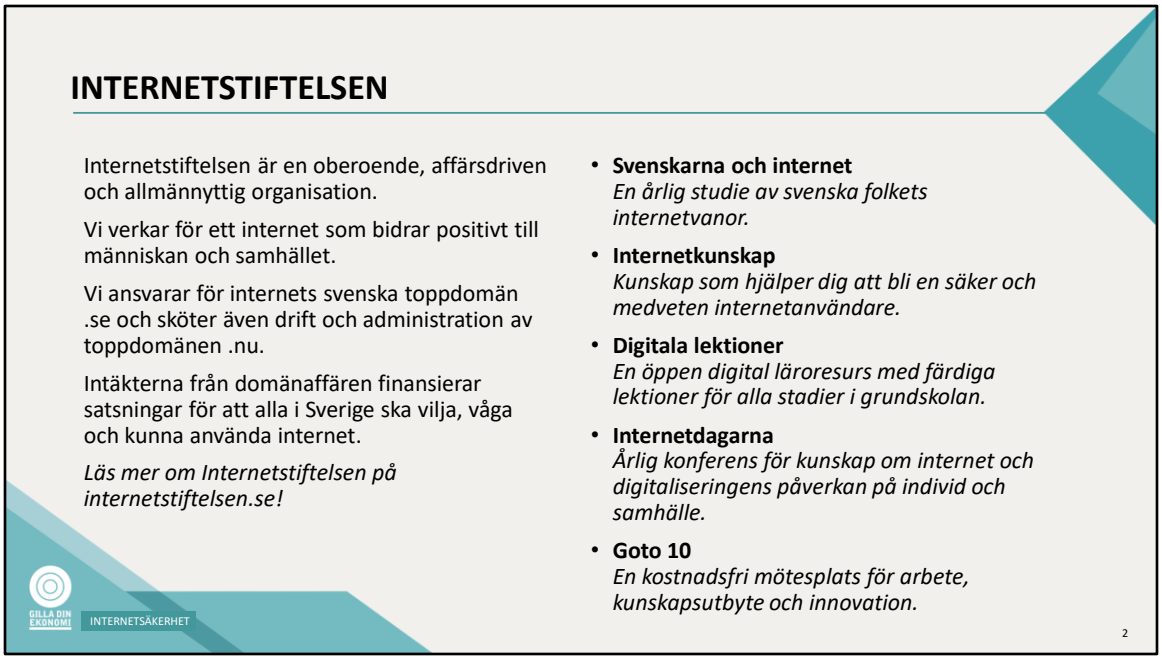
INTERNETSÄKERHET

Internetstiftelsen

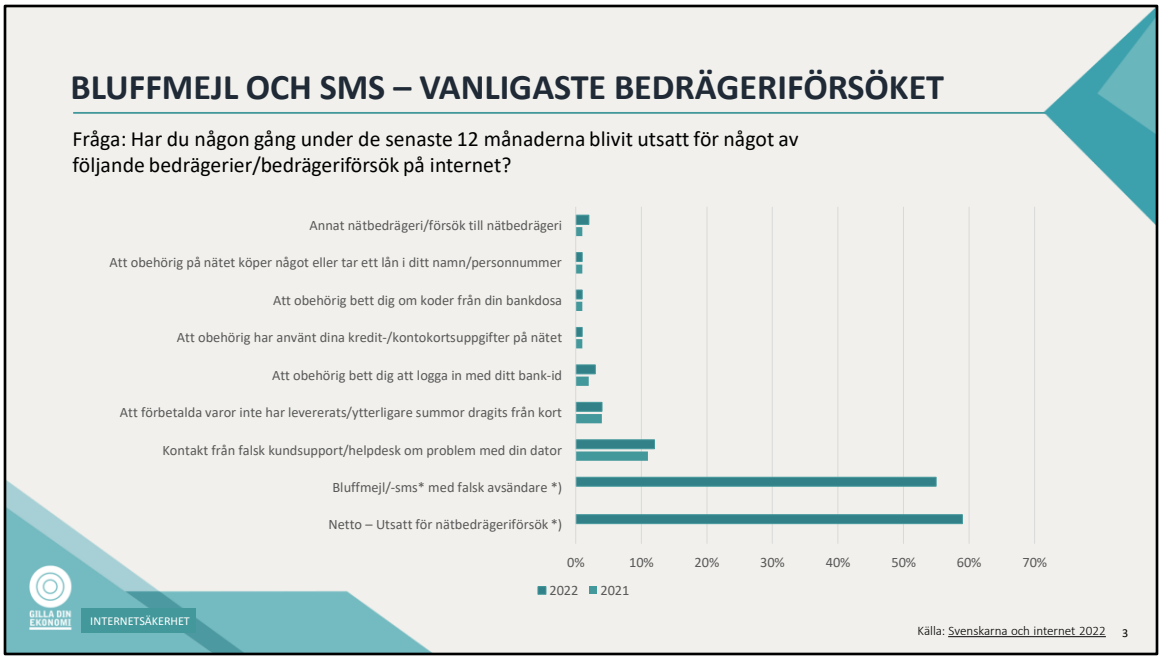
GILLA DIN EKONOMI



Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu.

Intäkterna från domänaffären finansierar satsningar för att alla i Sverige ska vilja, våga och kunna använda internet. Och till höger i presentationsbilden finns en del av det främjandearbete vi gör listat. Vill man hitta mer om det som jag tar upp idag ska man gå till internetkunskap.se och klicka på ”säkerhet på nätet”

Svenskarna och internet – https://svenskarnaochinternet.se/
Internetkunskap - https://internetkunskap.se/
Digitala lektioner - https://digitalalektioner.se/
Internetdagarna - https://internetdagarna.se/
Goto 10 - https://www.goto10.se/



För att få en uppfattning om hur vanligt det är med bedrägerier och bedrägeriförsök på nätet kan vi titta på den här bilden.
Den är från vår egen undersökning Svenskarna och internet 2022 där vi frågat internetanvändare från 16 år.

Här ser vi att nästan 6 av 10 internetanvändare över 16 år anger att de har blivit utsatta för någon typ av nätbedrägeri under det senaste året.

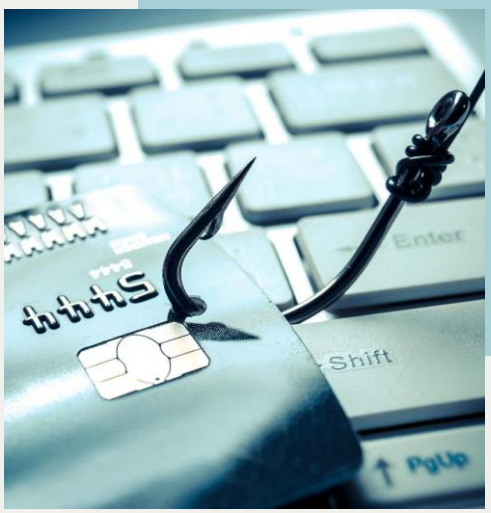
Vi ser också att det överlägset vanligaste nätbedrägeriet att bli utsatt för är olika typer av bluffmejl och bluff-sms, vilket mer än hälften av internetanvändarna har drabbats av.

VAD INNEBÄR NÄTFISKE?

Nätfiske är det svenska ordet för engelskans ***phishing*** och innebär att bedragare försöker lura – eller ”fiska” – av dig lösenord, koder, betalkortuppgifter eller annan personlig information.

Bedragarna vill åt den här informationen för att:

- Kunna stjäla dina pengar
- Sälja den vidare till andra bedragare
- Kapa din identitet
- Kapa dina användarkonton och lura andra



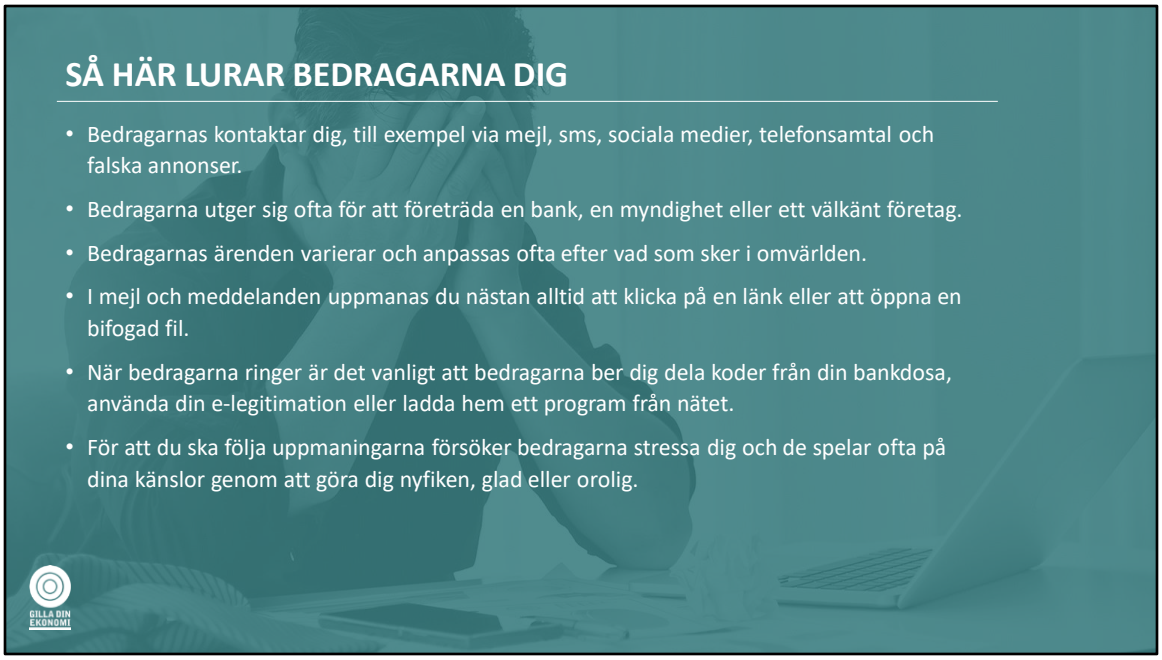
GILLA DIN EKONOMI INTERNETSÄKERHET

4

Den här vanligaste typen av internetbedrägerier ryms nästan alla inom det som man ibland kallar för nätfiske.
Därför känns det rimligt att ge en förklaring till det begreppet.

Nätfiske (efter engelskans phising) innebär att bedragaren försöker lura oss att själva dela med oss av personlig information,
Till exempel lösenord, koder eller betalkortuppgifter.

Och anledningen till att bedragarna vill lura till sig den här informationen är vanligtvis att:
- kunna stjäla dina pengar
- sälja den vidare till andra bedragare
- kapa din identitet
- eller kapa dina användarkonton och lura andra



Så hur luras bedragarna?
//
Jo, det startar alltid med att bedragarna kontaktar dig på något sätt.
Mejl och sms är vanligt som vi såg tidigare.
Andra kontaktvägar är sociala medier, telefonsamtal och falska annonser
//
För att lura dig är det vanligt att bedragarna låtsas företräda en bank, en myndighet eller ett välkänt företag.
Bedragarna försöker med andra ord utnyttja människors förtroende och beroendeställning till dessa institutioner.
//
Bedragarnas ärenden varierar och de är väldigt skickliga på att anpassa sig efter omvärlden.
Innan jul handlar många bluffar till exempel om paketleveranser,
Och i deklarationstider är det vanligt med bluffmejl som ser ut att komma från Skatteverket.
//
Gemensamt för bluffmejl och bluffmeddelanden är att man nästan alltid uppmanas att klicka på en länk eller att öppna en bifogad fil.
//
När bedragarna ringer är det vanligt att de:
- ber dig att dela koder från din bankdosa
- använda din bankdosa eller din e-legitimation

- eller att ladda att hem ett program från nätet

//

För att du ska följa uppmaningen försöker bedragarna stressa dig – det finns nästan alltid en tidsfrist

Och de spelar ofta på dina känslor genom att göra dig nyfiken, glad eller orolig.

EXEMPEL 1: SÅ HÄR LURAR BEDRAGARNA DIG

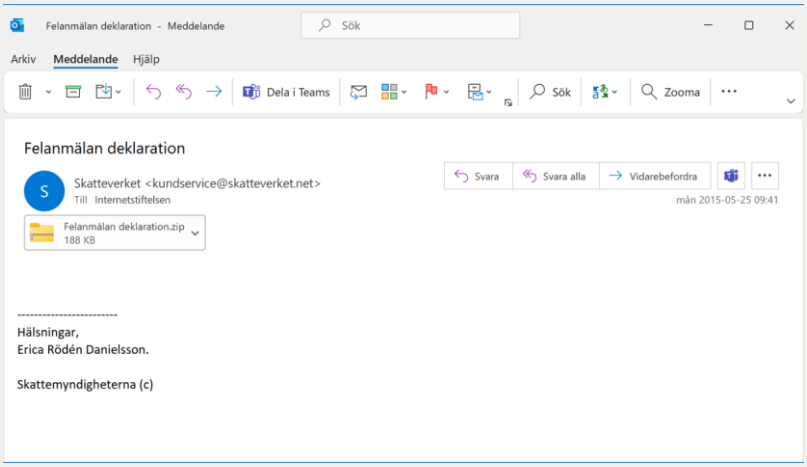
GILLA DIN EKONOMI INTERNETSÄKERHET

6

Här är ett exempel:

Avsändaren ser ut att vara ett välkänt företag, nämligen Coop.
Ärendet handlar om att 27101 bonuspoäng måste förbrukas – det finns en tidsfrist på 4 timmar
Och det finns en uppmaning att klicka på en länk.

EXEMPEL 2: SÅ HÄR LURAR BEDRAGARNA DIG



GILLA DIN EKONOMI

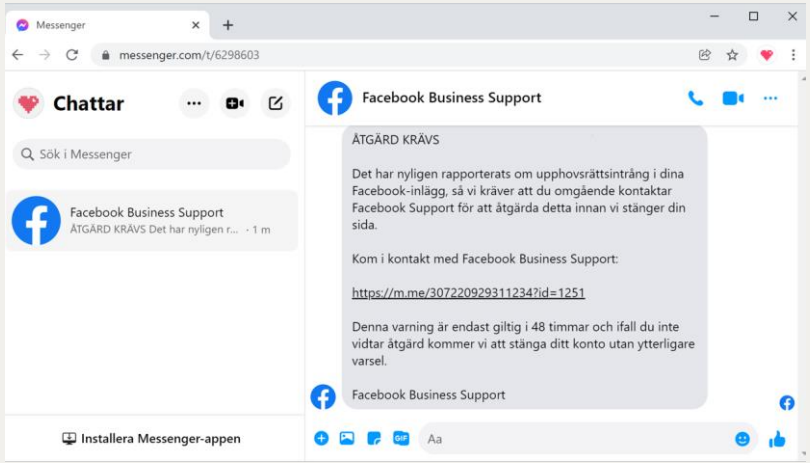
INTERNETSÄKERHET

7

Här är ett annat exempel på hur det kan se ut när mejlet innehåller en bifogad fil.

Avsändaren påstår sig vara Skatteverket och det finns en bifogad fil som är döpt ”felanmälan deklaration”

EXEMPEL 3: SÅ HÄR LURAR BEDRAGARNA DIG



GILLA DIN EKONOMI INTERNETSÄKERHET

8

Här påstår sig bedragarna vara Facebook vilket kanske är lite extra lurigt då bedrägeriförsöket sker på just Facebook Messenger.

Men kännetecknen för en bluff finns där:
Mottagaren uppmanas att klicka på en länk för att åtgärda ett påstått upphovsrättsintrång.
Och det finns en tidsfrist på 48 timmar, allt för att stressa mottagaren.

EXEMPEL 4: SÅ HÄR LURAR BEDRAGARNA DIG

GILLA DIN EKONOMI INTERNETSÄKERHET

9

Sen ett exempel som är något av ett undantag, för att visa att man alltid måste vara på sin vakt.

Ett sms som påstås komma från Handelsbanken, men utan någon länk att klicka på.
Här är uppmaningen istället att ringa ett specifikt nummer.
Och gör man det så fortsätter bluffen i det samtalet.

Så hur ska man skydda sig mot nätfiske då?

Här är 7 grundläggande tips som är ett första steg på vägen mot att undvika att bli lurad.

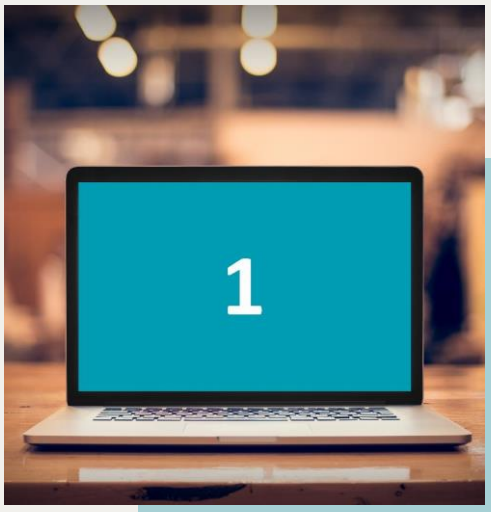
TIPS 1

Undvik att klicka på länkar i mejl, sms och textmeddelanden.

Klickar du på en länk i bedragarnas mejl och meddelanden leds du vanligtvis vidare till en falsk webbsida där du uppmanas att logga in med ditt lösenord, knappa in ditt kortnummer eller dela annan personlig information.

Det kan till exempel vara en falsk webbshop, en falsk kopia av en myndighetssida eller en falsk inloggningssida till en streamingtjänst.

De falska webbsidorna ser äkta ut, men så fort du knappar in din information stjäls den av bedragarna.



GILLA DIN EKONOMI INTERNETSÄKERHET

11

Tips 1 är att i största möjliga mån undvika att klicka på länkar i mejl, sms och olika textmeddelanden.

Det här är ett svårt råd att ge eftersom Internet handlar mycket om att klicka på länkar.
Men det går aldrig att vara 100% säker på att mejl eller sms är äkta.
Därför bör man vara väldigt försiktig med länkar och i alla fall dubbelkolla med den påstådda avsändaren via en kontaktväg som man själv letar upp innan man klickar på något.

Jag tänkte faktiskt att vi kunde titta på vad som vanligtvis händer om man klickar på en länk i ett bluffmeddelande.

EXEMPEL: UNDVIK ATT KLICKA PÅ LÄNKAR

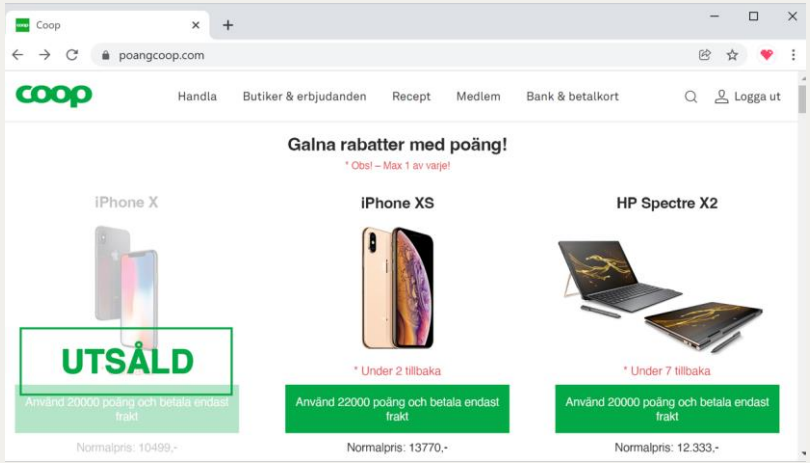
GILLA DIN EKONOMI INTERNETSÄKERHET

12

Här är bluff-sms:et som jag visade tidigare.
Det som påstod sig komma från Coop.

Klickar vi på den länken…

EXEMPEL: UNDVIK ATT KLICKA PÅ LÄNKAR



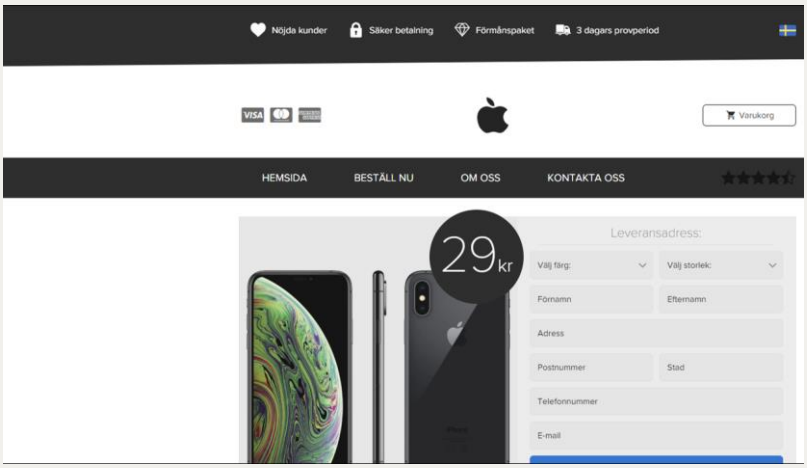
GILLA DIN EKONOMI INTERNETSÄKERHET

13

Hamnar vi här.
På en falsk webbsida designad för att likna Coops riktiga.
Men titta på adressen i webbläsaren.
Där står det *poangcoop.com* och inte *coop.se* som är Coops riktiga webbadress.
Vi är alltså på en falsk webbsida just nu

Hur som helst
Vi väljer iPhone XS och klickar på den…

EXEMPEL: UNDVIK ATT KLICKA PÅ LÄNKAR



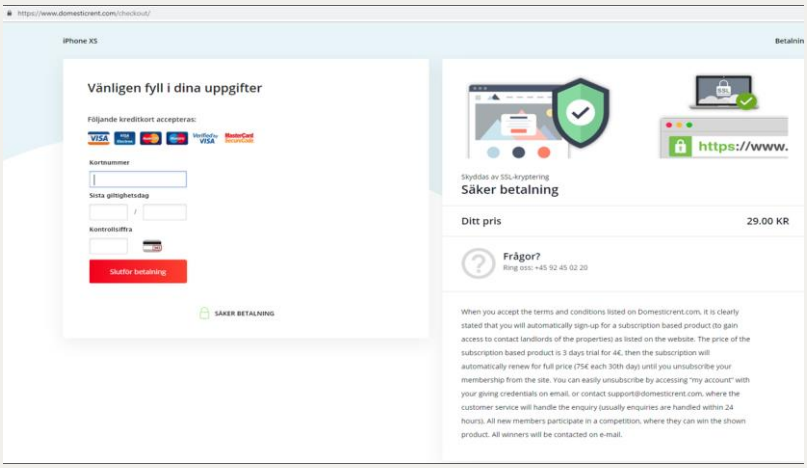
GILLA DIN EKONOMI INTERNETSÄKERHET

14

Då hamnar vi här.
På ytterligare en falsk sida designad för att likna Apples.

Här ombeds vi fylla i leveransadress och när vi gjort det…

EXEMPEL: UNDVIK ATT KLICKA PÅ LÄNKAR



GILLA DIN EKONOMI INTERNETSÄKERHET

15

Då hamnar vi här.

Nu är det alltså dags att betala den där lilla fraktavgiften på 29 kronor.

Och när vi knappar in våra kortuppgifter och trycker på ”Slutför betalning” så har vi både delat våra kortuppgifter, men i det här fallet har vi också godkänt det finstilta (till höger i bild) som i det här fallet är en prenumeration som kostar 75 euro i månaden.

TIPS 2

Undvik att öppna bifogade filer i mejl och andra textmeddelanden.

- Öppnar du en bifogad fil i bedragarnas mejl och meddelanden är risken stor att din dator infekteras med virus och spionprogram.
- Ett spionprogram är ett skadeprogram som registrerar allt du gör kan skicka din personliga information, till exempel lösenord och betalkortuppgifter, till bedragarna.

GILLA DIN EKONOMI INTERNETSÄKERHET

16

Tips 2 är likt tips 1 och handlar om att man ska undvika att öppna bifogade filer i mejl och andra textmeddelanden.

Även det här är ett svårt tips att efterleva, eftersom vi ganska ofta får filer skickade till oss.
Men ta för vana att dubbelkolla med den påstådda avsändaren innan ni öppnar något.

Öppnar man en bifogad fil från en bedragare är risken stor att datorn infekteras med virus eller andra skadeprogram.

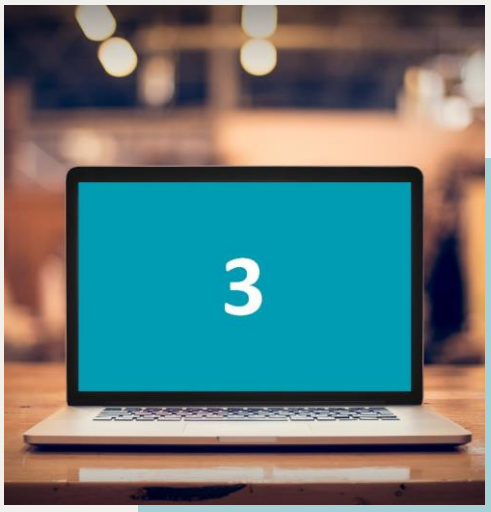
En typ av skadeprogram är så kallade spionprogram som registrerar allt du gör och skickar den informationen till bedragarna.
Det kan till exempel vara lösenord och kortuppgifter.

TIPS 3

Lägg på luren, våga vara bestämd!

Det här gäller om någon som ringer dig:

- Efterfrågar dina kortuppgifter
- Vill att du ska ladda ner ett program från internet
- Uppmanar dig att använda din bankdosa, ditt bank-id eller annan e-legitimation
- Ber dig att läsa upp koder från bankdosan eller ditt bank-id



GILLA DIN EKONOMI INTERNETSÄKERHET

17

Tips 3 är att lägga på luren om någon som ringer dig ber dig läsa upp dina kortuppgifter eller att ladda ner ett program från internet. Oavsett vad det är för anledning eller ärende.

Detsamma gäller om den som ringer uppmanar dig att använda din bankdosa, ditt bank-id eller annan e-legitimation.

Det gäller också om den som ringer ber dig att läsa upp koder från bankdosan eller ditt bank-id.

Kom ihåg att banker, myndigheter och seriösa företag aldrig tar kontakt med dig och ber om detta över telefon. De kan dock be dig om det här om du ringer dem. Så det finns en skillnad här i vem som kontaktar vem.

TIPS 4

Lita aldrig på avsändarnamn och uppringande nummer.

- Kom ihåg att du aldrig kan lita på avsändarnamn i mejl, sms och andra textmeddelanden. Det är superenkelt för bedragarna att förfalska.
- Du kan inte heller lita på att det uppringande numret eller det nummer som visas i ett sms är äkta.
- För att kontrollera om mejlet, telefonsamtalet eller textmeddelandet är äkta kan du kontakta den påstådda avsändaren via en kontaktväg som du själv letar upp.
- Svara aldrig på misstänkta mejl, telefonsamtal och textmeddelanden.

GILLA DIN EKONOMI INTERNETSÄKERHET

18

Tips 4 är att aldrig lita på avsändarnamn, uppringande nummer eller avsändarnummer i sms.

Det här är superenkelt för bedragarna att förfalska och kan inte användas för att avgöra äktheten.

Återigen:
Innan du agerar på ett mejl, meddelande eller telefonsamtal bör du dubbelkolla äktheten genom att kontakta den påstådda avsändaren via en kontaktväg som du själv letar upp.

TIPS 5

Var kritisk mot annonser på webben och sociala medier.

- Se upp för annonser med fantastiska erbjudanden, gratisprodukter, investeringsförslag, tävlingar och olika quiz.
- Kom också ihåg att din dator inte har fått virus bara för att det står så i olika pop up-fönster på webben. Dessa varningar är falska och syftar till att infektera din enhet med virus.

GILLA DIN EKONOMI INTERNETSÄKERHET

19

Tips 5

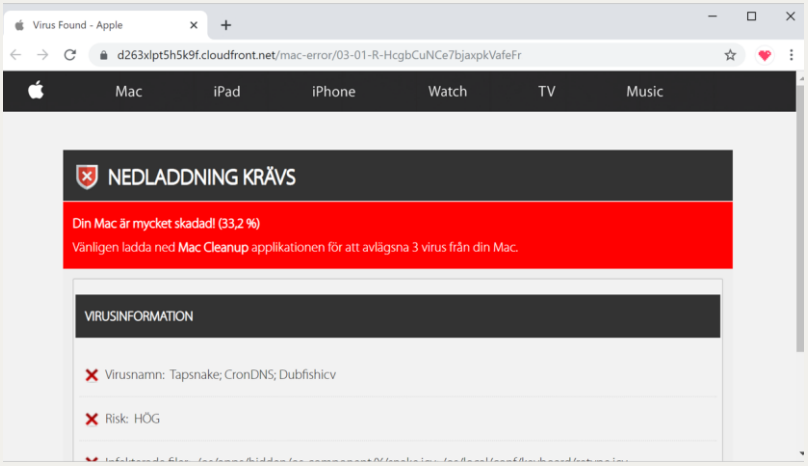
Var alltid kritisk mot annonser på webben och sociala medier. Annonser på nätet kontrolleras nämligen sällan av människor innan de läggs upp.

Falska annonser på webben och sociala medier är därför ett vanligt sätt för bedragare att lura till sig pengar, kortuppgifter och lösenord, eller för att sprida virus och andra skadeprogram.

Kom också ihåg att datorn inte har fått virus bara för att det står så i olika pop up-fönster på webben eller i webbläsaren.

Dessa varningar är falska och syftar tvärtom till att infektera din enhet med virus.

EXEMPEL: FALSK VIRUSVARNING



GILLA DIN EKONOMI INTERNETSÄKERHET

20

Så här kan en falsk virusvarning se ut.

Sajten försöker efterlikna Apples, men vi kan se på webbadressen att det är en falsk sida.

TIPS 6

Skydda dina dator mot virus och andra skadeprogram.

- Använd ett bra antivirusprogram och aktivera din dators brandvägg.
- Uppdatera operativsystem, appar och program direkt när det finns nya uppdateringar.
- Avinstallera och radera appar och program när du inte använder dem längre.

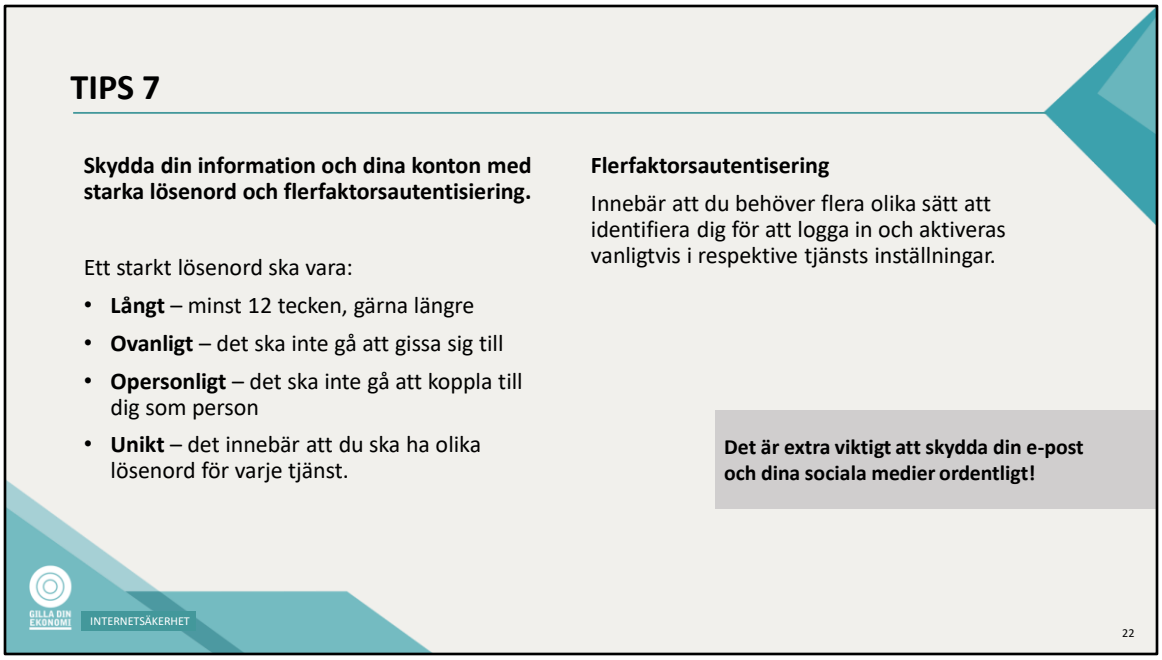
GILLA DIN EKONOMI

INTERNETSÄKERHET

21

Tips 6 är en viktigt hygienfaktor, nämligen att skydda sin dator mot virus och andra skadeprogram genom att använda ettt bra antivirusprogram och att aktivera datorns brandvägg.

Se också till att uppdatera operativsystemet, appar och program direkt när det finns nya uppdateringar. Uppdateringar täpper nämligen till kända säkerhetshål, som bedragare annars kan utnyttja.



Tips 7 – det sista tipset - handlar om lösenord.

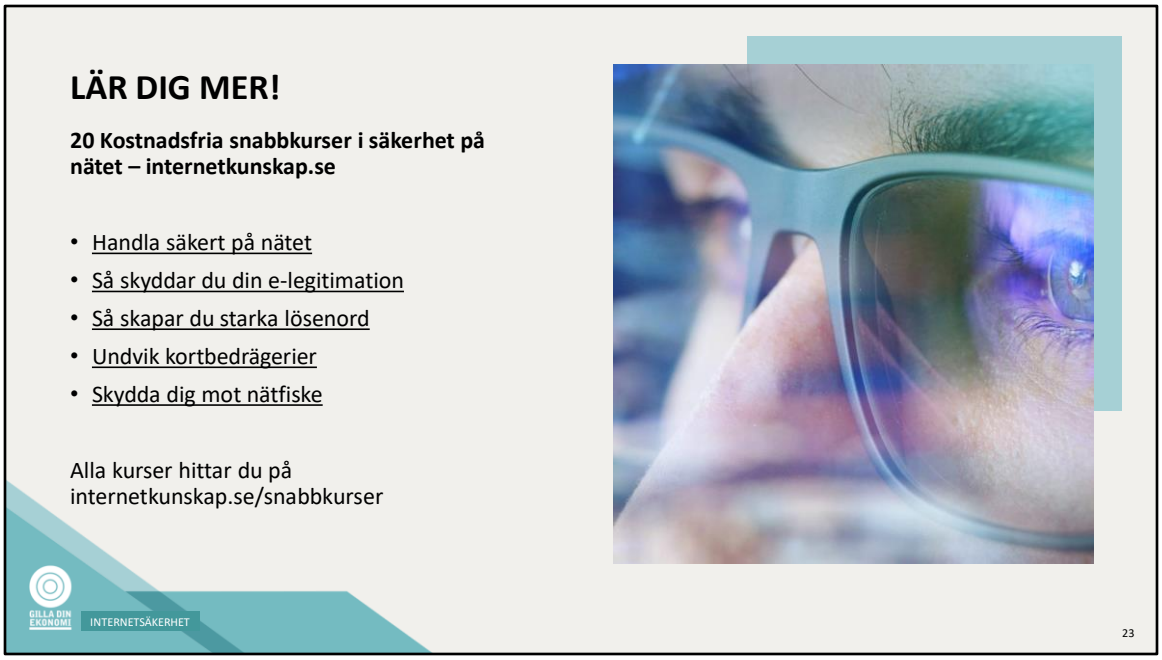
I många fall är det bara ett lösenord som skyddar din personliga information och din digitala identitet från obehöriga.
Därför är det viktigt att använda starka lösenord och att aktivera så kallad flerfaktorsautentisering på alla tjänster och konton som erbjuder det.

Ett starkt lösenord ska vara:

- **Långt** – minst 12 tecken, gärna längre
- **Ovanligt** – det ska inte gå att gissa sig till
- **Opersonligt** – det ska inte gå att koppla till dig som person
- **Unikt** – det innebär att du ska ha olika lösenord för varje tjänst.

Det är extra viktigt att skydda din e-post och dina sociala medier ordentligt.

(fördjupning)
För att komma ihåg dina lösenord kan du använda en lösenordshanterare, eller skriva ner dem på en lapp som du förvarar på ett säkert ställe.



Så det var 7 grundläggande tips.

Vill man få mer kontext och fördjupning rekommenderar jag våra kostnadsfria snabbkurser i säkerhet på nätet.

Det finns 20 stycken och på den här sliden har jag har lyft fram fem av dem lite extra på den här sliden.

En kurs tar mellan 3-5 minuter att göra och de får spridas fritt så länge det inte gör i kommersiella syften.

Länkar:

Handla säkert på nätet
https://internetkunskap.se/snabbkurser/handla-pa-natet/handla-sakert-pa-natet/

Så skyddar du din e-legitimation
https://internetkunskap.se/snabbkurser/losenord-och-e-legitimation/sa-skyddar-du-din-e-legitimation/

Så skapar du starka lösenord
https://internetkunskap.se/snabbkurser/losenord-och-e-legitimation/sa-skapar-du-starka-losenord/

Undvik kortbedrägerier
https://internetkunskap.se/snabbkurser/mejl-sms-och-telefonbedragerier/undvik-kortbedragerier/

Skydda dig mot nätfiske
https://internetkunskap.se/snabbkurser/mejl-sms-och-telefonbedragerier/skydda-dig-mot-natfiske/

HJÄLP OSS ATT SPRIDA KUNSKAP OM SÄKERHET PÅ NÄTET

- Beställ vår broschyr och sprid i ditt nätverk.
- Broschyren innehåller information om hur de vanligaste bedrägerierna går till och hur du kan skydda dig.
- Broschyren är kostnadsfri och finns på svenska, engelska och arabiska.
- Du beställer genom att skicka ett mejl till info@internetstiftelsen.se där du fyller i hur många exemplar du vill ha, på vilket språk och var de ska skickas.

GILLA DIN EKONOMI
INTERNETSÄKERHET

24

Avslutningsvis vill jag också pusha för en broschyr som vi tagit fram och som man som organisation gärna får hjälpa till att sprida till sina målgrupper.

Broschyren togs fram under Tänk säkert-kampanjen 2022 och har godkänts av både MSB och Polisen.

I dagsläget har vi skickat ut över 100.000 broschyrer till bibliotek, Polisen, Försvarsmakten, pensionärsorganisationer och digidelcenter.

https://internetstiftelsen.se/tanksakert/

Tack!

Kontakt:
Björn Appelgren
bjorn.appelgren@internetstiftelsen.se

GILLA DIN EKONOMI