SÄKERHET

Oktober - 2024

AGENDA

- Säker hårdvara – gör din enhet så säker som möjligt
  - iPhone och Android
  - Dator (Windows och Mac)
- Säkra betalningar
- Bluffmejl och SMS - bedrägeriförsök

Mobiltelefoner har blivit våra primära enheter

Mobiltrafik vs. Datortrafik: 55 % av världens onlinebesök kommer från mobiler, 43 % från datorer och
2 % från surfplattor.

Många förlitar sig helt på sina mobiltelefoner för kommunikation, shopping och till och med arbete. Ju mer vi använder dessa enheter, desto mer data och personlig information lagras på dem.

Mobiltelefoner har blivit våra primära enheter

Smartphones utvecklas snabbt och börjar kunna konkurrera med enklare datorer i prestanda.
Vi ser också en trend mot att mobiltelefoner kan anslutas till större skärmar och tangentbord för att utföra fler arbetsrelaterade uppgifter.

Banköverföringar: Eftersom fler använder sina mobiler för att göra och betala med appar som Swish eller Apple Pay, Google Pay, har hackare blivit mer intresserade av att utnyttja dessa betalningssystem.

Behövs antivirus-app/program?

Android telefon/surfplatta

Det är inte alltid nödvändigt att installera ett antivirusprogram på en Android-telefon, men det kan vara en bra idé beroende på hur du använder enheten. Här är några faktorer att överväga:

Om du installerar appar endast från Google Play, är försiktig med att klicka på länkar och meddelanden, är ett traditionellt antivirusprogram oftast överflödigt på en Android, men det kan ge extra trygghet om du är osäker.

Behövs antivirus-app/program?

iOS (iPhone/iPad)

Det är vanligtvis inte nödvändigt att installera ett antivirusprogram på en iPhone.

Apples iOS har en stark säkerhetsarkitektur och begränsar hur appar kan interagera med systemet, vilket minskar risken för virus och skadlig programvara. Här är några punkter att tänka på:

Om du installerar appar endast från AppStore, är försiktig med att klicka på länkar och meddelanden, är ett traditionellt antivirusprogram oftast överflödigt på en iPhone.

Behövs antivirus-app/program?

PC / Windows

Ja, på en PC med Windows rekommenderas det starkt att ha ett antivirusprogram. Windows är mer utsatt för virus och skadlig programvara jämfört med andra operativsystem, främst på grund av dess popularitet och de breda användningsområdena.

Windows 10 och 11 har ett inbyggt skydd. Normalt sett behövs inget separat antivirusprogram.

Om du ofta laddar ner filer från osäkra källor, besöker tveksamma webbplatser eller arbetar med känslig information, kan ett separat antivirusprogram ge extra trygghet.

Behövs antivirus-app/program?

Apple / MAC

Generellt sett anses Mac-datorer vara säkrare än många andra plattformar, delvis på grund av deras Unix-baserade arkitektur och Apples säkerhetsåtgärder. Men det betyder inte att de är helt immun mot virus och skadlig programvara.

För de flesta användare räcker det med sunt förnuft och att följa säkerhetsriktlinjer. Men om du vill ha extra skydd, kan ett antivirusprogram vara en bra idé.

<u>Gäller ALLLA typer av utrustning!</u>

Generellt råd är att

<u>ALLTID</u>

hålla system och appar/program

<u>uppdaterade</u>!

Att INTE ha ett lås på din mobiltelefon,
är som att inte ha lås till din dörr!

Var surfar jag säkrast?

- Wifi-hemma
  - Hög säkerhet om det är inställt rätt. Krypterat.
- Wifi - offentligt (café, hotell, etc.)
  - Låg säkerhet. Okrypterat.
- Mobilnätverk via masterna
  - Hög säkerhet. Krypterat.

Google Play Butik och Apple App Store

Att ladda ner appar från Google Play Butik och Apple App Store är i allmänhet säkert, men det finns vissa faktorer att tänka på för att minimera risker:

Google Play Butik

Google Play har vissa skyddsmekanismer, men eftersom det är mer öppet för utvecklare än App Store, kan det förekomma appar med skadlig kod eller oönskade funktioner.

Apple App Store

Apple App Store är i regel säkrare eftersom Apple granskar alla appar innan de publiceras. De har en striktare godkännandeprocess, vilket minskar risken för skadlig kod. Men det finns fortfarande appar som kan samla in personlig information eller använda tveksamma metoder.

Fysiskt skydd för din telefon/platta!

1. Skärmskydd
    - **Typ:** Härdat glas eller plastfilm.
    - **Funktion:** Skyddar skärmen mot repor, sprickor och smuts. Härdat glas är mer hållbart och ger ett extra lager av skydd mot stötar och fall, medan plastfilm mest skyddar mot repor.
2. Mobilskal
    - **Typ:** Skal av silikon, hårdplast, gummi, eller läder.
    - **Funktion:** Skyddar telefonens baksida och sidor mot slag, fall och repor. Vissa skal har extra stötdämpning för bättre skydd vid fall från höjd.

- **Tips:** Välj ett skal som täcker hörnen och har upphöjda kanter runt skärmen för att skydda telefonen vid fall med framsidan neråt.

Vad innebär s.k. säkra betalningar?

En säker betalning på nätet innebär att transaktionen skyddas genom olika metoder och protokoll för att säkerställa att både köpare och säljare är skyddade mot bedrägerier och dataintrång. Här är några centrala aspekter:

1. Kryptering: Informationen som överförs mellan din webbläsare och betalningssidan krypteras, vilket gör det svårt för obehöriga att avlyssna.

2. Säkerhetsprotokoll: Användning av HTTPS (Hypertext Transfer Protocol Secure) som säkerställer att kommunikationen är säker.

Vad innebär s.k. säkra betalningar?

3. Betalningsmetoder: Användning av pålitliga betalningstjänster som PayPal, Klarna eller kreditkort med extra säkerhetsfunktioner (t.ex. 3D Secure) ger ytterligare skydd (gäller betalningar på nätet). Du kan dessutom betala med din mobil eller smartklocka.

4. Autentisering: Många tjänster kräver extra verifiering, som en engångskod skickad till din telefon, för att bekräfta att du är den som genomför köpet.

5. Återbetalningsskydd: Många plattformar erbjuder skydd för köpare, vilket gör att du kan få tillbaka pengar om något går fel, som om varan inte levereras eller inte stämmer överens med beskrivningen.

Tycker du att integritet är viktig på nätet?
Vill du inte ha annonser som baseras på vilka sidor du har besökt?
BYT I SÅ FALL SÖKMOTOR!
(görs i din webbläsare under Inställningar)

Google och DuckDuckGo är två sökmotorer, men de har olika fokus och funktioner:

1. **Integritet**:
    1. **Google**: Samlar in och lagrar användardata för att ”förbättra” sina tjänster och för att visa personligt anpassade annonser.
    2. **DuckDuckGo**: Samlar inte in någon personlig information och spårar inte användare, vilket ger en högre grad av integritet.

Kom till vår handledning så hjälper vi dig!

Faktura väljs för att det upplevs som säkrast

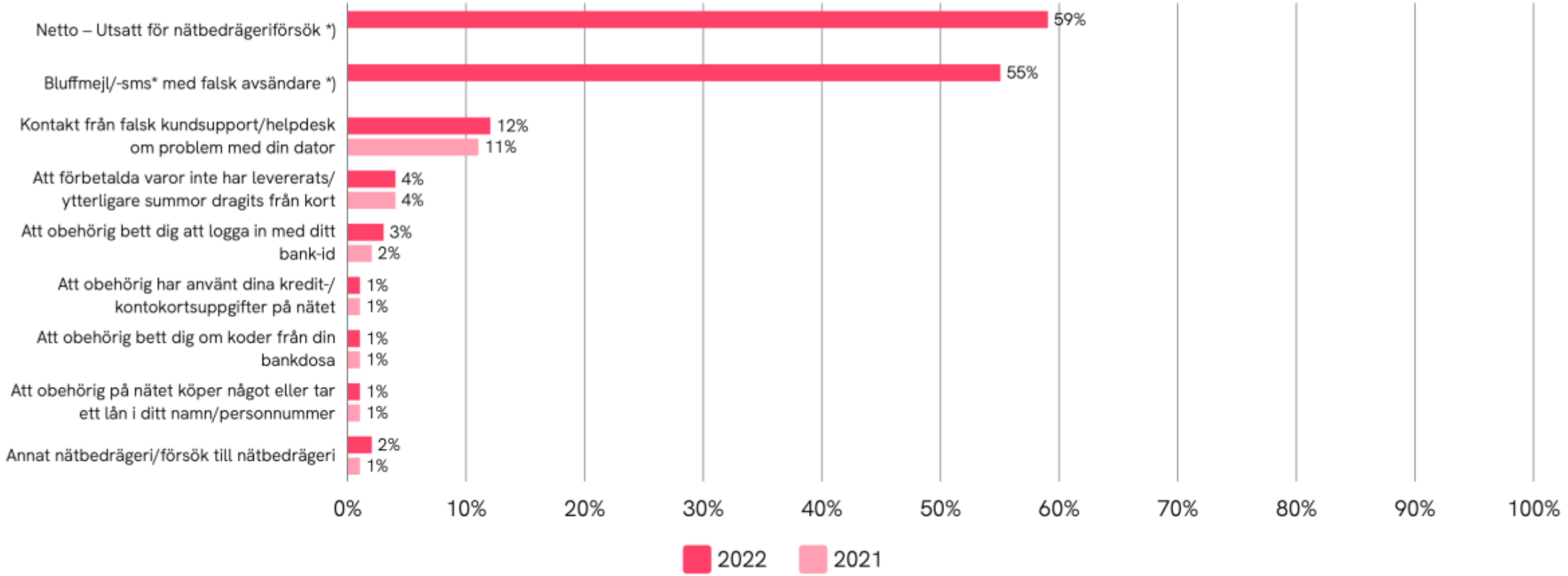
Faktura föredras framförallt för att det upplevs som säkert,
förmodligen eftersom man inte behöver lämna ifrån sig sina kontouppgifter
vid köptillfället och kan få hem varan innan betalning.

Det betydligt fler äldre än yngre som föredrar att betala med faktura på nätet.

Tid för en bensträckare?

Bluffmejl och sms – vanligaste bedrägeriförsöket

Fråga: Har du någon gång under de senaste 12 månaderna blivit utsatt för något av följande bedrägerier/bedrägeriförsök på internet?



INTERNETSTIFTELSEN

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

INTERNETSTIFTELSEN

SÅ HÄR LURAR BEDRAGARNA DIG

- Bedragarnas kontaktar dig, till exempel via mejl, sms, sociala medier, telefonsamtal och falska annonser.
- Bedragarna utger sig ofta för att företräda en bank, en myndighet eller ett välkänt företag.
- Bedragarnas ärenden varierar och anpassas ofta efter vad som sker i omvärlden.
- I mejl och meddelanden uppmanas du nästan alltid att klicka på en länk eller att öppna en bifogad fil.
- När bedragarna ringer är det vanligt att bedragarna ber dig dela koder från din bankdosa, använda din e-legitimation eller ladda hem ett program från nätet.
- För att du ska följa uppmaningarna försöker bedragarna stressa dig och de spelar ofta på dina känslor genom att göra dig nyfiken, glad eller orolig.

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.

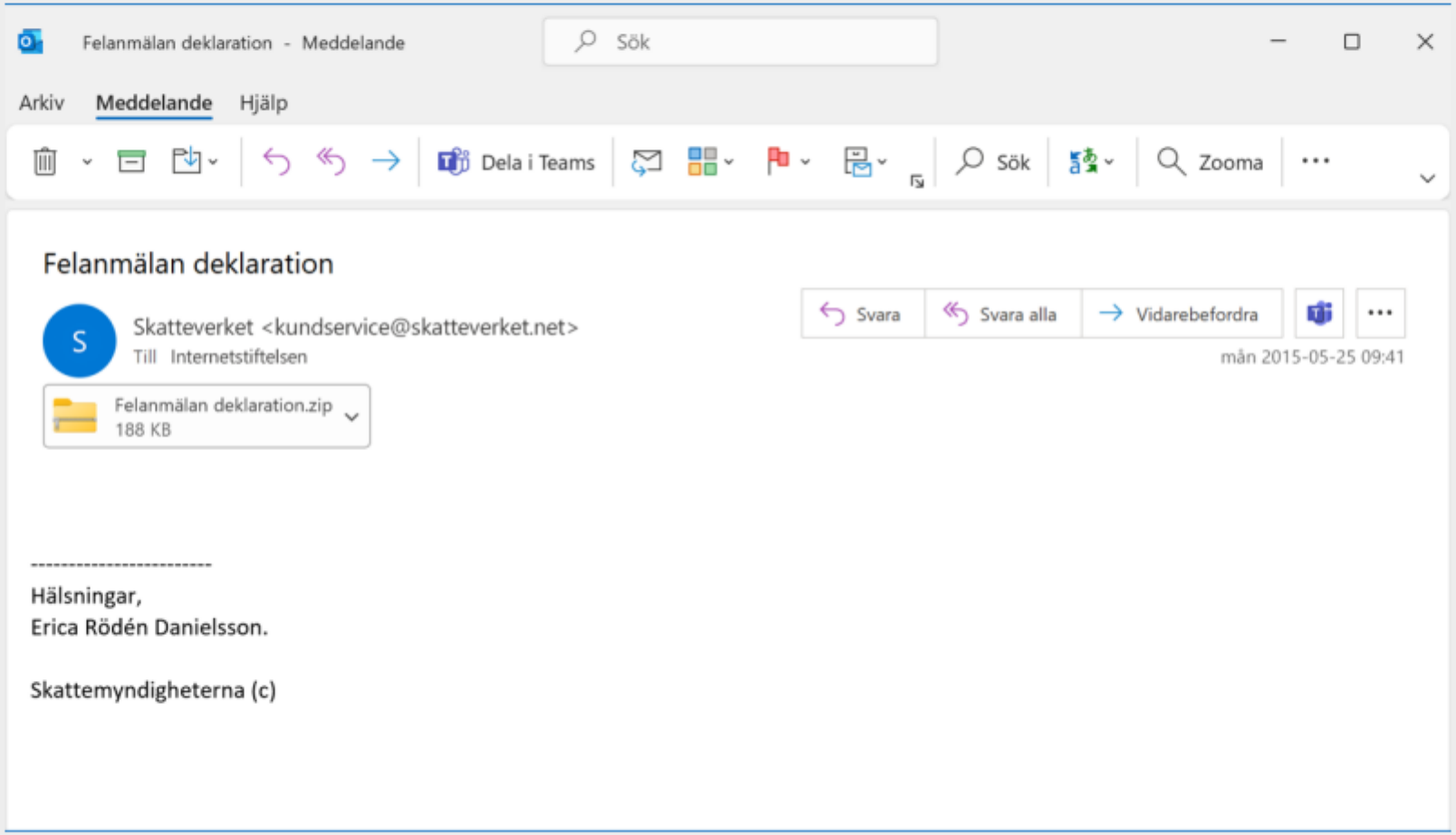
Det kan till exempel vara en falsk webbshop, en falsk kopia av en myndighetssida eller en falsk inloggningssida till en streamingtjänst.

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

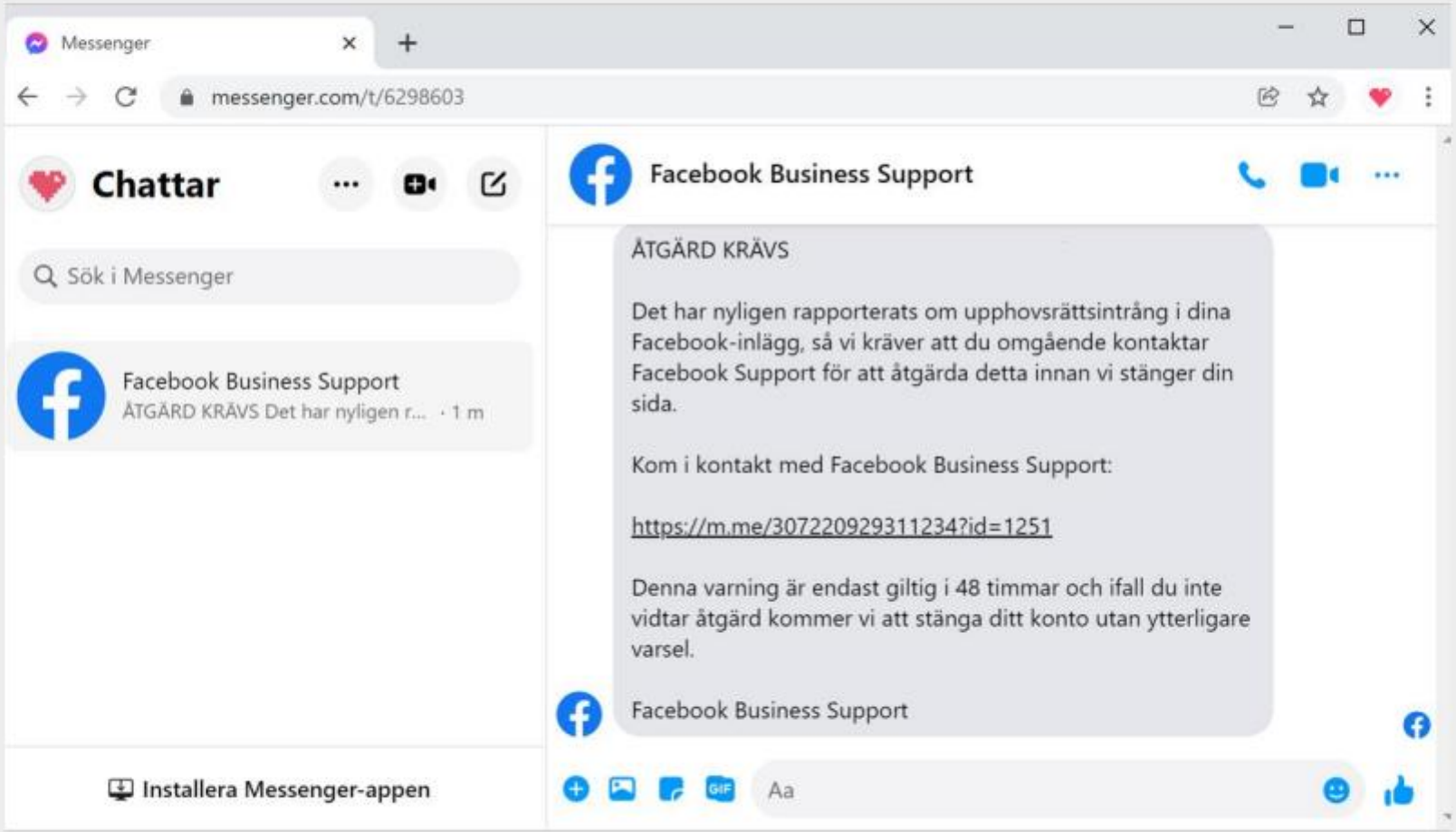
INTERNETSTIFTELSEN

EXEMPEL 1: SÅ HÄR LURAR BEDRAGARNA DIG

EXEMPEL 2: SÅ HÄR LURAR BEDRAGARNA DIG

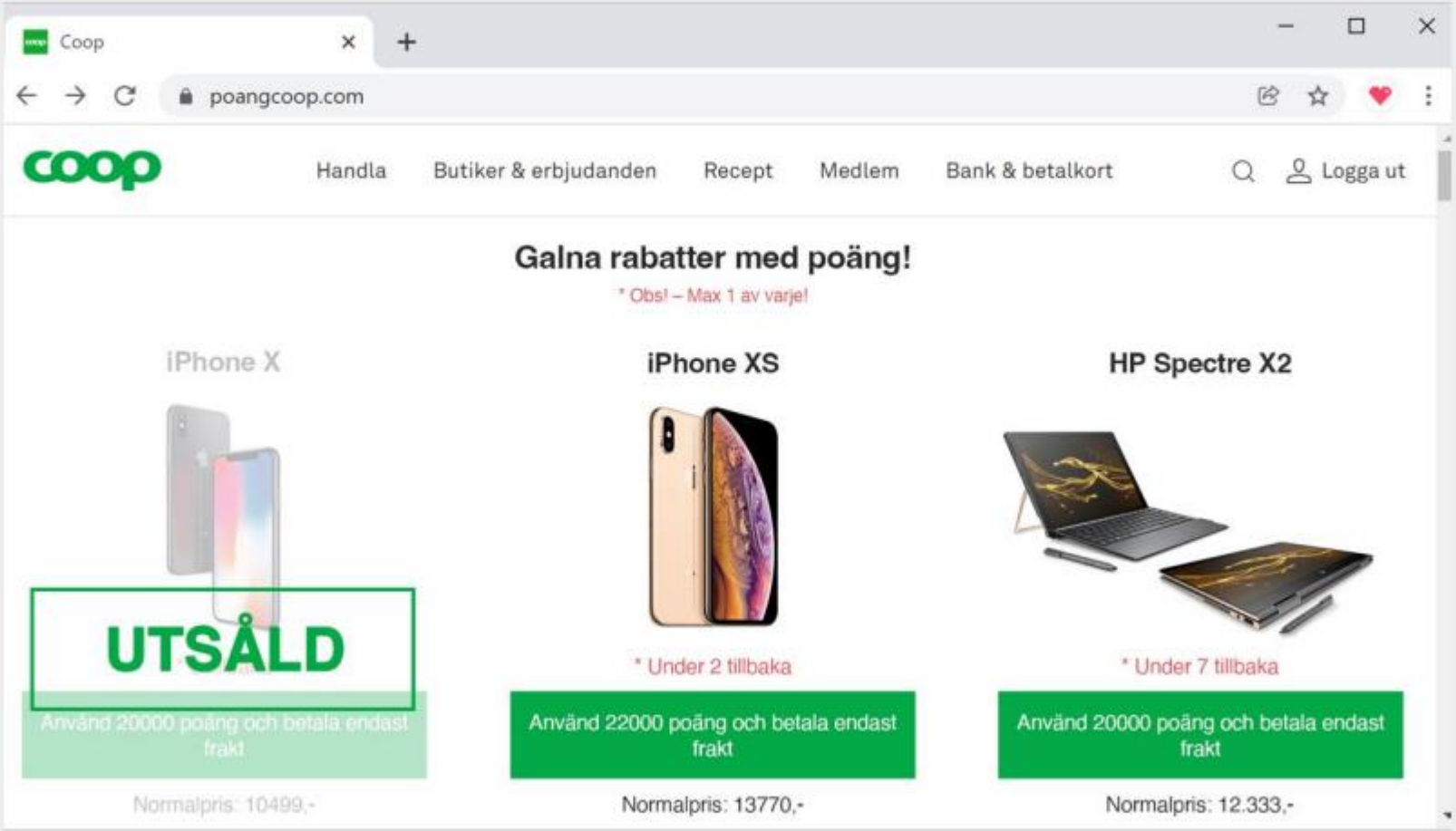


EXEMPEL 3: SÅ HÄR LURAR BEDRAGARNA DIG



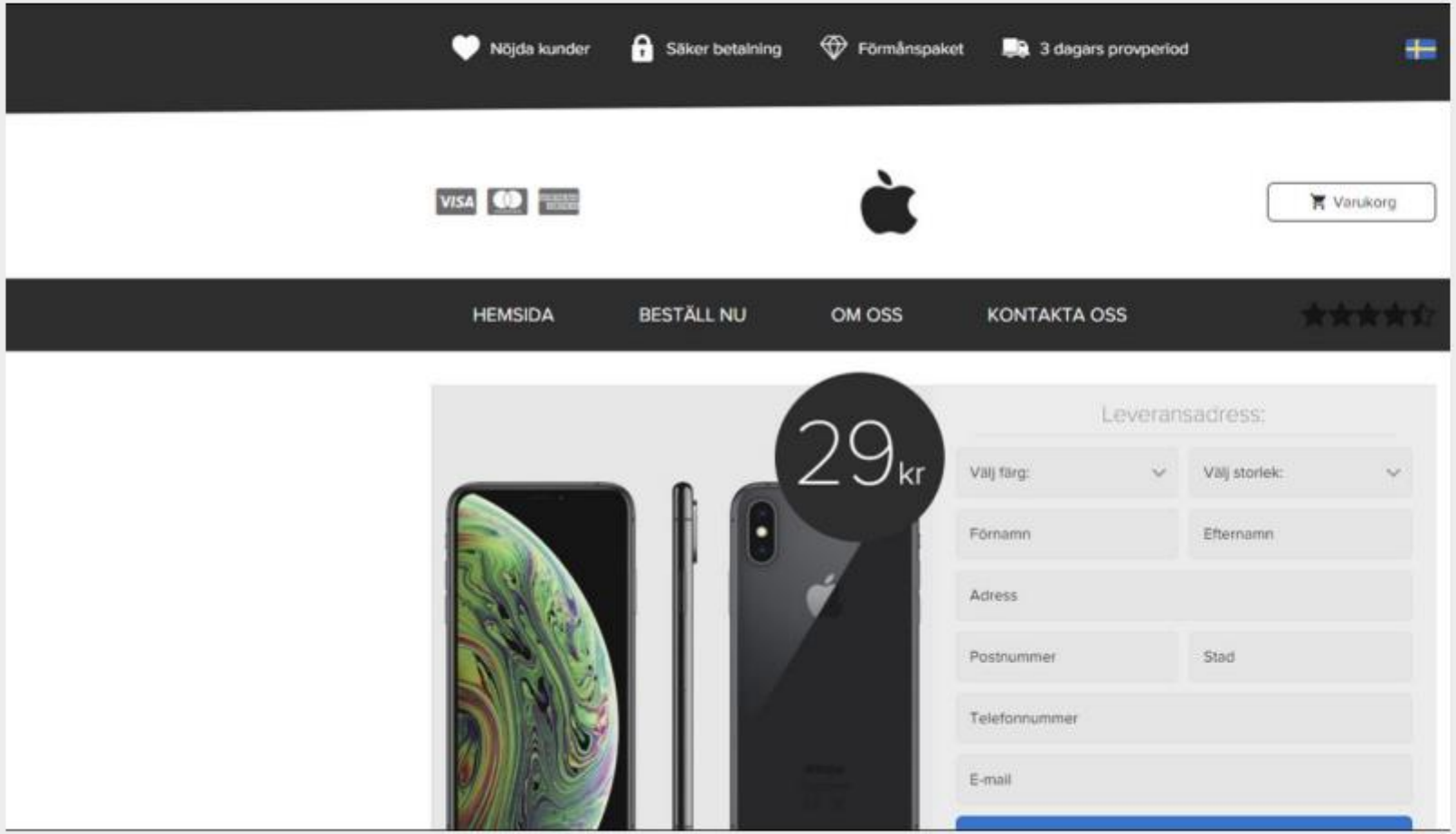
Exempel 1

TIPS 1: UNDVIK ATT KLICKA PÅ LÄNKAR



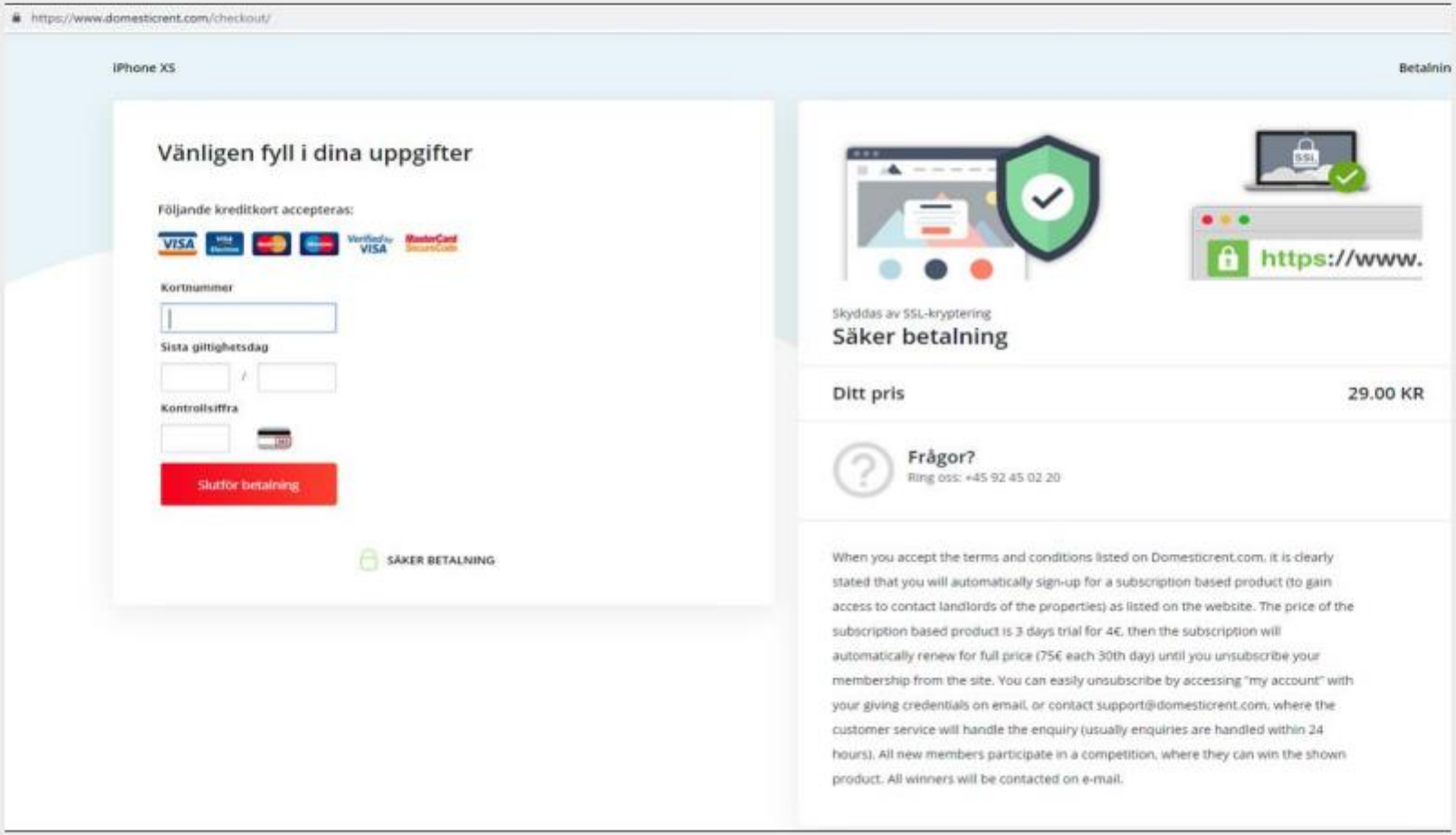
Exempel 1

TIPS 1: UNDVIK ATT KLICKA PÅ LÄNKAR



Exempel 1

TIPS 1: UNDVIK ATT KLICKA PÅ LÄNKAR



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.

TIPS 3

Lägg på luren, våga vara bestämd!

Det här gäller om någon som ringer dig:

- Efterfrågar dina kortuppgifter eller lösenord
- 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

INTERNETSTIFTELSEN

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.

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.

EXEMPEL: SPOOFING

Konversationstråd

Bluff-sms

Gittes svar

Äkta autosvar

INTERNETSTIFTELSEN

20 kostnadsfria snabbkurser i säkerhet på nätet

Ett urval:

- Handla säkert på nätet
- Så skyddar du din e-legitimation
- Så skapar du starka lösenord
- Undvik kortbedrägerier
- Skydda dig mot nätfiske

Alla kurser hittar du på
internetkunskap.se/snabbkurser

INTERNETSTIFTELSEN

Frågor?

Tack för att ni lyssnade!

Applåder, tack!