Lär dig genomskåda bedrägeriförsök

Mer än 50 procent säger sig ha blivit utsatta för bedrägeri eller bedrägeriförsök på nätet det senaste året, enligt Internetstiftelsens undersökning. Så här undviker du att gå i fällan!

Över hälften av alla internetanvändare säger att de utsatts för bedrägeri eller bedrägeriförsök på nätet det senaste året. Det visar Internetstiftelsens undersökning Svenskarna och internet 2022.

I de allra flesta fallen handlar det om bluffmejl och bluff-sms, alltså där avsändaren är någon annan än vad det verkar. Här får du veta mer om hur bedragarna går till väga och hur du kan undvika att gå i fällan.

Vinna ditt förtroende

”Idag är sista dagen att använda dina intjänade poäng. Gå in i vår poängshop via länken här för att lösa in dem.”

Avsändaren till sms:et ovan är en stor livsmedelskedja. Idag är det väldigt enkelt för bedragare att använda sig av spoofing-tjänster som gör att deras mejl och sms ser ut att komma från någon annan. Genom att använda sig av företag där många svenskar är kunder är chansen större att bedragarna lyckas lura dig. De vet också att vi har stort förtroende för myndigheter och välgörenhetsorganisationer.

Rätt timing

”Vi saknar uppgifter i din deklaration, se bifogad fil.”

Mejlet, som verkar komma från en handläggare på Skatteverket, skickas i deklarationstider. Tajmingen är en medveten taktik för att minska din vaksamhet. Innan jul ökar exempelvis mängden sms om falska paketleveranser, där leverantören vill få ”bekräftelse” för att dela ut paket.

Trigga stress

”Det har skett ett intrång på ditt Facebook-konto. Om du inte kontaktar vår support via denna länken inom 48 timmar tvingas vi stänga ditt konto.”

Den vanligaste taktiken som används av bedragare är stress. Under tidspress tappar vi en del av vårt logiska och kritiska tänkande. Ta för vana att alltid ifrågasätta mejl och sms som innehåller en tidsbegränsning, oavsett om det gäller en varning eller ett erbjudande.

3 tips för att slippa bli lurad:

1. Lita inte på avsändarnamnet eller avsändarnumret

Det är enkelt för bedragarna att förfalska avsändaren och du kan aldrig vara helt säker på att mejl eller sms är äkta. Innan du agerar, dubbelkolla äktheten genom att kontakta den påstådda avsändaren via en kontaktväg som du själv letar upp.

2. Klicka inte på länkar i mejl, sms och andra textmeddelanden

Genom att få dig att fylla i personliga uppgifter på en förfalskad webbsida eller kontakta ett falskt telefonnummer vill bedragarna komma åt dina personliga uppgifter. De kan till exempel användas till att stjäla dina pengar eller ta lån i ditt namn.

3. Öppna inte bifogade filer i mejl och andra textmeddelanden

Öppnar man en bifogad fil från en bedragare är risken stor att datorn infekteras med virus eller andra skadeprogram. Filen kan innehålla ett virus eller skadligt program. En vanlig typ är så kallade spionprogram som registrerar allt du gör på laptopen eller mobilen och skickar den informationen till bedragarna, inklusive när du fyller i dina lösenord och kortuppgifter.

Så skyddar du din dator och mobil

- Se till att ha ett bra antivirusprogram och aktivera din dators brandvägg.
- Uppdatera operativsystem, appar och program direkt när det finns nya uppdateringar. De täpper till säkerhetshål vartefter de upptäcks.
- Använd olika, unika lösenord till alla dina inloggningar.

Källa: Internetstiftelsen