- Ber dig lämna ifrån dig lösenord.
- Ber dig att klicka på okända länkar.
- Ber dig verifiera din kontoinformation.
- Hotar med att stänga ner ditt konto på kort tid.
- Lockar med osannolika erbjudanden.
- Innehåller dålig grammatik, stavning eller ordföljd.
- Innehåller konstiga rubriker eller icke-personligt tilltal i e-post.

Om du tror att du är utsatt av phising. Stanna upp och tänk efter. Öppna inte någon bilaga, klicka inte på någon länk och agera inte på någon instruktion. Fråga någon om hjälp eller en andra åsikt. Om du känner den påstådda avsändaren så kontakta denne på ett annat sätt för att fråga om detta stämmer.

Smishing – smsfiske

Du får sms där de vill att du ska lämna ut dina uppgifter. De vill att du ska klicka på en viss länk för att sedan fylla i dina uppgifter så de kommer åt pengar från dig. Klicka inte på okända länkar eller bifogade filer.

Vishing – röstfiske

Du blir uppringd och de försöker lura dig att ge ifrån dig dina kontouppgifter. Det kan vara så att de kan ditt personnummer och ber dig logga in på ditt Bank-ID. Du tror du loggar in på en viss sida, men i själva verket loggar du in på en annan sida och de kan föra över pengar från dig. Den enda gången du får logga in med ditt Bank-ID är när du själv ringer upp banken, ett företag eller en myndighet. Blir du uppringd så be att du får deras namn och telefonnummer så att du kan ringa upp till tex företaget/myndigheten och höra efter så att det stämmer.

Påhälsning hemma

Om någon kommer och ringer på dörren hos dig, så måste du inte öppna och släppa in personen. Det är ditt hem och du bestämmer där. Känner du dig osäker

så be att du får se deras legitimation. Fota av eller skriv ner personens uppgifter och varifrån de säger att de kommer. Säg att du inte har tid att släppa in dem just nu och be dem återkomma. Tills de kommer åter har du möjlighet att i lugn och ro ringa och höra efter så att detta är en okej person.

ID-kapning

Någon har stulit din identitet för att ta lån i ditt namn. De köper saker och fakturan går till dig. Andra personer blir lurade för de tror att det är du som hör av sig. Dina uppgifter kan säljas vidare för att fler och fler ska kunna fortsätta att kapa dig.

Lösenord

Det är viktigt att ha bra och svåra lösenord till sina tjänster. Ett lösenord är en av de två ”nycklarna” som behövs för att komma åt ditt konto. Den andra ”nyckeln” är ditt användarnamn. Har en person bara ena kan de ej komma åt din information, men så fort en person har båda dina uppgifter kan de logga in på ditt konto.

De vanligaste lösenorden enligt Internetstiftelsen

- 123456
- 123456789
- Qwerty
- Password
- 1234567
- 12345678
- 12345
- Iloveyou
- 111111
- 123123

Använder du något av dessa lösenord ska du genast byta till ett svårare och krångligare. Du ska välja ett ovanligt lösenord och gärna är långt helst nio till tio tecken långt. Ju längre och konstigare desto bättre är det. Använd ditt lösenord till endast en tjänst. Lösenordet du har till din e-postadress ska du endast använda till den tjänsten. Det är bättre att använda en fras i stället för ett ord. Tycker du att det är svårt att komma ihåg alla lösenord kan du använda dig av en lösenordshanterare. Det är också säkert att använda tvåvägsautentisering.

Tecken som kan användas till lösenord

Det finns totalt 95 olika tecken som du kan använda för att skapa ett lösenord. Blanda stora bokstäver, små bokstäver, siffror och symboler. Det kan vara lätt för dig, men krångligt för andra.

- Versaler: A till Z (26 tecken)
- Gemener: a till z (26 tecken)
- Siffror: 0 till 9 (10 tecken)

- Symboler: (mellanrum) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 tecken)

Exempel på lösenord kan vara Frankrike98# (1998 var du i Frankrike och klättrade över staket. Enkelbeckasin 23!FB (Du har sett en bild på Facebook med 23 stycken Enkelbeckasiner). Jag-Gillar-Goda-Kakor (du blandar olika tecken till en mening). Det finns många sätt att skapa lösenord. Skapa dig ett sätt att göra dem. Använd detta sätt i olika former när du kommer på dina lösenord.

Ju längre lösenord du skapar ju längre tid tar det för en dator att hacka ditt lösenord. Sex tecken tar 30 sekunder att knäcka, åtta tecken tar 29 timmar att knäcka, tio tecken tar elva år att knäcka och 12 tecken tar ca 37 millennier att knäcka.

Lösenordshanterare

För att du inte ska behöva komma ihåg dina krångliga lösenord kan det vara bra att använda en lösenordshanterare. De finns oftast inbyggda i telefonen, i en webbläsare eller att du installerar ett program på datorn eller telefonen. På iPhone är den inbyggd i ditt moln i Cloud och på en Android är den inbyggd på Googlekontot.

Tvåfaktorautentisering

Ett sätt att skydda sig är att använda tvåfaktorautentisering. Det betyder att du måste bekräfta inloggningen på flera ställen än ett. Det kan vara så att du ska godkänna med bank-ID eller att du får en kod på sms eller e-post som du ska skriva in för att få logga in. Detta är en säkerhet för att inte någon annan ska logga in på ditt konto. Fördelen är att du får ett meddelande (oftast på e-post) att någon har försökt att logga in.

Lösenord till Bank-ID

Det kan vara svårt att komma ihåg alla siffror som ska vara med i lösenordet till bank-ID. Det sämsta lösenordet är ditt eller någon i din närhets personnummer. Ett sätt att komma ihåg sitt lösenord är att göra om siffrorna till bokstäver som du kan bilda ett ord eller mening av. En ett genererar ingen bokstav, en tvåa genererar A, B eller C. En trea genererar D, E eller F. Så fortsätter det. Bokstäverna syns på knapparna. Exempel kan vara sjumilakliv blir 75864525548 och HarryPotter blir 42779768837.

Byta lösenord

Du kan behöva byta ditt lösenord om du inte känner att det är så bra eller om du tror att du blivit hackad. Om du kan ditt nuvarande lösenord kan du logga in på sin sida och gå till din profil. Därifrån kan du oftast byta lösenord. Om du inte kan ditt lösenord brukar det finnas en länk där det står tex ”Glömt lösenord”. Klicka på den länken och följ instruktionerna. Glöm inte att anteckna dina lösenord så du kan logga in nästa gång.