Bli inte lurad!

Polisen

Handelsbanken

Sparbanken i Enköping

Telefonen ringer…

Du blir uppmanad att logga in med ditt BankID

Stopp!

2023 rekordår för telefonbedrägerier

Ökning med 22% sedan 2022 enligt Brottsförebyggande rådet

Bedrägeri genom social manipulation är en typ av bedrägeri där bedragaren tar kontakt med en person, exempelvis genom ett telefonsamtal, och vilseleder den att göra något som syftar till att ge bedragaren ekonomisk vinning. Ett vanligt tillvägagångssätt är att bedragare utger sig för att vara en banktjänsteman eller myndighetsperson, säger Matheus Eriksson, statistiker, Brå.

Exempel från SSF

Vad är egentligen vishing? (telefon)

Ordet Vishing är en kombination av voice (röst) och phishing.

Vishing är när en bedragare kontaktar dig på telefon och utger sig vara någon annan, till exempel banken eller polisen. Ofta påstår bedragaren att det är bråttom för att stressa dig och att du inte ska tänka igenom situationen.

Varningstecken

Lär dig känna igen de vanligaste varningstecknen

Det är bråttom

Oväntad kontakt

De ber dig använda din e-legitimation

Varningstecken

Det är bråttom

Bedragare bygger ofta upp en känsla av att det är bråttom –du måste agera snabbt. Samtidigt anspelar de många gånger på rädsla. Det kan till exempel handla om att någon närstående ligger på sjukhus och behöver hjälp, eller att de säger sig se obehöriga transaktioner på ditt konto.

Varningstecken

Oväntad kontakt

Ibland utger sig bedragare för att vara någon du känner.

Till exempel från en bank, ett känt företag eller någon i familjen. Ett vanligt bedrägeriförsök är när en bekant som du inte haft kontakt med på länge hör av sig på Messenger och frågar hur du mår. Då finns risk att det är en bedragare som kapat din bekants Facebookprofil.

Kom även ihåg att sms, telefonnummer och e-post kan förfalskas och se ut att komma från en annan avsändare än den du tror. Använd heller inte telefonens återuppringningsfunktion, då kan du komma till bedragaren i stället för den du tror är avsändaren.

Varningstecken

De ber dig använda din e-legitimation

Om någon uppmanar dig att använda och signera med din säkerhetsdosa eller e-legitimation (som Mobilt BankID), klicka på länkar, ladda ner program eller skicka pengar – avsluta konversationen.

Hur går det till?

Just nu: Bedragare ringer och uppger sig vara från närliggande sjukhus eller hälsovårdscentral

Bedragaren säger att det gäller en kommande hälsokontroll och att läkaren önskar ha ett underlag inför besöket och frågar därför allmänt:

hur mår du?

äter du några mediciner?

stämmer det att du heter...

och har personnummer..

Bedragaren uppmanar därefter att ta fram bankdosa eller logga in på mobilt bank-id för att scanna en QR kod som bedragen då kommer att skicka. I samma veva så erbjuder bedragaren en tid för läkarbesöket.

Exempel:

Du får ett samtal från en någon som påstår sig ringa från banken eller polisen. Bedragaren säger sig behöva exempelvis din personliga kod till Kundcenter/telefonbanken, PIN-kod till ditt kort eller ber dig logga in med Mobilt BankID.

Exempel:

Förklaringen till varför bedragaren ber om dessa uppgifter kan variera. Det kan till exempel vara att banken har datafel alternativt att banken eller polisen har funnit ditt stulna kort och behöver koden för att spärra kortet. Bedragaren kan även påstå att du blivit utsatt för ett bedrägeri och att banken eller polisen behöver din hjälp för att se till att du inte blir av med pengar.

Exempel:

Bedragarna kan även påstå

De ska **stoppa ett pågående bedrägeri** på ditt konto eller kort

De kan hjälpa till med **skatteåterbäringen**

De ska hjälpa dig med **coronarelaterade tjänster,** som vaccinering

De kan **ge tillbaka pengar** som du blivit lurad på

Du har **vunnit pengar**

En **närstående** har råkat illa ut och **behöver din hjälp**

Din **dator har fått virus** eller andra problem som de säger sig kunna hjälpa dig med

Du ska ladda ner en **programvara för att förhindra en pågående virusattack**

Så skyddar du dig

Så skyddar du dig

Om någon påstår att den ringer från visst företag - kolla upp numret personen ringer ifrån och se om det stämmer.

Var försiktig med återuppringning av missade samtal. Det kan ske en koppling så att du hamnar på ett bedrägeri-nummer av något slag.

Lämna aldrig ut personliga koder via telefon även om personen ifråga påstår sig ringa från banken eller polisen.

Svara inte på konstiga frågor per telefon från okända personer.

Om du trots allt lämnat ut personliga uppgifter - kontakta din bank omgående.

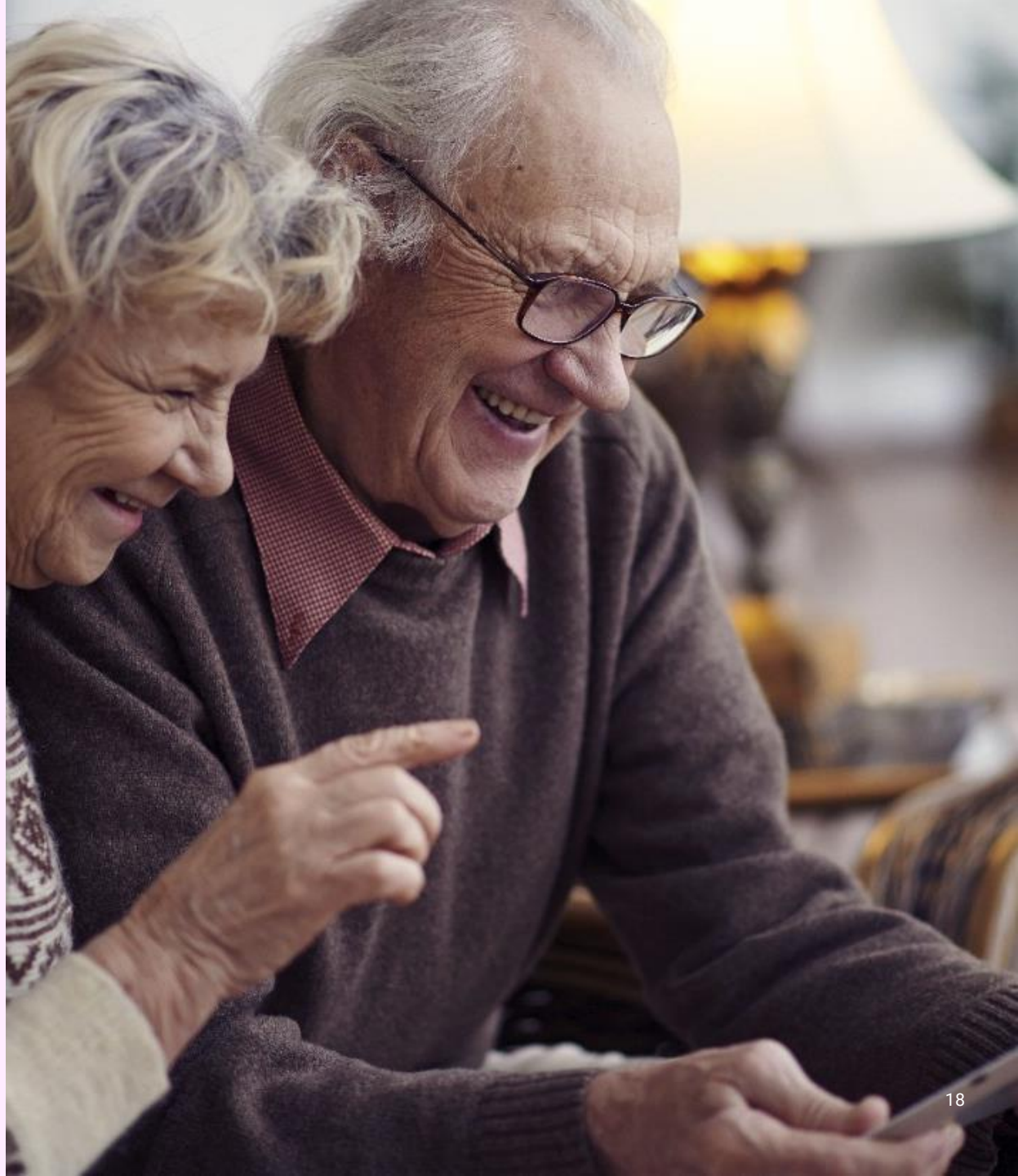
Äldre personer mest drabbade

Brottsvinsterna gällande vishing är stora vilket gör att polisen måste vara snabba i sitt arbete.

Återtagandet av brottsvinster och säkerställandet att målsägare inte förlorar sina pengar är a och o för polisen, och arbetet med att kunna spåra konton och säkra pengar via banken går framåt.

Chansen är dock väldigt liten att du ska få tillbaka några pengarna när du har drabbats. Vi lyckas ta en del pengar i beslag genom att banken fryser penningtvättarnas konton, men huvudbudskapet är att de försvinner, säger Maria Karlsson.

Vem som i slutändan får det här pengarna är svårt att säga. Det går i många penningtvättsled där många yngre personer utnyttjas för penningtvätt genom att vara målvakt.



Många anmälningar

Under 2022 upprättades 1600 anmälningar om bedrägerier genom social manipulation i region Mitt, och här innefattas telefonbedrägerier.

Under det första halvåret 2023 har den siffran passerats.

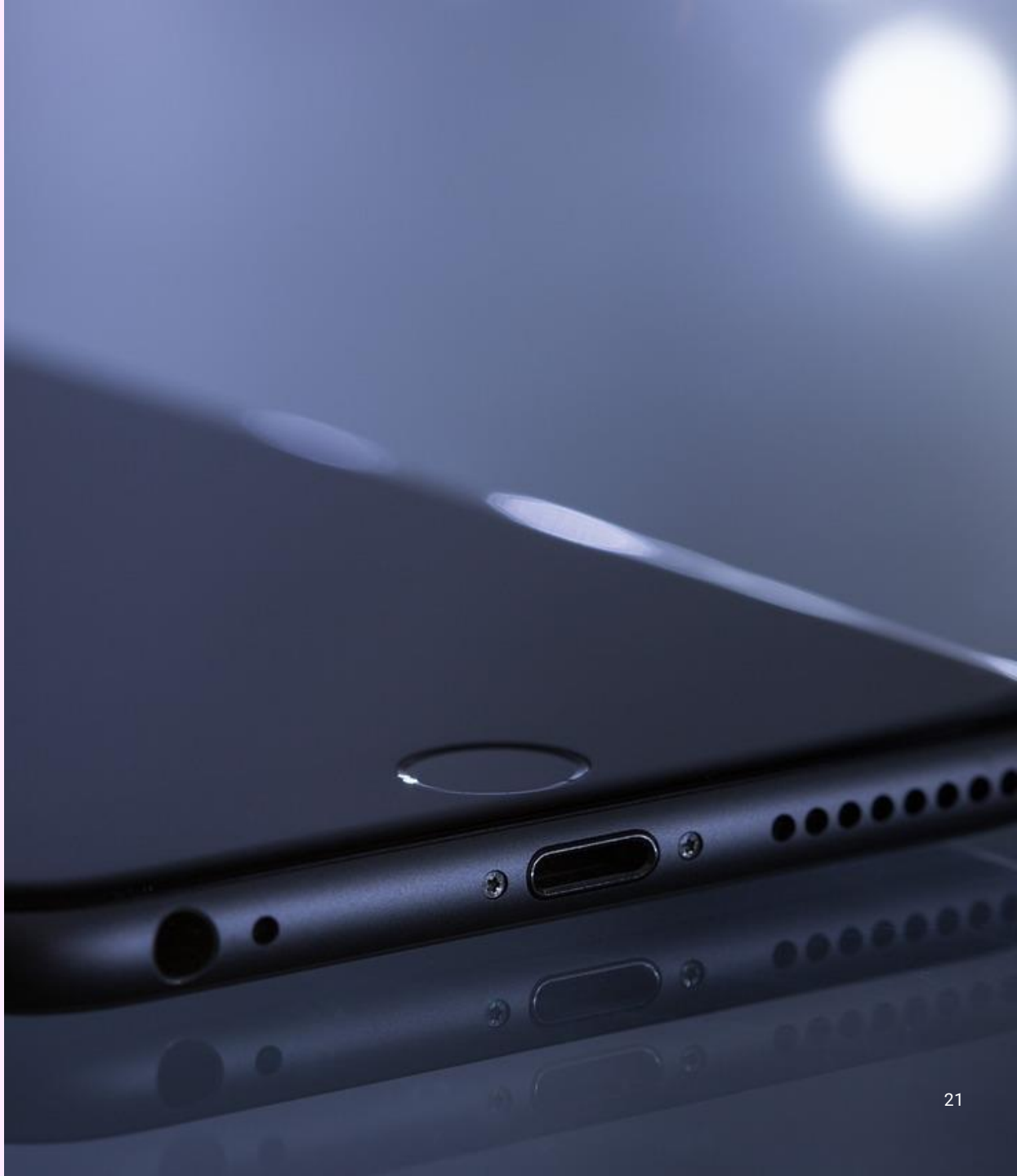
Vad gör du om du blivit drabbad?

Kontakta genast din bank!

Polisanmäl alltid ett bedrägeriförsök.
Ring polisen på 114 14.

Andra typer av bedrägerier

- SMS-bedrägerier
- Oväntat hembesök
- Mailbedrägerier
- Romansbedrägerier
- Investeringsbedrägerier
- Falska annonser
- Fysiskt bedrägeri




Frågor?

Tack!

Polisen

Handelsbanken

Sparbanken i Enköping