Bilaga med tilläggsuppgifter: Aktuella exempel på nätbedrägerier och tips för att skydda sig mot dem.

Fiskeri i samband med näthandel

En bedragare som utger sig för att vara köpare på en plattform för näthandel skickar ett sms eller ett WhatsApp-meddelande till säljaren med en länk till en falsk sida för transportservice eller till en falsk betaltjänst för näthandelsplattformen. På den falska sidan begär man säljarens kortuppgifter och bankkoder för att bedragaren ska kunna betala de inköp bedragaren gjort.

Så här skyddar du dig:

- Köparen eller betaltjänsten behöver inte försäljarens nätbankskoder eller betalkortsuppgifter. Köparen behöver endast säljarens kontonummer. Den som frågar efter nätbankskoder eller uppgifter om betalkort är sannolikt en bedragare. Anmäl detta till polisen och banken.
- Om du får en länk till en betaltjänst är det sannolikt ett bedrägeri. Anmäl detta till polisen eller banken.
- Om du har lämnat ut dina nätbankskoder eller kortuppgifter eller du misstänker att du betalat en bluffbetalning, ska du omedelbart kontakta din bank och därefter polisen.

Bedrägerier på Facebook

En bedragare kapar ett Facebook-konto, tar via Messenger kontakt med personens Facebook-vänner och meddelar om en lotterivinst. Därefter ber bedragaren om offrets telefonnummer för att per sms kunna skicka en länk till en bluffsida. På bluffsidan ber man offret om nätbankskoder eller kortuppgifter för att lösa ut vinsten. Som ett resultat av detta kommer bedragaren åt att göra betalningar från offrets konto och vid behov manipulerar bedragaren offret att godkänna betalningarna.

Liknande metoder förekommer också på Instagram, så det lönar sig att överlag vara skeptisk till onormala kontakter i sociala medier.

Ett annat bedrägeri som sker på Messenger är att en kod skickas till offret och när offret matar in koden kommer man åt att kapa offrets användarkonto. Innan detta händer fortsätter ändå diskussionen och man berättar om möjligheten att delta i en utlottning eller tävling. Man ber offret om nätbankskoder och lurar offret att själv godkänna betalningarna. I vissa fall installerar bedragarna åt sig själva den identifieringsapp som offret använder, så att de själva kan använda offrets konto.

Du ska vara speciellt försiktig om någon du känner via Messenger frågar exempelvis efter ditt telefonnummer eller ber dig skicka ett sms som du fått. I stället för din bekant är det en bedragare som frågar efter uppgiften. Om du lämnar ut dem kan bedragaren eventuellt kapa ditt Facebook-konto.

Så här skyddar du dig:

- Lämna inte ut nätbankskoder eller betalkortsuppgifter till någon, inte ens till närstående eller vänner.
- Betalaren behöver inte dina nätbankskoder eller dina kortuppgifter. Betalaren behöver endast ditt kontonummer. Den som frågar efter nätbankskoder eller kortuppgifter är alltså en bedragare. Anmäl detta till polisen eller banken.
- Fast det ser ut som om meddelandet kommer från en bekant person så kan avsändaren vara en bedragare som kapat din bekants användarkonto.
- Om du har lämnat ut dina nätbankskoder eller kortuppgifter eller du misstänker att du betalat en bluffbetalning, ska du omedelbart kontakta din bank och därefter polisen.

Bedrägeri via WhatsApp

Bedragaren uppger sig vara offrets vuxna barn som berättar att han eller hon varit tvungen att byta både telefon och telefonnummer eftersom den föregående telefonen gått sönder (t.ex. i tvättmaskinen). Därefter meddelar bedragaren att han eller hon genast behöver pengar och ber offret om pengar. Vanligtvis ber man att pengarna ska betalas till ett utländskt konto.

Så här skyddar du dig:

- För inte över pengar till kontot innan du är säker på att personen som skickat meddelandet verkligen är den person som han eller hon uppgett sig vara.
- Kontrollera via personens tidigare telefonnummer om han eller hon faktiskt har bytt telefonnummer och om personen har skickat dig ett meddelande.
- Om kontonumret som finns i meddelandet är ett annat än det kontonummer personen tidigare har använt ska du också kontrollera numret. Om kontonumret har någon annan landskod än Finland (FI) i början, ska du kontrollera extra noggrant med mottagaren om kontonumret är rätt. Försäkra dig om att kontonumret är rätt på något annat sätt än via det telefonnummer som man ber om pengarna.
- Om personen inte svarar på det tidigare telefonnumret ska du kontrollera att meddelandet är äkta genom att träffa personen ansikte mot ansikte, om detta är möjligt.
- Om du har lämnat ut dina nätbankskoder eller kortuppgifter eller du misstänker att du betalat en bluffbetalning, ska du omedelbart kontakta din bank och därefter polisen.

Flubot-bluffmeddelanden

Under våren 2022 fick speciellt användare av Android-telefoner bluffmeddelanden vars avsikt var att få mottagarna av meddelandet att ladda ner skadeprogram på sin telefon. Med hjälp av skadeprogrammet kommer brottslingarna åt telefonens innehåll, kontakter och meddelanden. De använder dessa uppgifter för att komma åt användarens konton på sociala medier och för annan ekonomisk vinning.

Europol lyckades i slutet av maj splittra den kriminella organisation som låg bakom bedrägerierna.

Falska poliser och falska banker

Offret får ett telefonsamtal. Offret får veta att hans eller hennes bankkonto har kapats och att polisen eller banken behöver nätbankskoderna och eventuellt betalkortsuppgifterna för att förhindra ett brott.

Bedragare som utger sig för att vara poliser verkar också utanför nätet. De kan dyka upp hemma hos offret och begära nätbankskoder och betalkort.

Så här skyddar du dig:

- Polisen eller banken ringer aldrig upp eller kommer på hembesök och ber om nätbankskoder eller kortuppgifter. Om det här händer är det ett bedrägeri. Avsluta genast samtalet eller stäng dörren. Anmäla detta till banken och polisen.
- Om du har lämnat ut dina nätbankskoder eller kortuppgifter eller du misstänker att du betalat en bluffbetalning, ska du omedelbart kontakta din bank och därefter polisen.

Begäran per sms

Se upp och förhåll dig skeptisk till alla sms du får där du ombes öppna en länk eller en bilaga, installera ett program eller överlåta information. Bedragare kan skicka dig meddelanden också i en banks eller myndighets namn.

Förfalskning av telefonnummer

Bedragare kan också förfalska telefonnummer. Om du får ett telefonsamtal från ett finländskt nummer och du efter samtalet misstänker att det var en bluff eller du annars är orolig över samtalet, kan du ringa tillbaka till numret för att kontrollera saken. Till utländska telefonnummer lönar det sig inte att ringa, för till dem kan man ha kopplat olika faktureringsbedrägerier.

Cybersäkerhetscentret vid Transport- och kommunikationsverket och teleoperatörerna har utvecklat olika tekniska lösningar för att förhindra nummerförfalskning. Om ett samtal som ser ut att komma från ett finländskt nummer i själva verket kommer från utlandet kan man i fortsättningen förhindra att telefonnumret visas.

Bedrägerier med QR-koder

Under den senaste tiden har man lagt märke till förfalskade QR-koder i samband med försäljningspunkter, t.ex. vid servicestationer. När man läser koden hamnar man på en förfalskad webbplats. Var uppmärksam när du använder QR-koder vid betalning.

Gör så här om du misstänker att en bedragare kommit åt dina betalningsuppgifter

Följ anvisningen från Myndigheten för digitalisering och befolkningsdata: Mina personuppgifter har stulits eller läckt ut - Suomi.fi