BLI SÄKER PÅ NÄTET

MARGARETHA ERIKSSON, CIVILINGENJÖR KTH,
INFORMATIONSSÄKERHETSSPECIALIST

HÄRNÖSANDS PENSIONÄRSUNIVERSITET (HPU)
SAM-BIBLIOTEKET 29/4 2025

HUR BLI SÄKER PÅ NÄTET?

- Varför det här superviktigt!
- Varför blir vi lurade?
- Hur blir vi lurade?
- Bedrägerier och lurendrejeri
- Bli svårlurad!
- Bonus – roa dig!

BEDRÄGERIER OCH LURENDREJERIER

- Vi är målgruppen – pensionärer
- Kvinnor över 80 år extra ansatta!
- 2023
  - 29 347 anmälda vishingbrott (via telefon)
  - Brottsvinster 708 miljoner
  - Mörkertal?

Uppdrag Granskning på SVT 7/2 2024

- Uppdrag-granskning/bedragarna

Plånboken i P1 7/2 2024

- manga-luras-av-nya-fejkbutikerna

BRÅDSKANDE: Uppdatera betalningsinformation för gunnesfelag.nu External Spam ×

Loopia <contact4b3b7aef@jdg.cat>
to kontakt

Feb 21, 2024, 10:37 AM (1 day ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

Translate to English

God morgon Gunnesfelag,

Det är absolut nödvändigt att du uppdaterar betalningsinformationen för ditt domännamn gunnesfelag.nu omedelbart. Vårt försök att förnya misslyckades på grund av detta och för att undvika permanent avstängning av din domän måste du genast.

För att hålla dina tjänster aktiva, klicka på länken här nedan för att uppdatera dina betalningsuppgifter utan dröjsmål:

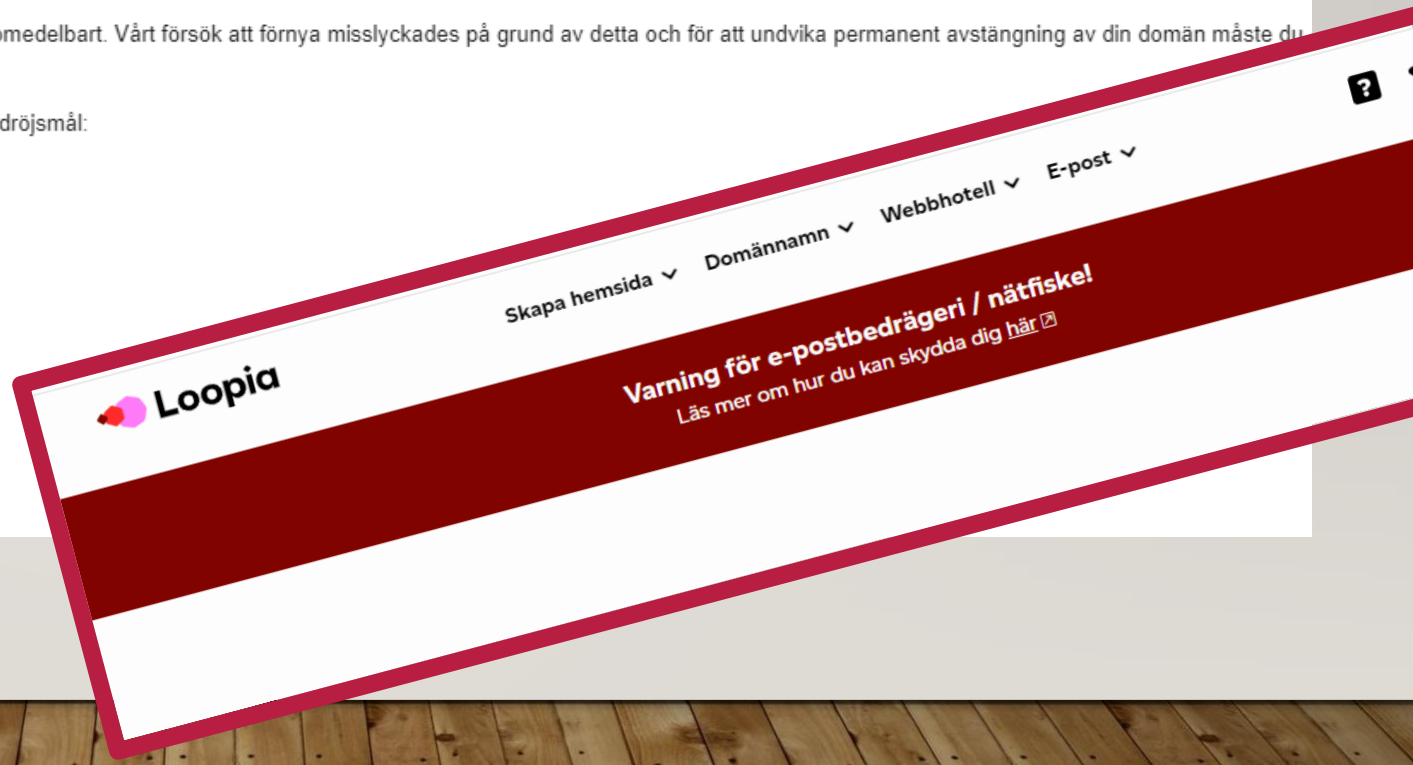
Klicka här för att förnya din domän.

Tack så mycket för din snabba åtgärd.

Tack,

Loopia

Reply Reply all Forward



BEDRAGARE KAN PÅSTÅ ATT

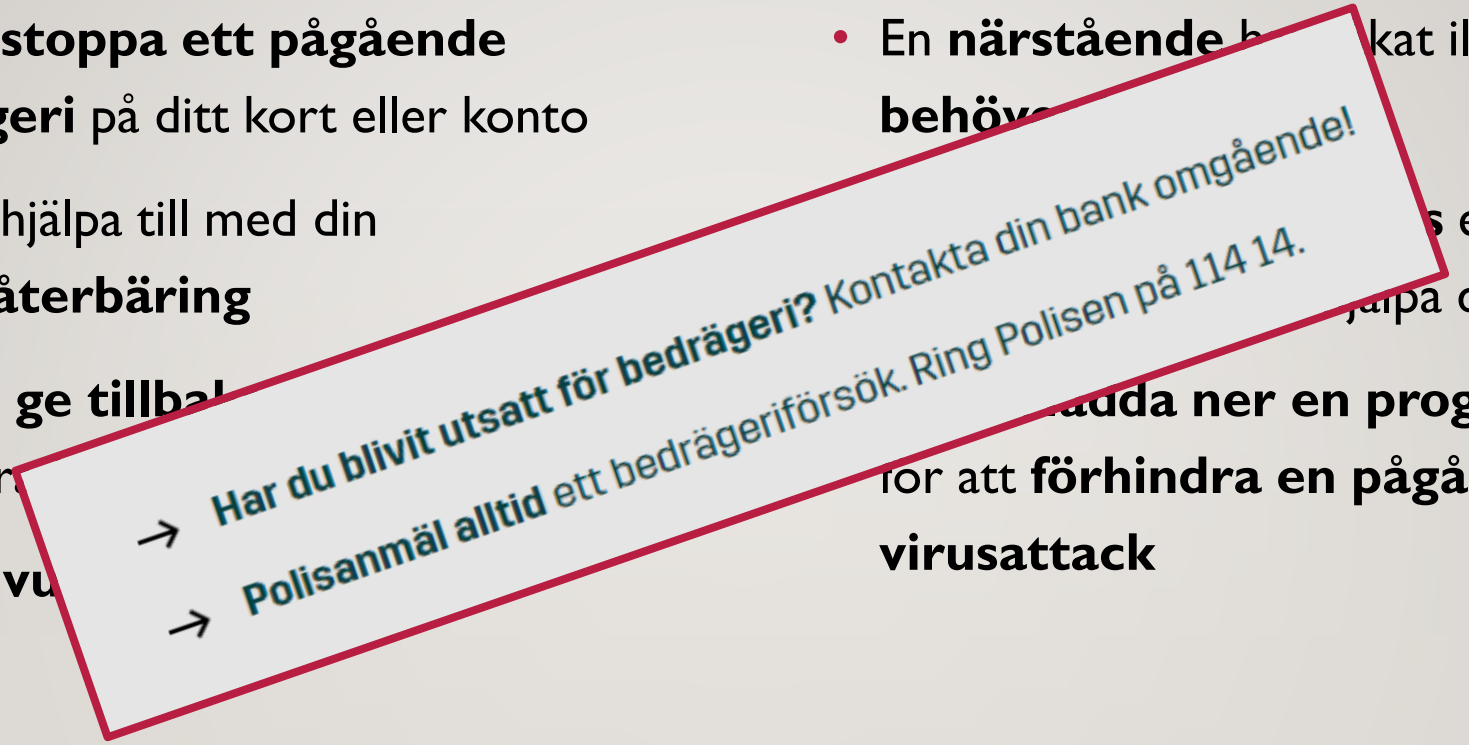
- De ska **stoppa ett pågående bedrägeri** på ditt kort eller konto
- De ska hjälpa till med din **skatteåterbäring**
- De ska **ge tillbaka pengar** som du har blivit lurad på
- Du har **vunnit pengar**

BEDRAGARE KAN PÅSTÅ ATT

- De ska **stoppa ett pågående bedrägeri** på ditt kort eller konto
- De ska hjälpa till med din **skatteåterbäring**
- De ska **ge tillbaka pengar** som du har blivit lurad på
- Du har **vunnit pengar**
- En **närstående** har råkat illa ut och **behöver hjälp**
- Din **dator har fått virus** eller andra problem och de ska hjälpa dig tillrätta
- Du ska **ladda ner en programvara** eller **app** via **länk** för att **förhindra en pågående virusattack**

BEDRAGARE KAN PÅSTÅ ATT

- De ska **stoppa ett pågående bedrägeri** på ditt kort eller konto
- De ska hjälpa till med din **skatteåterbäring**
- De ska **ge tillba**
  blivit lur
- Du har **vu**
- En **närstående h** kat illa ut och **behöv**
  s eller andra
  jälpa dig tillrätta
  adda ner en programvara
  för att **förhindra en pågående virusattack**



Varning för bedragare – var försiktig med ditt BankID

För närvarande ser vi en markant ökning av bedragare som ger sken av att företräda Svea Bank, Svea Inkasso eller
verksamhet.

- Starta och använd aldrig BankID på uppmaning av någon som kontaktat dig
- Avsluta samtalet och ring upp oss – tänk på att inte använda telefonens återuppringningsfunktion
- Klicka aldrig på länkar i mejl eller sms om du inte är helt säker på avsändaren
- Polisanmäl alltid om du misstänker att du blivit utsatt för ett bedrägeriförsök

Varning för bedrägeriförsök

Branschföreningen Svensk Inkasso vill varna allmänheten för ett pågående bedrägeriförsök där meddelanden per SMS och e-post skickas ut i inkassobolags namn.

Meddelandena uppmanar mottagaren att ringa ett angivet nummer eller att besöka en hemsida som verkar tillhöra inkassobolaget, och i vissa fall att swisha in pengar för en påstådd skuld. Numret i meddelandet går inte till inkassobolaget i fråga och hemsidesadressen leder till en kopia av inkassobolagets egen webbplats. Det har också förekommit att privatpersoner i kontakterna blivit uppmanade att ladda ner olika typer av appar.

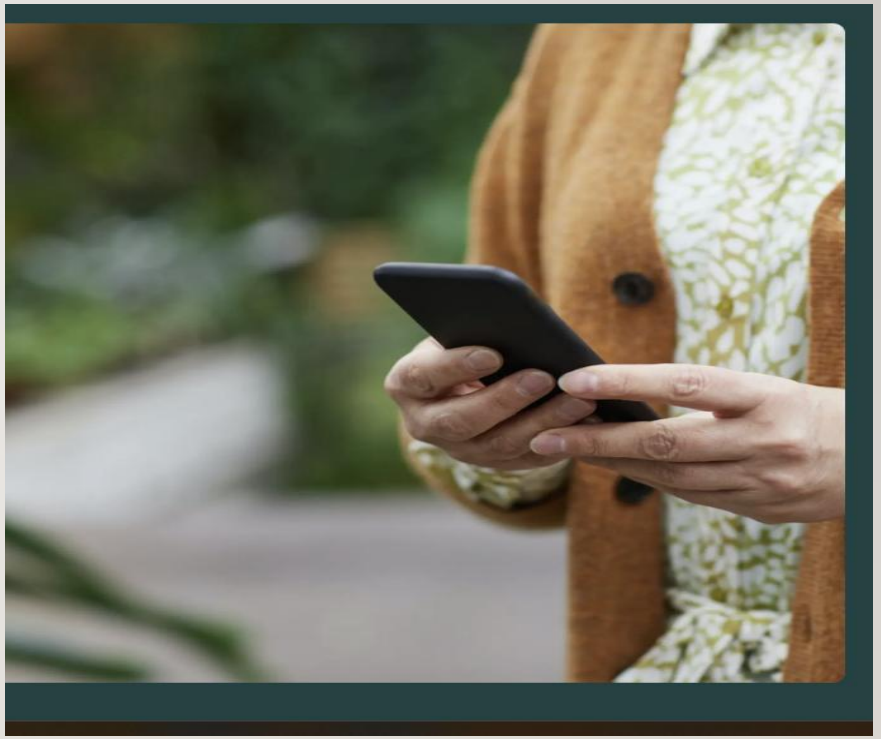
Såvitt Svensk Inkasso erfar har bedragarna hittills utgivit sig för att representera Alektum Group, Gothia Inkasso, Intrum, Sergel, Svea Inkasso och Visma.

Vi uppmanar den som tar emot sådana meddelanden att följa nedanstående råd för att undvika att bli drabbad av detta bedrägeriförsök:

1. **Kontrollera inkassobolagets officiella kontaktuppgifter.** I stället för att ringa det angivna numret, bör du besöka inkassobolagets officiella hemsida och kontrollera bolagets kontaktinformation där. Dubbelkolla att det nummer som anges i meddelandet stämmer överens med det officiella numret innan du ringer upp.
2. **Swisha inte pengar utan att kontrollera mottagaren**. Bedragarna kan be att du swishar in pengar för att lösa den påstådda skulden. Gör inte det innan du har verifierat att det verkligen rör sig om ett korrekt inkassokrav och att pengarna faktiskt överförs till inkassobolaget.
3. **Använd inkassobolagets online-tjänster och ladda inte ner appar**. De flesta inkassobolag har "mina sidor" där du kan logga in och hantera dina ärenden. Använd dessa säkra online-tjänster för att kommunicera med inkassobolaget i stället för att ringa upp numret i meddelandet. Ladda inte ner några appar till din telefon – inkassobolagen använder inte

TELEFONBEDRÄGERIER – SÅ GÅR DET TILL

- Uppringaren utger sig för att ringa från banken, polisen, ett företag, en myndighet eller påstår sig vara din närstående.
- Bedragaren stressar dig, något måste åtgärdas omedelbart. Det är BRÅTTOM.
- Telefonnumret kan vara manipulerat så att det ser ut som från banken.
- Bedragaren vill hjälpa dig att lösa det (påhittade) problemet eller rätta till situationen.
- Bedragaren ber dig använda ditt bank-id eller skriva under en Swish-betalning.
- Lita inte på uppringare bara för att de har dina personuppgifter. Bedragare är skickliga på att samla personlig information som används för att skapa förtroende och luras.



- **Lägg på och ring din bank eller någon närstående som du litar på vid minsta osäkerhet.**

SMS-BEDRÄGERIER – SÅ GÅR DET TILL

- Bedragare skickar SMS för att komma över information som används för att begå brott.
- Bedragare manipulerar telefonnumret så att det ser ut som att det är banken, polisen, en myndighet eller en närstående som är avsändare.
- Meddelandet uppmanar dig att hämta ut en vinst, få ett erbjudande eller betala en fraktavgift för ett paket.
- Du ger bedragaren tillgång till privata uppgifter eller betalar för något som du inte har köpt.
- Bluff-sms är inte farliga i sig, så länge som du inte agerar på det som bedragaren uppmanar dig att göra.

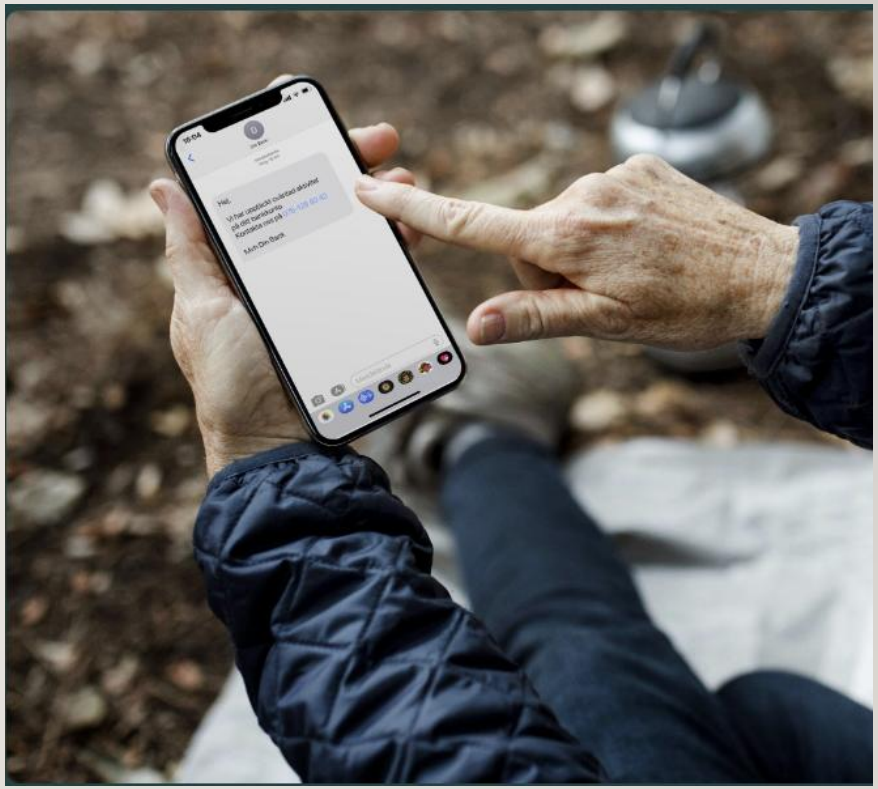
Klicka inte på länkar i sms

Ring inte okända telefonnummer

på någon annans uppmaning.

Prata med någon du litar på om du är osäker.

Kontakta först din bank och sedan polisen om du misstänker brott.



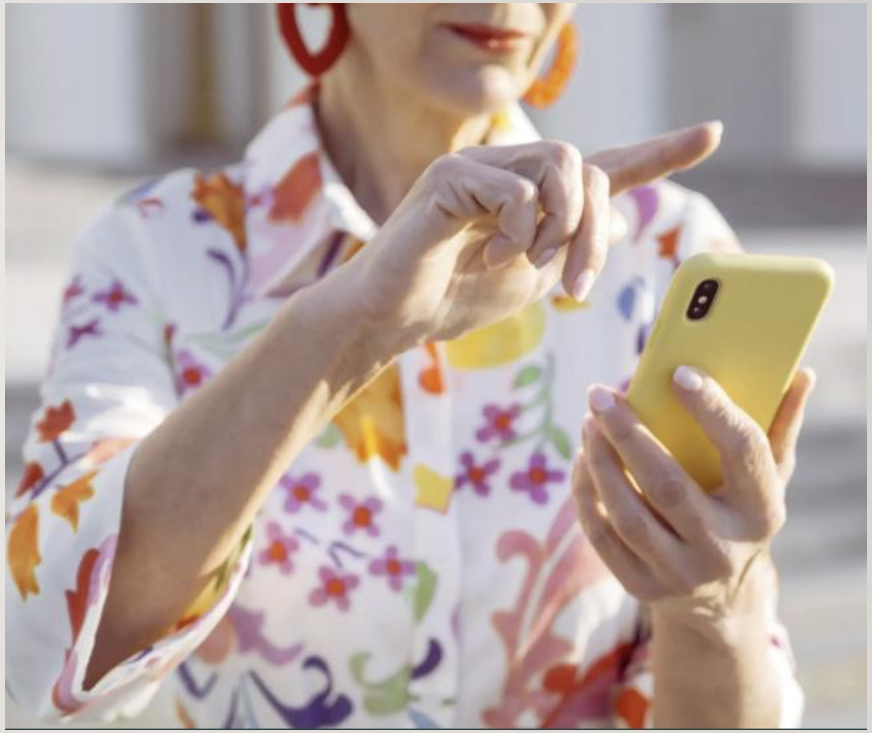
E-POSTBEDRÄGERIER – SÅ GÅR DET TILL

- Du får e-post från en känd avsändare som erbjuder en tjänst via en länk till en hemsida.
- Hemsidan är en **kopia** en känd och seriös hemsida.
- Hemsidan ber dig om personlig information, t ex **uppdatera Bank-ID** för att få tillgång till skatteåterbäring, uppdatera **kontouppgifter** på ett abonnemang eller **personlig information** för att hämta ut paket.
- ”Tjänsten” syftar till att komma åt dina pengar på något sätt.
- Var misstänksam mot erbjudanden och uppmaningar – seriösa aktörer ber inte om personlig information via e-post.

- **Öppna inte e-post eller bifogade filer som du inte förväntat dig att få.**
- **Lämna aldrig ut personlig information, koder eller lösenord i e-post eller på osäkra hemsidor.**

ROMANSBEDRÄGERIER – SÅ GÅR DET TILL

- Bedragaren **söker kontakt**, ofta slumpartat, via en dejtingsida, Facebook eller någon annan **social media**. Eller möte i verkliga livet.
- Bedragaren spelar på dina **känslor** och tillit. Du känner dig uppskattad, omtyckt och **förälskad**. Det blir intensiv kontakt via sms, i chattar och telefonsamtal.
- Bedragaren lovar **guld och gröna skogar** för att så småningom be om tjänster och pengar.
  Väldigt mycket pengar.
- Bedragaren använder **falsk identitet**, stulna foton och påhittade historier för att luras.
- **Ett romansbedrägeri då du blir lurad på både pengar och kärlek kan sätta djupa spår.**
- **Ta hjälp av din omgivning och lyssna till dina närstående.**
- **Kontakta polisen om du misstänker brott.**



HAR DU BLIVIT LURAD?

KÄNNER DU SKAM?

- Normalt, men det ska DU inte göra

Bedragarna ska skämmas!

- Spelar på din tilltro, skräms och hotar, stressar dig till snabba beslut

FÖRSVARA DIG I STÄLLET!

- Anmäl till Polisen!
- Statistik ger polisen ökade resurser
- Anmälningar kan läggas ned, men data samlas in till Interpol

ANMÄL TILL POLISEN

[Nätfiske, phishing | Polismyndigheten (polisen.se)]

RAPPORTERA BLUFF-SMS

SPAM = 7726

Rapportera misstänkta bluff-sms till 7726

Har du fått ett misstänkt bluff-sms? Vidarebefordra meddelandet till **7726**. Siffrorna motsvarar ordet SPAM på knappsatsen i telefonen och är globalt etablerat för att rapportera bluff-sms.

Det är ett operatörsoberoende nummer som alla kan använda. På så sätt får teleoperatörerna veta vilka bluff-sms du får.

IT-GRUNDSKYDDA DATOR OCH MOBIL

Skydda dator

- Välj **Hämta uppdateringar automatiskt** i Inställningar
- Microsoft Windows
  - Inbyggt virusskydd
- Apple Mac, Ipad
  - Inbyggt virusskydd
- Tvåstegsverifiering ”dubbla lås”
  - Du får en verifieringskod eller e-postmeddelande

Skydda mobiltelefon

- Välj **Hämta uppdateringar automatiskt** i Inställningar
- Öppna med biometri
  - Fingeravtryck
  - Ansiktsigenkänning
  - Pekmönster
  - Kod
- Tvåstegsverifiering ”dubbla lås”
  - Du får en verifieringskod eller e-postmeddelande

FÖRSVARA DIG!

Skydda dig

- ID-kapning
  - **Spärra** att någon obehörig kan ändra din postadress via Skatteverket/Privat/Folkbokföring och e-legitimation
- Adresskapning
  - Spärra att någon kan ändra din adress via Adressändring www.adressandring.se
  - Kostnadsfritt

Skydda dina pengar

- Undvik alltid ”väldigt bra erbjudanden”
- Konto/kreditkort
  - Skaffa separat konto/kreditkort
  - Spärra för utrikes handel
  - Spärra för handel online
    Öppna kort vid behov
- Skaffa flera e-postadresser
  - Privat/personlig e-postadress
  - ”Slask”-adress för mindre viktiga kontakter via t ex Hotmail eller Gmail

SKYDDA DINA PENGAR!

- Bankens krav på ”kundkännedom” stoppar bedrägeriförsök
- Ge **aldrig** bort pengar i god tro
  - ”Nödlån”
  - Romansbedrägerier
  - Betala inte för en vara utan att ha sett den på riktigt

Lär dig mera

- Bli svårlurad (Bankerna)
- Säkerhetskollen (SSF) https://säkerhetskollen.se

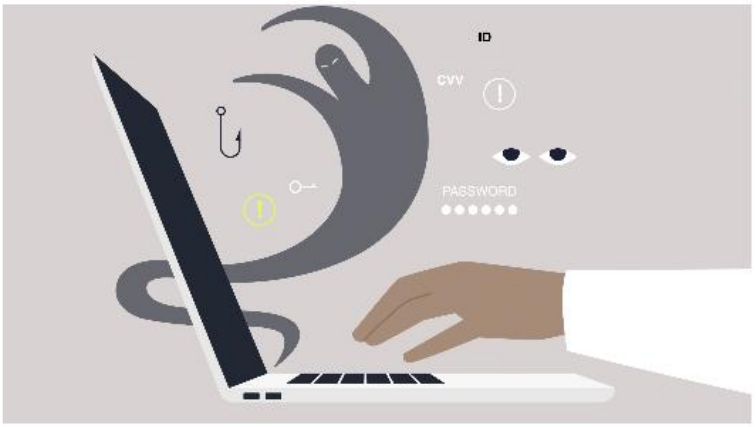
TESTA DIN SÄKERHET

5 min lästid

Bedrägeri eller ej?

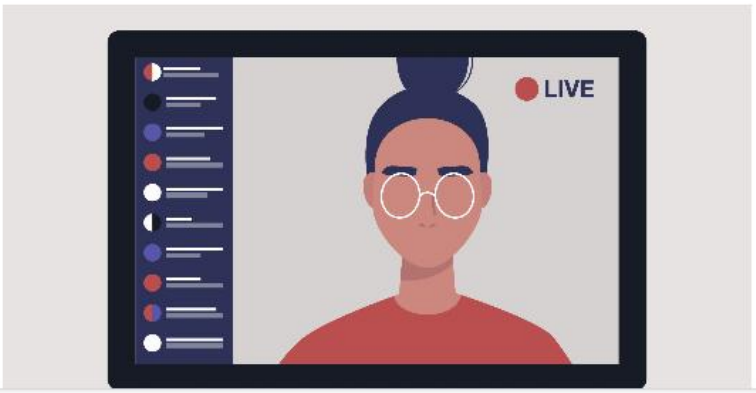
2 min lästid

Är min mejladress säker?



2 min lästid

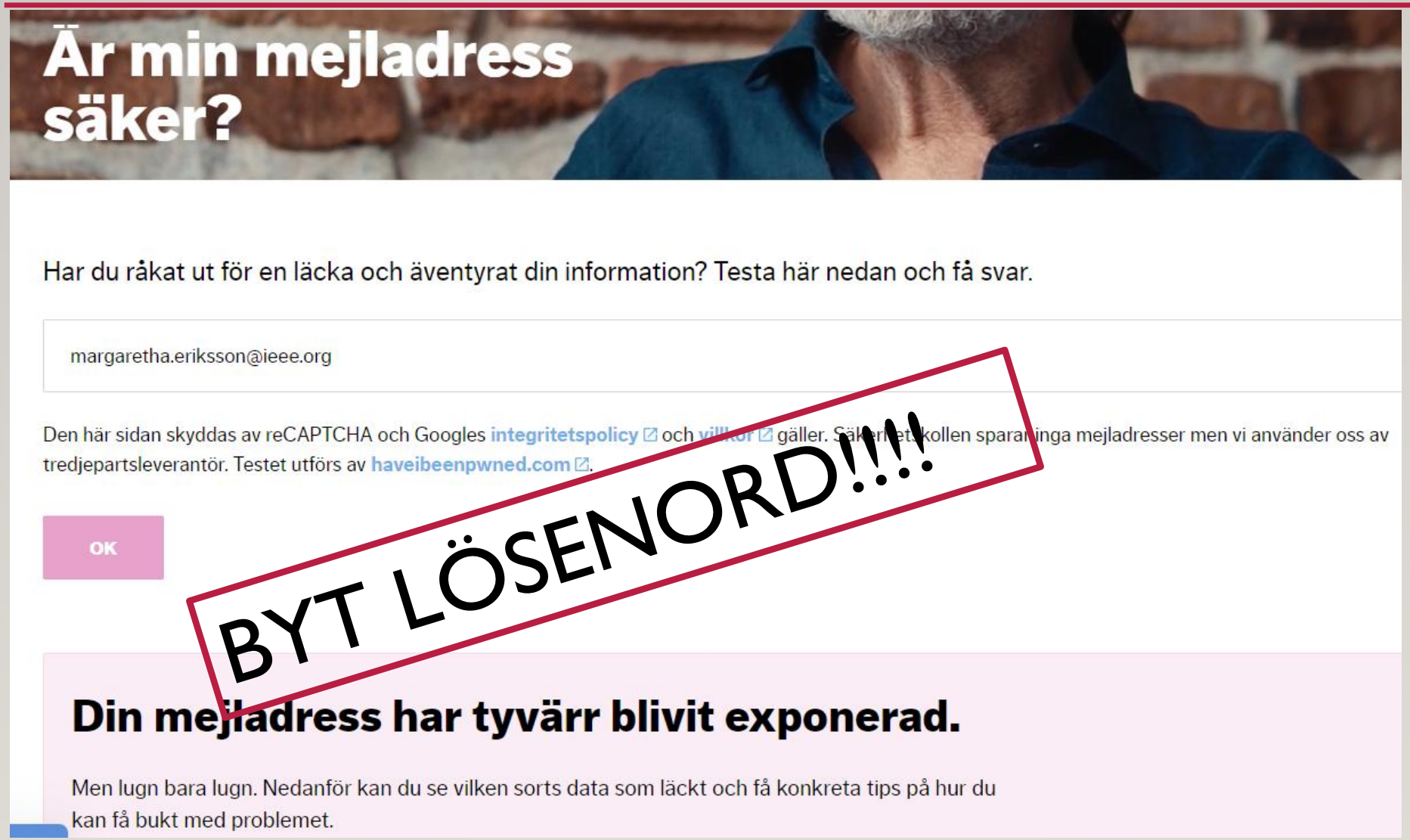
Vad är ett säkert lösenord?



Testa min säkerhet | Säkerhetskollen)

KOLLA DIN DIGITALA PROFIL MED ETT QUIZ

BEHÖVER DU BYTA LÖSENORD?



FÖR DIG SOM VILL BLI MER SÄKER

- Spärra mot ID-kapning via Skatteverket/Privat/Folkbokföring
- Spärra mot adresskapning via www.adressandring.se
- Bli svårlurad https://svarlurad.se/
- Säkerhetskollen för privatpersoner https://sakerhetskollen.se/privat
- Testa om mejladress har läckts https://haveibeenpwned.com/

- Skicka bluff-sms till **7726** (SPAM)
- Anmäl bedrägeribrott till Polisen **11414**
- Anmäl kortbedrägeri via webben Vad har hänt? - Anmälan av kortbedrägeri | Polismyndigheten

Bonus - var medvetet respektlös!

FORTSÄTT VARA SVÅRLURAD!

Margaretha Eriksson

Irbis Konsult AB

070-7747530

irbiskonsult@gmail.com

Informationen är hämtad Polisen,
Internetstiftelsen, ”Bli svårlurad” och
Stöldskyddsföreningen (Säkerhetskollen)