

Skydd mot nätbedrägerier



How to protect yourself against online scams

Hur känner du igen en nätbedragare?

How to recognize an online scammer?

Du får tomma löften

- Din varningsklocka borde ringa om en överraskande kontakt innehåller något av följande:
 - ett fantastiskt och unikt erbjudande, en lottovinst, ett arv, affärs- och placeringsmöjligheter
 - ett överraskande meddelande från en okänd beundrare som vill vara med dig
 - du erbjuds en möjlighet till lättförtjänta pengar

Du hotas och utpressas

- En bedragare kan utsätta dig för utpressning och hota med att du till exempel förlorar ditt rykte och egendom genom att:
 - hen sitter på känsligt material om dig
 - hen slår ut ditt företags eller din organisations webbtjänst med ett överbelastningsangrepp eller dataintrång
 - hen sitter på uppgifter om ditt företag eller din organisation som erhållits genom dataintrång
 - det är bråttom och hen uppmanar dig att agera snabbt

They give you promises they cannot keep

- You should be highly suspicious if someone contacts you unexpectedly, indicating any of the following:
 - an amazing and unique offer, winning the lottery, getting an inheritance, a business and investment opportunity
 - a surprising message from an unknown admirer who wishes to be with you
 - you are offered an opportunity to earn money easily

You are threatened and blackmailed

- A scammer can blackmail and threaten you with things such as losing your reputation and possessions by claiming that:
 - they hold sensitive materials of you
 - they are going to crash your company's or organization's online service with a denial of service attack or hacking
 - they hold information about your company or organization obtained via hacking
 - they are in a hurry and are asking you to act quickly

Hur känner du igen en nätbedragare?

How to recognize an online scammer?

Du hamnar på en bluffside

- Den förfälskade webbplatsen ser nästan äkta ut, men detaljerna avslöjar bedrägeriet

Under förevändning av att det är bråttom eller en undantagssituation måste du vidta åtgärder eller lämna ut dina uppgifter

- du ombeds logga in på till exempel din nätbank eller ditt e-postkonto via länken i meddelandet
- du eller din organisation får en oväntad och brådskande faktura där avsändaren utger sig för att vara till exempel en känd verkställande direktör
- du får ett e-postmeddelande med en bilaga med en (brådskande) "faktura"
- en person som presenterat sig som teknisk stödperson ber om dina användarnamn, lösenord eller distansförbindelse till din dator

You end up on a scam website

- The fake website also looks almost authentic, but the details reveal the scam

Using being in a rush or exceptional circumstances as an excuse for requiring your actions or information

- you are asked to log in your online bank or email account via a link in a message sent to your email account
- you or your organization receive a surprising and urgent invoice whose sender presents themselves as a managing director you know, for instance
- you receive an email to which an (urgent) "invoice" has been attached
- a person presenting as an IT support person asks you for your user ID, password or remote connection to your computer

Hur skyddar du dig mot bedrägerier?

How do you protect yourself against a scam?

Lita inte blint på avsändaruppgifterna i ett e-postmeddelande

- Adressen kan vara förfalskad, avsändarens dator kan vara hackad eller någon har kunnat gissa avsändarens e-postlösenord
- Klicka inte på en länk i ett meddelande som verkar misstänkt, utan öppna webbläsaren och gå direkt till tjänstens webbplats

Lita inte på alla webbplatser

- Ange inte in dina kreditkortsuppgifter eller nätbankskoder på en webbplats som verkar misstänkt utan övervägande

Kontrollera adressen i webbläsaren

- I nätfiskesyfte registrerar bedragarna domännamn som ser nästan likadana ut och med nästan samma namn som de ursprungliga domännamnen

Do not blindly trust email sender information

- The address may be fake, the sender's computer may have been hacked, or someone may have guessed the person's email password
- Instead of clicking on the link in a message that appears suspicious, use your browser to go directly to the website of the service you are looking for

Do not trust all websites

- Do not enter your credit card information or online banking details on a suspicious website without consideration

Check the destination address on your browser

- Online scammers register domain names for their phishing sites that are almost identical with original domain names in form and name

Hur skyddar du dig mot bedrägerier?

How do you protect yourself against a scam?

Är datatrafiken i webbläsaren krypterad?

- Att en nätbank är krypterad ser du särskilt på att det finns en låsikon i webbläsarens adressfält och att adressen börjar med https://

Byt ett hackat lösenord

- Om ditt lösenord har hackats, byt det omedelbart

Använd olika lösenord i olika tjänster

- Skapa ett eget lösenord för varje tjänst du använder

Have you enabled encrypted communication on your browser?

- You can particularly check the encryption of online banks from the lock icon on your browser's address bar and by looking for an online address starting with https://

Change a hacked password

- If your password has been hacked, change it immediately

Use a different password for different services

- Create a separate password for each service you use

Gör så här om du blir lurad

What to do if you get scammed

- Gör en polisanmälan
- Underrätta även andra berörda parter
 - Om du har blivit utsatt för ett bedrägeri där någon utgett sig för att vara ett finansinstitut, ska du också underrätta finansinstitutet om detta
- Förhindra ytterligare skador
 - Om ditt lösenord eller dina kreditkortsuppgifter har hamnat i fel händer, byt lösenord och kontakta din bank för att spärra kortet
- Report the incident to the police
- Also inform the parties concerned
 - If you are a victim of a scam made by someone pretending to be financial institution, you should also report it to the financial institution
- Prevent further damage
 - If your password or credit card information has ended up in the wrong hands, change your password and contact your bank to cancel the card

Gör så här om du blir lurad

What to do if you get scammed

- **Hjälp på andra webbplatser**
 - **Brottsofferjouren**
 - <https://www.riku.fi/sv/>
 - **Konsumentförbundets bedrägeriinformation**
 - <https://www.kuluttajaliitto.fi/2020/08/19/huijausinfo-auttaa-digihuijausten-uhreja-ja-heidan-laheisiaan/>
- **Anmäl falska webbplatser**
 - **Finska Kyberturvallisuuskeskus kan vidarebefordra informationen så att bluffsidorna fås bort**
- **Other online sources to help you**
 - **Victim Support Finland**
 - <https://www.riku.fi/sv/>
 - **Consumers' Union of Finland scamming info**
 - <https://www.kuluttajaliitto.fi/2020/08/19/huijausinfo-auttaa-digihuijausten-uhreja-ja-heidan-laheisiaan/>
- **Report a scam site**
 - **Finnish Kyberturvallisuuskeskus can forward the information so that the scam pages are removed**



Tom Tuunainen
Centria SecuLab
seculab@centria.fi
<https://seculab.fi>

