



Säkert på nätet

2026

Trygg användning av koder

- Dina koder är personliga, **och du ska aldrig överlåta dem eller låna ut dem till någon annan**. Då du använder dina koder motsvarar det din underskrift.
 - Avtal, uppdrag, ansökningar och meddelanden som har undertecknats med dina koder är bindande för dig. När du identifierar dig eller bekräftar transaktioner med dina koder ska du alltid kontrollera att tjänsten som du knappar in koderna i är säker.
 - När du får en begäran om att bekräfta något med Mobilnyckeln, ska du alltid kontrollera alla uppgifter i transaktionen. Om uppgifterna är korrekta och du själv håller på att sköta ett ärende med dina koder, kan du bekräfta begäran.
- Om du inte själv kan sköta ärenden med dina koder, **får du ändå aldrig överlåta dem till någon annan**. Om du behöver hjälp med dina dagliga penningaffärer kan du ge en pålitlig närstående person dispositionsrätt till ditt konto.

Så här ser du till att dina ärenden sköts tryggt

- Låt aldrig någon annan använda dina koder och avslöja aldrig dina lösenord för någon
- Använd appen OP-mobilen för dina ärenden om det är möjligt. Via den kan du inte hamna på bluffwebbplatser
- Kontrollera att du säkert är på OP:s webbplats när du använder nätbanken
 - Om du loggar in i nätbanken via en webbläsare i datorn eller någon annan enhet, ska du själv skriva hela adressen www.op.fi på webbläsarens adressrad eller använda ett bokmärke som du har sparat
 - Logga inte in i nätbanken via sökmotorer. De leder ofta till bluffwebbplatser
- Mata aldrig in dina nättjänstkoder via en länk som du fått per e-post eller textmeddelande
- Bekräfta inte betalningar eller transaktioner som du inte själv håller på att göra och valt att bekräfta
- Förvara dina koder och lösenord omsorgsfullt och förvara dem inte på samma ställe
- Se till att programvaran och skyddet i din dator och dina mobilenheter är uppdaterade
- Följ dina kontotransaktioner och kreditkortsdebiteringar, aktivera t.ex. notiser
- Fundera ut en lämplig säkerhetsgräns, alltså en bruksgräns per dygn, för dina betalkort och konton

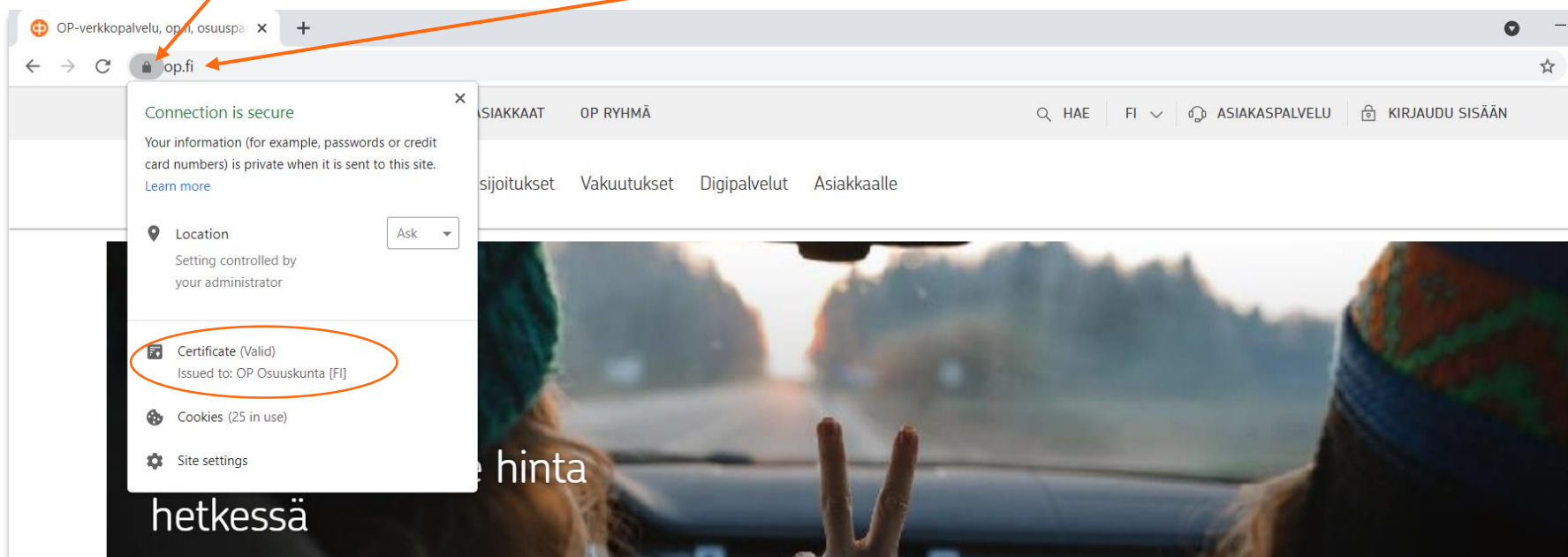
OP:s riktiga nättjänst

OP:s certifikat
(OP Osuuskunta [FI])

På webbläsarens
adressrad op.fi

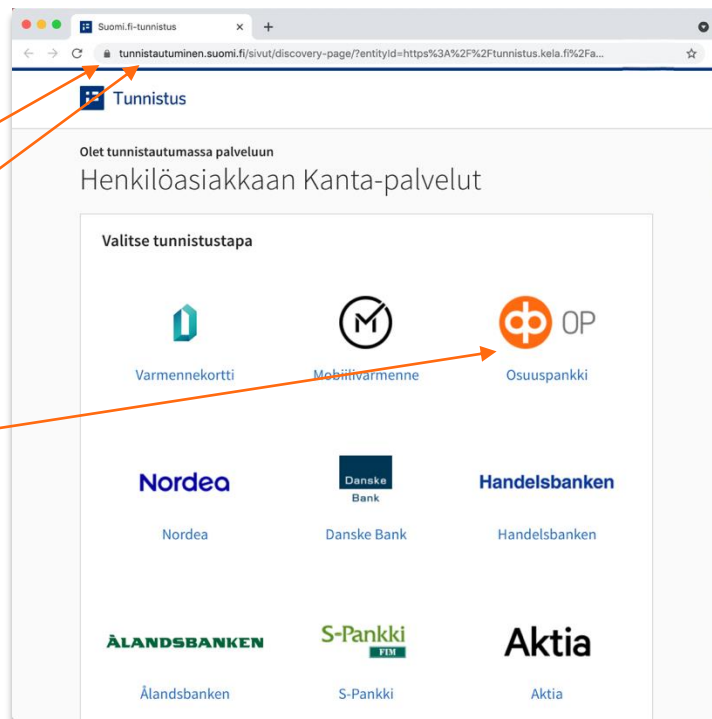
Logga aldrig in i nätbanken via en sökmotor, eftersom du kan hamna på en bluffwebbplats – Logga alltid in i OP:s nättjänst genom att skriva adressen **op.fi** på webbläsarens adressrad. Vi rekommenderar att du sköter ärenden med appen OP-mobilen, som du kan ladda ner via appbutiken.

Obs. Webbläsaren Chrome



Sköt ärenden tryggt i andra tjänster

- Kontrollera alltid att tjänsten som du knappar in din kod i är säker
- Du kan kontrollera att du är på rätt sida
 - via certifikatet som du ser då du klickar på bilden av ett lås på adressraden
 - via adressen som du ser på webbläsarens adressrad
- Du känner igen knapparna för OP:s identifiering och nätbetalning på OP:s logo



Misstänker du att dina uppgifter har hamnat i fel händer? Gör så här:

- Ta omedelbart kontakt med OP:s kundtjänst, om
 - dina nätbankskoder, numret på ditt betalkort eller någon del av dem har hamnat i fel händer
 - ditt identitetsbevis eller en kopia av det har försvunnit.
 - du till exempel på ditt konto upptäcker transaktioner som du inte själv har utfört.
 - Gör en polisanmälan om du misstänker eller vet att någon använder dina person- eller bankuppgifter. Följ myndigheternas anvisningar.
 - Förhåll dig skeptiskt till okända som kontaktar dig, oavsett om det sker per telefon eller e-post. Uppge aldrig dina lösenord eller koder per telefon eller e-post.
- Kundtjänst för privatkunder 0100 0500.
 - Kundtjänst för företagskunder 0100 05151
 - Om kundtjänsten inte är öppen ska du spärra dina koder genom att ringa OP Spärrtjänsten 0100 0555 (24 h/dygn). Anmäl det som hänt också till kundtjänsten när den öppnat.
 - Spara på förhand numret till spärrtjänsten i din telefon.
 - Numren finns på sidan Kundtjänst i op.fi.

Kom ihåg att banken, polisen eller någon annan pålitlig part ALDRIG ber dig uppge dina nätbankskoder eller lösenord per telefon eller att logga in i nätbanken via en länk!

Fick du ett konstigt meddelande eller hamnade du på en misstänkt webbplats?

- Skicka oss en anmälan per e-post till adressen tietoturvailmoitukset@op.fi, om
 - du misstänker att du har fått ett falskt e-postmeddelande eller textmeddelande i OP:s namn
 - du i tjänsten op.fi får ett meddelande som avviker från det normala eller en misstänkt vy.
- Uppge följande uppgifter i din anmälan:
 - ditt namn, dina kontaktuppgifter och namnet på din andelsbank.
 - det suspekta e-postmeddelandet helst som bilaga. Du kan i allmänhet spara ett e-postmeddelande genom att välja Arkiv – "Spara som". När du har sparat filen kan du bifoga den till ditt e-postmeddelande.
 - Om du har besökt en suspekt webbplats och tagit till exempel en skärmbild av den eller om du har sidans källkod, kan du bifoga dem till din anmälan.

Skriv aldrig dina koder på en webbplats som öppnas via en länk
och gå aldrig till nätbanken via en sökmotor!

Exempel på bluffmeddelanden

Som säkerhetsåtgärd
är ditt kort hindrat.

Bekräfta
din identitet
för att återaktivera
ditt kort: [http://\[redacted\].info](http://[redacted].info)
[/Vahvistus](#)

Länkar till nätfiskesidor

Banktjänster uppdateras
inte per e-post

Konstig e-postadress för
avsändaren
Avsändaruppgiften "OP" har
förfalskats

From: OP <cvcats@mundo-r.com>
Sent: Thursday, April 15, 2021 8:01:15 PM
To:
Subject:



Bästa kund

Av säkerhetsskäl har vi tillfälligt hindrat ditt kort för att återaktivera det, vi bjuder dig att klicka på länken nedan.

[Klicka här för att aktivera ditt kort](#)

Tack, för att du inte svarade på detta meddelande.

Bedragare skapar en känsla av brådska för att man inte ska hinna
tänka igenom saken rationellt! Inget ärende är så brådskande att det
inte kan vänta tills du hinner fråga om det på kontoret eller via
telefon tjänsten.

Nätbedrägerier: Placeringar, kärlek, arv, lotterivinster eller lån från utlandet

1

Löfte om stora summor, men det krävs förhandsavgifter för att ta hem dem

2

Begäran om att förmedla pengar för bland annat tullavgifter, skatter, visum eller flygbiljetter (förfalskade dokument)

3

Placeringar eller valutahandel med löfte om hög avkastning. Övertalning och påtryckning utnyttjas för att skapa en känsla av att man inte kan tacka nej till erbjudandet.

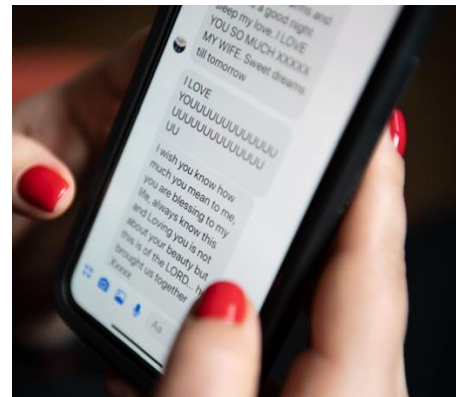
4

Man vinner förtroende eller kärlek innan man ber om hjälp och pengar.
För bra för att vara sant!

Det effektivaste sättet att skydda sig mot manipulation och brottslighet på nätet är att känna igen olika bedrägeriförsök och de vanligaste formerna av missbruk

Tips för att känna igen bedrägerier

- ✓ En överraskande förfrågan av en okänd person (till exempel via Facebook, Instagram)
- ✓ Ett samtal från någon som utger sig för att vara till exempel en myndighet och en brådskande begäran om att ge ut nättjänstkoder eller kortuppgifter under samtalet under hot om att kunden annars förlorar sina pengar
- ✓ En tidigare okänd part erbjuder en stor summa pengar eller ett placeringserbjudande som låter för bra
- ✓ Meddelandena är skrivna på dåligt språk
- ✓ En begäran om att uppdatera personlig information via e-post eller textmeddelande (meddelandet innehåller en länk)
- ✓ Meddelandet har sänts vid ett konstigt klockslag eller på en konstig veckodag (till exempel natt, helg)
- ✓ *En känsla av brådska och press!*



Tips för att känna igen bedrägerier

- ✓ Whatsapp-meddelande av någon som verkar vara bekant med som de facto är en bedragare. I meddelandet ber hen dig skicka en verifieringskod som du fått per textmeddelande till hen.
- ✓ På riktigt är det fråga om din egen sexsiffriga verifieringskod för Whatsapp som du inte ska ge ut till någon.
- ✓ Med verifieringskoden kan bedragaren kapa ditt Whatsapp-konto. Så har det gått för din bekanta som meddelandet kom från.
- ✓ Själv behöver du verifieringskoden endast då du håller på att överföra ditt Whatsapp-konto till en ny enhet.
- ✓ På Instagram och Facebook Messenger finns motsvarande bedrägerier. Där försöker bedragaren först få reda på ditt telefonnummer och sedan verifieringskoden som skickats till dig i ett textmeddelande. Med hjälp av dessa uppgifter kan bedragaren kapa ditt Instagram- eller Facebook-konto.
- ✓ Det är svårt att få tillbaka kontrollen över användarkontot från bedragaren.



Gör så här om du misstänker att du blivit lurad

- Sluta omedelbart hålla kontakt med brottslingarna.
- Om brottslingar har fått reda på eller det finns risk för att de fått reda på dina nättjänstkoder eller kortuppgifter eller om pengar har överförts från ditt konto genom ett bedrägeri, ska du omedelbart kontakta OP:s kundtjänst eller din andelsbank.
 - Vid behov hjälper banken med att göra begäranden om återbetalning och med fortsatta åtgärder
- Anmäl fallet till myndigheterna.
- Kontakta också vid behov brottsofferjouren (<https://www.riku.fi/sv/>).
 - Kontakt per telefon eller nätet

Så här får du hjälp med bankärenden per telefon



Behöver du hjälp med dina bankärenden i vardagen?

Vi står till tjänst per telefon i vår särskilda kundtjänst för seniorer. Samtalen besvaras alltid av en rådgivare som känner till seniorkundernas särskilda behov och kan erbjuda just rätt slags handledning.

Kundtjänsten för seniorer: 010 252 9627

Tjänsten är öppen vardagar kl. 9–16

Samtalspris: 0,0835 €/samtal + 0,167 €/minut.

Priset gäller även kötid.

Det finns ingen åldersgräns för tjänsten, utan alla som behöver särskilt stöd kan ringa tjänsten.

Har du en dator och internetuppkoppling? Du får fler anvisningar och tips för bankärenden på vår webbplats på adressen **op.fi/seniorer**

Du kan också alltid be din andelsbank om hjälp med skötseln av bankärenden och till exempel användningen av nättjänster.



Har ditt kort försvunnit eller stulits?

Spärrtjänst för kort: 0100 0555

Spärrtjänsten är öppen dygnet runt.

För samtal tar vi ut den normala lokalnätsavgiften/mobilsamtalsavgiften. Priset gäller även kötid.



Du får alltid hjälp också genom att ringa vår allmänna kundtjänst.

OP:s kundtjänst 0100 0500

Tjänsten är öppen vardagar kl. 8–16.

För samtal tar vi ut den normala lokalnätsavgiften/mobilsamtalsavgiften. Priset gäller även kötid.