

230330



Banken berättar om bedrägerier!

Sveriges banker och Bankföreningen, tillsammans med Polisen, har nyligen startat en kampanj för att göra folk mer uppmärksamma på det ökande antalet bedrägerier, särskilt riktade mot äldre, - "Svårlurad".

Vi bad vår närmaste bank, Westra Wermlands Sparbank, att bjuda in oss till en informationsträff, och det gjorde de, förstås!

Så igår, torsdag eftermiddag, fylldes bankens samlingsal med Jösse-seniorer som ville lära mer!



Stig Olsson t.v., på marknadsavdelningen, hälsade oss välkomna.

Därefter var det Emil Sjöberg, privatrådgivare, som berättade om det digitala banklivets olika fördelar och fällor.



Emil gick igenom digitala verktyg och tjänster. Han gav information och tips om mobil och internetanvändning. Han visade olika betalningsalternativ på sparbanksappen, berättade om vad man ska tänka på med swishappen (t.ex. kolla upp att mottagaren faktiskt är den som man avsett att skicka pengarna till!) och om mobilt bankID.



Antalet digitala bedrägerier ökar alltså konstant, - förra året inkom 159.000 anmälningar till polisen, därtill kommer ett förmodligen betydande mörkertal. Äldre personer är särskilt ofta utsatta: Vi är ofta ovana och oroliga inför det tekniska, och kanske har vi också större summor på banken än yngre.

Hur går bedragarna tillväga?

De kan ringa upp på mobilen, låta förtroendeingivande, säga sig ringa från bank eller myndighet, de kan t.ex. berätta om pågående bedrägeri som måste stoppas, och om att det är bråttom...! Eller om något annat aktuellt, - deklARATION, elbidrag etc., etc. Vi får se några videos om hur det kan låta.

Det kan vara investeringsbedrägerier på sociala medier, erbjudanden om att prova på. Det kan vara länkar i mejl eller i sms, t.ex. om paketförsändelser och annat. Och det kan j´handla om förslagna och tålmodiga romansbedragare, som utsätter sina offer för långvarig uppvaktning. Och mycket annat - uppfinningsrikedomen är stor,

Så vad ska vi tänka på för att vara säkra på nätet?

Varningstecken vid samtal:

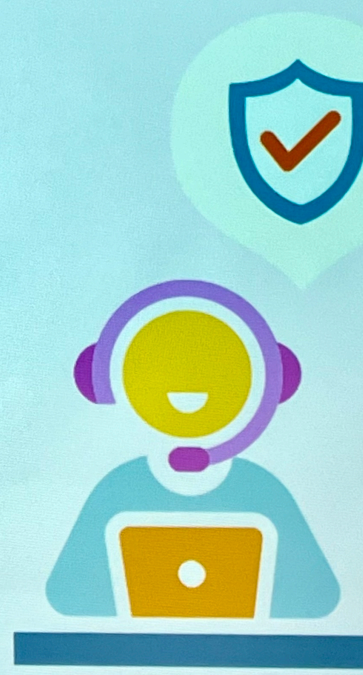
- Ett **oväntat** samtal.
- Du uppmanas **legitimeras** dig.
- Det är **bråttom!**

Banker och myndigheter ringer aldrig upp på det sättet! Lagg på luren, och gör själv ett eget samtal till din bank, eller till myndigheten ifråga, sök själv upp rätt nummer! Logga aldrig in på någon annans uppmaning. När du själv loggar in på BankID, kolla alltid upp att det står rätt mottagare!

Det svåra här är ju att inte i stress göra saker mot bättre vetande!!

Om det ändå händer...

- Hör av dig till banken direkt!
Vardagar 8.00-18.00 när du oss på 0570-848 00
övrig tid ring 0771-97 75 12
- Spärra det som behövs, till exempel e-legitimation (som Mobilt BankID) genom att ringa 08-411 10 11
- Polisanmäl alltid.
- Reklamera till berörda banker och företag



Inte så många frågor kom, men några:

- Om **bankens ansvar** för överföringar? ARN säger nu att bankerna måste ta ett större ansvar, och kolla upp! vid oväntade och större överföringar, frågan är aktuell. Emil menar, att kruxet från bankernas sida är att ett större återbetalningsansvar måste innebära att bankerna blir mer restriktiva med att ge ut mobila bankID, och att det får konsekvenser för många användare som då inte kommer att kunna komma åt nödvändig samhällsservice.
- Någon bank sägs ha **en överförings spärr** vid 25.000 kr, vid högre belopp ringer man, men hur det är med Westra Wermlands Sparbank kan Emil inte ge något tydligt svar på.
- **Statligt mobilt ID?** Det sägs vara på gång, men osäkert när.
- **FrejaID?** Har motsvarande säkerhet som BankID, det är bara ett annat bolag, och som är kopplat till vissa företag och tjänster.
- **Kan man bli bedragen utan att själv uppge Mobilt BankID?** Inget fall med detta hittills!
- Däremot **bedrägeri med betal- och kreditkort:** Lämna aldrig ifrån dig kortet på en restaurang, t.ex. Var försiktig med hur du hanterar kortuppgifter. Han inte heller stora summor på det kort du använder för att handla på nätet med. Tänk också på att spärra kortet för internetanvändning, ha det öppet bara när du själv ska handla.
- **Legitimation med tumavtryck eller ansiktsigenkänning?** Lika säkert som med kod.

Det kommer hela tiden nya sätt att bedra, det är viktigt att hålla sig uppdaterad. Här nedan ses några länkar som det är bra att regelbundet följa!



Håll dig uppdaterad

Bra hemsidor:

- Westra Wermlands Sparbank www.wwsparbank.se/bedrageri
- Bankföreningen www.svarlurad.se
- Polisen www.polisen.se/bedrageri
- Finansinspektionen www.fi.se/konsumentskydd
- Stöldskyddsföreningen www.stodskyddsforeningen.se/bedrageri

Bedragarna hittar hela tiden nya sätt att luras



Efter att frågorna sinade ut, så bjöd banken på lite förfriskningar, och mingel, och sedan var det Tack och slut!

Fler fakta kan du också läsa i broschyren "Svårlurad", bifogad här nedan, på nästa sida!

Vid dator och kamera,

Annelise Paulsen



Svårlurad – i korthet

Det kan vara svårt att **genomskåda** skickliga bedragare som försöker lura dig. Här är tre tips för att minska risken att det sker.

- 1 **Lägg på om samtalet känns obekvämt, stressande eller konstigt.**
- 2 **Logga inte in med din säkerhetsdosa eller e-legitimation (exempelvis BankID) på någon annans uppmaning. Lämna inte ut lösenord eller koder till någon.**
- 3 **Banken ringer inte för att be dig logga in eller lämna ut personliga uppgifter.**

→ **Har du blivit utsatt för bedrägeri?** Kontakta din bank omgående!
→ **Polisanmäl alltid** ett bedrägeriförsök. Ring Polisen på 11414.

Skriv gärna ner numren till din bank och en närstående:

Allt fler människor utsätts för bedrägerier och det finns ett stort behov av att informera om detta brett i samhället.

Bakom initiativet Svårlurad! står Sveriges banker och Svenska Bankföreningen. Initiativet syftar till att ge konkreta tips och information om hur man kan skydda sig själv och sina närstående mot bedrägerier.

Kontakta gärna din bank med frågor om säkerhet. Läs mer på svårlurad.se

**SVÅR-
LURAD,**
ETT INITIATIV AV
SVERIGES BANKER

Så kan bedragare försöka lura dig

Bedrägeriförsöken ökar och metoderna ändras hela tiden. Ju mer du känner till om hur det kan gå till desto lättare är det att undvika att bli lurad. De senaste åren har det blivit vanligare att bedragaren utger sig för att ringa från din bank, polisen, företag, en myndighet eller påstår sig vara din närstående. Bedragarna kan manipulera telefonnummer så att det ser ut som att det exempelvis är banken som ringer.

Bedragarna kan försöka stressa dig, till exempel genom att påstå att du är utsatt för en situation som måste åtgärdas omedelbart. Ofta påstår bedragarna att det är mycket bråttom.

I nästa steg kan bedragaren erbjuda hjälp att lösa det påhittade problemet och rätta till situationen. Bedragaren kan be dig att lämna ut svarskoder från säkerhetsdosan, använda din e-legitimation (exempelvis BankID) eller skriva under en Swishbetalning.

Var på din vakt vid spontana kontakter! Bedrägeriförsök sker inte bara över telefon. Bedragare kan även försöka lura dig genom sms, i sociala medier eller mejl. Det kan också ske genom att de knackar på hemma. Tänk alltid igenom rimligheten i det personen ber dig om att göra – dela aldrig personlig information eller koder. Logga inte in om du känner dig det minsta osäker.

Bedragarna kan påstå att:

- 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**



**SVÅR-
LURAD,**
ETT INITIATIV AV
SVERIGES BANKER

Det är lätt att bli svårlurad!

En broschyr med tips om hur du kan skydda dig och dina närstående mot bedrägerier.

Bakom initiativet står Sveriges banker och Svenska Bankföreningen.
Lär dig mer på svårlurad.se

Så blir du svårlurad

Det är lätt att bli svårlurad – och alla kan bli det. Du kan alltid avbryta ett telefonsamtal som känns konstigt. Be att få återkomma och lägg på. Ring sedan din bank eller en närstående och berätta vad som hänt – sök hjälp och stöd hos någon du litar på. Här beskrivs några vanliga varningstecken och viktig information:

→ **Tänk på** att bedragarna kan säga sig ringa från banken, polisen, ett företag, en myndighet eller påstå sig vara en närstående.

→ **Väntar du samtal från banken eller det här företaget?** Om svaret är nej så bör du vara försiktig med vilken information du lämnar ut. Be att få återkomma om du är osäker på vem som ringer.

→ **Lägg på om samtalet känns obekvämt, stressande eller på något vis konstigt.**

→ **Logga aldrig in på någon annans uppmaning. När du använder e-legitimation (exempelvis BankID) läs noggrant vilken tjänst du identifierar dig mot och vad du skriver under.**

→ **När du använder säkerhetsdosan** tänk på att skydda din pinkod och att inte lämna ut svarskoder från den till någon annan.

! **Kom ihåg!** Banken ringer inte upp dig för att be dig logga in eller lämna ut personliga uppgifter.

Detta kan du som närstående göra

Du som närstående spelar en viktig roll i att sprida information och kunskap. Prata med dina nära om risken att luras av bedragare och hur de bäst undviker det.

Dela gärna med dig av din erfarenhet till den som inte har samma kunskap som du. Du är ett viktigt skydds nät för den som känner sig osäker och ovan. Tillsammans skapar vi en tryggare vardag för alla.

Läs mer på www.svårlurad.se

