Undvik att bli lurad!

Kom ihåg att alla kan bli lurade. Är man stressad är man särskilt utsatt. Som brottsutsatt upplever man ofta stor skam. Information och råd om detta finns i en senare del av webinariet nedan som alla dessa uppgifter hämtats ifrån (adress längst ner).

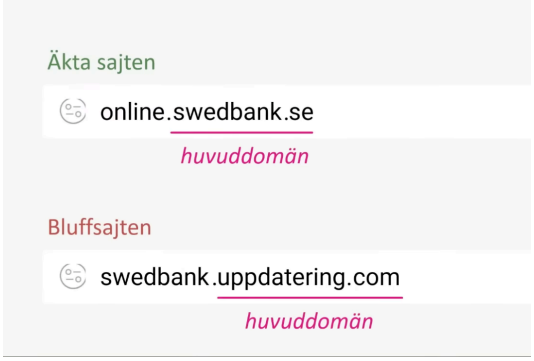
Falska SMS

Bedragare kan skicka SMS som ser ut att komma från en av dig känd avsändare. Om man tidigare haft SMS kontakt grupperas de bedrägliga SMS i samma SMS tråd som de riktiga. Ett exempel är avsändaren ”Din Bank” som Sparbankerna ofta använder och de blir därför särskilt svåra att upptäcka.
Vid minsta misstanke lita inte på att avsändaren är den uppgivna och följ inte uppmaningarna. Om du är osäker leta själv upp telefonnumret.

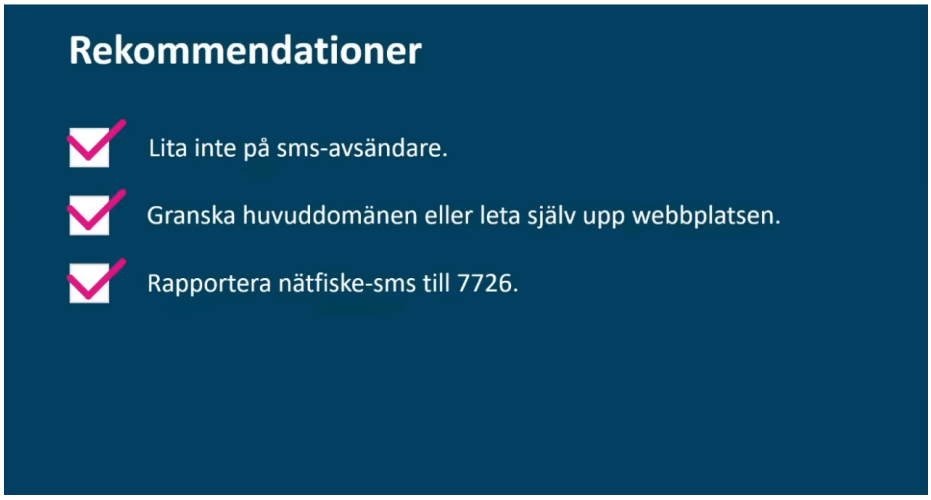
Du kan hjälpa andra genom att skicka en kopia av bilden i mobil eller dator till telefonnumret som du får om du ändrar bokstäverna SPAM i mobilen till siffror, **7726**. Det går till alla operatörer.

Falska webbplatser

För att kolla om en webbplats är äkta eller inte, **kolla huvuddomänen** = sista delen i adressen före .se eller .com eller liknande.
Exempel



Undersök hemsidans adress!
Det som står före och efter huvuddomänen är det som domänägaren själv kan ändra (Subdomäner) och som kan vara avsett att lura oss.



Falska annonser på ex. Meta (Face-book)

Ofta handlar det om uppmaningar att investera. Bedragare utnyttjar t.o.m. profiler från *Uppdrag Granskning*. Allt är fake.

Annonsen går till SVT.se eller Aftonbladet.se sägs det längst ner i annonsen. Men det gör det inte! Kolla på huvuddomänen!
Webbplatsen är kopierad.

Klicka inte på annonser på sociala medier utan att ha säkerställt att det inte är bedragare bakom (domängranskning).

Källa

Uppgifterna kommer från en webföreläsning på Youtube av Internetstiftelsen
Hela Sveriges säkerhetsevent – Tänk Säkert 2025