Säkerhet

Seniornet Lidingö
Mars-2024

Jan Ekberg
Stefan Ternvald

Här kikar vi på en rad saker du kan göra för att hålla dig säkrare på nätet.

1. **Lösenord**
2. **Håll koll på/skydda dina enheter**
3. **Se upp för bedrägerier**
4. **Ladda bara ner programvara som du känner till**
5. **Använd säkra internetanslutningar**
6. **Berätta inte för mycket om dig själv på nätet**
7. **Handla säkert på nätet**

1. Lösenord

➢**Använd starka och säkra lösenord**

- Se alltid till att du skapar starka lösenord.
- Aktivera också tvåfaktorsautentisering på alla dina viktiga konton så att du har dubbelt skydd och så att det blir svårare för hackaren att komma åt dem.

➢**Välj ett långt lösenord**

- Välj helst ett lösenord som innehåller minst 10 tecken – då tar det längre tid för hackaren att knäcka.

➢**Lösenordet bör vara någorlunda komplext**

- Använd komplexa lösenord, minst 10 tecken: versaler, gemener, siffror och specialtecken.
- Använd gärna en ”lösenordsmening”: Jag bor i Rudboda sedan (1974) – JbiRs(1974)
- Spara dina lösenord i en lösenordslista (vi har en mall)
- Använd gärna ”betydelselösa” lösenord på mindre viktiga appar som DN, SVD, Expressen m.fl.

Kan ditt lösenord ha hamnat i orätta händer?

Kolla här: https://haveibeenpwned.com/

2. Håll koll på/skydda dina enheter

- Installera aldrig program/appar i onödan. Det är också viktigt att installera nya uppdateringar direkt eftersom det kan finnas säkerhetslösningar i uppdateringarna som fixar eventuella säkerhetshål i programmet.

- Ladda aldrig ned programvara på uppmaning från någon annan eller genom popup-fönster.

- Du kan t.ex. få upp fönster som säger att du fått virus på din dator och måste ladda ned ett program för att få bort det. Ladda inte ned programmet, då det troligtvis är bedrägeri, och kör en säkerhetssökning av datorn om du har ett säkerhetsprogram installerat.

2.1 Håll koll på/skydda dina enheter

- **Ha en brandvägg aktiverad:** Det är viktigt att din enhet har brandväggar. De fungerar nämligen som en barriär och håller ute virus, skadlig kod och annat som kan komma åt din dator.

- **Använd antivirus:** Det är bra att ha ett antivirus installerat på din enhet eftersom att det jobbar för att hålla din enhet säker. Ett antivirusprogram skannar din enhet och tar bort skadlig programvara som trojaner eller spionprogram.

- Windows Defender innehåller såväl brandvägg som virusskydd.

3. Se upp för bedrägerier

- Bedragare finns på nätet!
- Det är vanligt att hackare skapar en hemsida som är snarlik en redan existerande hemsida och sedan försöker lura dig att tro att den fejkade hemsidan är den riktiga och att få dig att uppge dina personliga uppgifter.
- Det kan hackarna exempelvis göra genom att skicka ut nätfiske-mail eller genom smishing.
- Om du får ett sådant meddelande så bör du inte klicka på några länkar utan istället kolla upp om flera fått ett liknande meddelande och om det är fejkat eller ej.

3.1 Se upp för bedrägerier

Nedan är några exempel på hur smishing kan se ut i praktiken:

- **Du får ett SMS från din bank** där de uppmanar dig att klicka på en länk. I verkliga fallet är det istället en bedragare som utger sig för att vara en kontaktperson hos den bank du använder. Banker skickar aldrig ut SMS eller mail med uppmaning att klicka vidare.

- **Du får ett SMS där det står att du har vunnit ett lotteri** eller en summa pengar, och allt som krävs är ett kontonummer eller signering med BankID för att sätta in pengarna på ditt konto.

- **Du får ett SMS eller meddelande från en vän eller familjemedlem som är i knipa.** Här ber de om pengar snabbt, eftersom de behöver dem för att ta sig ut från affären, betala en räkning eller liknande. Detta kan även komma från deras riktiga enheter om de har blivit infekterade av virus eller skadlig programvara.

Metoder som bedragarna använder

Här är några metoder polisen vet förekommer.

1. Du blir uppringd av en ”teleoperatör” som vill erbjuda dig förmånlig rabatt på ett abonnemang. Personen ber dig logga in med ditt BankID.

2. En väldigt trevlig ”banktjänsteman” ringer och säger att ditt ID utsatts för bedrägeriförsök. Du uppmanas att lämna kontouppgifter och kod.

3. Du får ett SMS om kommande paketleverans. Du uppmanas att ringa numret i SMS:et. I samtalet ombeds du att logga in med BankID eller swisha.

4. Du blir uppringd av en elektronikkedja som säger att någon försökt köpa varor i ditt namn. De kopplar dig till ”en säkerhetsavdelning” där du uppmanas att logga in med BankID.

5. Det ringer på din dörr och en person utger sig för att vara ”vårdpersonal”.

Så kan du göra för att minska risken att drabbas

- Lägg på luren om någon okänd ringer. Svara inte i mobilen om numret är okänt.
- Släpp aldrig in en okänd person.
- Lämna aldrig ut en kod eller bankkortsnummer.
- Prata med någon du litar på om du misstänker bedrägeri.
- **Erbjudanden som verkar för bra för att vara sanna är det också oftast.**

4. Ladda bara ner programvara som du känner till

- Innan du laddar ner vilken programvara som helst bör du göra efterforskning om den.

Kolla upp vad andra skriver om den på nätet.

- Om det finns några säkerhetsbrister och om någon råkat ut för virus på grund av den bör du undvika att ladda ned programmet.

- Ladda aldrig ned okänd programvara utan ladda enbart ned programvara som du känner till och litar på. Gör du inte det så behöver du i alla fall ta reda på så mycket som möjligt om programmet innan du laddar ned det.

5. Använd säkra internetanslutningar

Om du ska surfa på nätet är det viktigt att du använder säkra internetanslutningar.
Det kan du exempelvis göra genom att använda ett VPN som döljer dig och krypterar din information. Om du inte använder ett VPN eller något annat skyddsprogram bör du aldrig surfa på offentliga nätverk. På offentliga nätverk surfar du helt öppet och det är väldigt lätt för hackare att komma åt din privata information.

Tänk på att det inte bara är din dator som kan bli hackad. Din mobil kan också bli det.
Så undvik att surfa med din mobil på ett offentligt nätverk om du inte har ett VPN installerat.
Om du har surfat öppet utan skydd kan det vara nödvändigt att söka igenom din telefon och kolla om du blivit hackad.

6. Berätta inte för mycket om dig själv på nätet

Just nu berättar vi mer om oss själv på sociala medier än någonsin förut. Men tyvärr kan det också leda till att vi utsätter oss för sårbarheter.

Det finns många risker med sociala medier och just nu är ett av de största cyberrelaterade hoten att vi delar med oss så mycket om oss själva på nätet, som sedan kan användas till att hacka våra konton och få tag på vår personliga information.

Var källkritisk till sociala medier. Exempel på ”deepfake”
https://www.facebook.com/reel/348874478137844 4

7. Så handlar du säkert på nätet –och skyddar dina personuppgifter

- **Ge inte bort dina uppgifter i onödan**
- **Använd falska uppgifter när du inte litar på sajten**
- **Hindra obehöriga att ändra din adress**
- **Undvik typiska bedrägeriförsök**
- **Bestäm kodord med släkt och vänner**
- **Använd virtuella engångskort**
- **Använd fejkade svar på säkerhetsfrågor**
- **Bestrid falska fakturor och polisanmäl bedrägeriförsök**

OBS! Se också sid. 23-31

I datorn – vid surfning

- Surfa helst bara på kända internetsiter. Om du surfar på okända siter – klicka aldrig på länkar.
- Kolla sitens adress. Ser den korrekt ut? https://polisen.se – OK, http://polisens.se – **inte OK**
- Handla på nätet – kontrollera alltid att du är på rätt site. Använd helst fakturametod för betalning. Få varan först – betala sedan.
- Om du använder betal-/kreditkort – spara aldrig ditt kortnummer på siten i fråga.
- Mail på dator. Får du mail från okända avsändare – kolla noga avsändaradressen.
- Är du det minsta osäker – **RADERA och klicka aldrig på länkar.**

En sammanfattning av hur du håller dig säker på nätet

Avslutningsvis kan man aldrig vara för skyddad på nätet och det är bättre att extra försiktig istället för helt oförsiktig.

- Använd alltid starka lösenord och håll koll på vilka hemsidor du surfar på.
- Ladda bara ned program du litar på och uppdatera dem löpande.
- Ha också säkerhetsprogram nedladdade som ett VPN och antivirus. Använd ditt sunda förnuft och lämna inte dina uppgifter till sajter som du inte litar på.
- Var också försiktig när du handlar på nätet. Surfa inte på offentliga nätverk såvida du inte har ett VPN installerat och dela inte heller för mycket privat information på nätet.

Om du följer de råden så finns det en större chans att du identifierar möjliga hot och undviker att falla offer för cyberattacker.

Så lätt kan din röst stjälas – och användas för AI-bedrägerier

Att bedragare ringer upp främst äldre människor, utger sig för att vara ett barnbarn och ber om pengar, har varit ett problem i Sverige i många år.

Nu har en ny variant börjat förekomma i USA: Bedrägerier som utförs med AI-klonade röster.

- Personen i telefonen lät exakt som Ruth Cards barnbarn Brandon. Han behövde pengar snabbt och eftersom Ruth kände igen hans röst begav hon sig till banken.
- Benjamin Perkins föräldrar blev uppringda av en man som sa att han var jurist. Benjamin påstods ha kört ihjäl en annan man och behövde pengar till borgen. Juristen räckte över telefonen till någon – som lät exakt som Benjamin.

I båda fallen, som Washington Post rapporterat om, handlade det om en ny bedrägeriform – röster klonade med hjälp av artificiell intelligens.

Så lätt kan din röst stjälas – och användas för AI-bedrägerier

”Omöjligt att tänka sig för ett år sen”

Tidigare har stora mängder ljudmaterial krävts för att trovärdigt kunna klona någons röst, men AI-utveckligen går i rasande takt – nu är det snabbare, enklare och mer lättillgängligt än förut.

– Det som var omöjligt att tänka sig för ett år sedan, det är gratis i dag. Företagen som gör och säljer AI vill ha mycket data – därför ger de bort sina tjänster,

säger Tobias Falk, lektor på institutionen för data- och systemvetenskap vid Stockholms universitet, till SVT Nyheter.

”Kommit till en punkt där maskinerna kan härma oss”

– Algoritmer tränas på att härma hur den mänskliga hjärnan fungerar. Det går jättefort nu, men det har tagit decennier att komma till en punkt där maskinerna kan härma oss så bra som de gör i dag.

Polisens nationella bedrägericenter skriver i ett mejl till SVT Nyheter att man ”känner till fenomenet” men att man i nuläget inte sett några ärenden i Sverige.

”Vi bevakar detta och har kommunikation med internationella kontakter”, skriver polisens presstalesperson.

Hur många sekunder långt klipp räcker för att kunna klona någons röst? Och hur bra funkar det egentligen på svenska?

Åtgärd:
Använd kodord eller RING och kontrollera

Artificiell Intelligens (AI)
är inte smartare
än den data
vi människor matar den med.

https://www.altinget.se/artikel/ai-hotar-inte-vaar-plats-i-varlden-utan-vaar-formaaga-att-existera-i-den

En sista påminnelse!

Det allra bästa skyddet är ***din egen kunskap***

- Håll alltid dator och program uppdaterade!
- Var uppmärksam när du surfar!
- Glöm inte att säkerhetskopiera viktiga filer/foton!

...och klicka aldrig på sådana här erbjudanden!

Tack för oss!

Jan Ekberg

Stefan Ternvald

Följande sidor beskriver nedan-stående punkter lite mer!

- Ge inte bort dina uppgifter i onödan
- Använd falska uppgifter när du inte litar på sajten
- Hindra obehöriga att ändra din adress
- Undvik typiska bedrägeriförsök
- Bestäm kodord med släkt och vänner
- Använd virtuella engångskort
- Använd fejkade svar på säkerhetsfrågor
- Bestrid falska fakturor och polisanmäl bedrägeriförsök

Så handlar du säkert på nätet –och skyddar dina personuppgifter

Till skillnad från ute i verkligheten där du kan ta dig fram relativt anonymt kan det kännas som att hela webben är ute efter att suga upp så många personuppgifter som möjligt.
Är det inte för att rikta reklam mot dig så är det för något annat.
Vare sig det är något rimligt, som en butik som måste ha din adress för att skicka en vara du köper, eller onödig insamling som bryter mot GDPR, är det lätt att dela uppgifter lite för frikostigt och öppna sig för större risker än nödvändigt.

Ge inte bort dina uppgifter i onödan

Alla personuppgiftsläckor börjar med att användaren delar sina personuppgifter med organisationen som senare utsätts för ett intrång där hackare kommer över dem.
Om du minimerar uppgifterna du frivilligt delar med olika webbplatser minskar du risken att själv drabbas.
Det här behöver inte handla om att vägra använda sajter som till exempel kräver namn och adress för något. Behandling av personuppgifter kan trots allt vara nödvändigt.
En butik behöver namn och adress för att skicka varor hem till dig. Ett finansinstitut behöver betydligt mer än så för att inte bryta mot penningtvättslagar.
Vad det kan betyda är att du inte använder ditt fullständiga eller riktiga namn där det inte är nödvändigt. Att du inte slentrianmässigt fyller i adress och annat.

Använd falska uppgifter när du inte litar på sajten

Om en sajt du skapar ett konto på begär uppgifter som namn och adress, men det inte behövs för något uppenbart syfte – som att skicka något till dig eller av juridiska krav – kan du använda ett alias. Använd en påhittad adress så att ingenting skickas hem till någon oskyldig som råkar på på adressen du väljer. Du kan spara dina fejkuppgifter i till exempel en lösenordshanterare för att snabbt komma åt dem och inte behöva sitta och tänka ut nya uppgifter varje gång.

För telefonnummer föreslår jag inte ett slumpmässigt nummer utan till exempel 0701234567 eller 0730000001. Många sajter vill ha ditt nummer, men med undantag för tvåstegsverifiering via sms är det få som faktiskt behöver det.

Tack vare Bank-ID är vissa typer av bedrägerier mycket svårare att genomföra i Sverige, och om ett företag hackas och uppgifter kommer på vift utsätter det inte de drabbade kunderna för lika stor risk som i länder utan liknande system. Ingen kommer in på ditt bankkonto, hos Skatteverket eller någon annanstans som använder Bank-ID för inloggning genom att kunna din adress, ditt personnummer och när ditt pass går ut.

Med mobilt Bank-ID går det snabbt och enkelt att logga in och numera behöver du oftast inte ens fylla i personnummer först.
Förutom att använda Bank-ID överallt där det erbjuds kan du använda det för att hindra obehöriga att till exempel ändra din adress hos både Skatteverket och Svensk Adressändring. Kreditupplysningsfirman UC har också en tjänst som spärrar ditt personnummer i två veckor så att det inte går att använda efter identitetsstöld för att exempelvis ta ut lån i ditt namn.

Undvik typiska bedrägeriförsök

Det absolut viktigaste att tänka på med Bank-ID är att aldrig logga in med eller godkänna något med det på uppmaning av någon annan. Ingen bank, kreditkortsutgivare, myndighet eller annan seriös organisation gör det normalt, och skulle det hända med till exempel din egen bank så skulle de inte aktivera det åt dig utan till exempel be dig logga in i din bankapp själv.
Om Bank ID-appen visar ett inloggningsförsök som du inte precis innan själv aktiverade så ska du avbryta. Sedan Bank-ID införde qr-koder för inloggning på känsliga tjänster som banker har telefonbedrägerier för att länsa kontot genom att be offret logga in för att ”kontrollera” något minskat kraftigt. Ett nytt bedrägeriupplägg att se upp för nu är att bedragarna ber dig ta fram bankdosan istället för mobilt Bank-ID, naturligtvis med någon mer eller mindre trovärdig ursäkt om du ifrågasätter varför det ska behövas. Lägg på direkt om någon påstår sig ringa från banken och ber dig logga in eller godkänna något med dosa.
Andra typer av bedrägerier som är vanliga idag är klassiker som ”Nigeriabrev” och olika romansbedrägerier. En nykomling som är på kraftig och skrämmande frammarsch är bedrägerier med AI. Bedragarna använder deepfake-tekniker för att till exempel härma en nära släktings röst och utseende. Nästan alltid går det ut på att ”släktingen” behöver hjälp med pengar och det är bråttom. Självklart kan du inte swisha till deras vanliga nummer heller, utan måste skicka till något anonymt bankkonto utomlands.

Bestäm kodord med släkt och vänner

Om du är orolig över att utsättas för bedrägerier som handlar om att lura dig att skicka pengar eller göra något annat för att hjälpa en släkting eller nära vän i nöd, utan samtidigt vill kunna vara till hjälp om någon verkligen befinner sig i knipa, kan du använda delade hemligheter.
Du och dina släktingar och vänner kan komma överens om kodord, eller kanske en mer lekfull variant som i någon gammal spionrulle. ”Nu blommar persiljan” – ”Och hackspettarna dukar bordet” till exempel (men ta inte det, nu när jag redan har använt det). Det viktiga är att ingen utomstående ska kunna gissa sig till eller ta reda på svaret.

Skulle någon av er senare faktiskt behöva hjälp på distans kan ni försäkra er om att det inte är någon bedragare på andra sidan skärmen, oavsett hur bra AI-systemen blir på att härma röster och ansikten.

Använd virtuella engångskort

Ska du köpa något från en mindre känd butik du inte vet om du kan lita på? Du kan få lite mer trygghet genom att inte använda ditt vanliga betalkort utan någon metod som gör att företaget (eller en hackare som tagit sig in hos det) inte kan dra några pengar igen vid senare tillfälle.

Ett relativt enkelt sätt att åstadkomma det är med virtuella engångskort. Det kan du skaffa hos bland annat Klarna och Revolut och innebär att du får ett kortnummer, utgångsdatum och cvv-kod som vanligt men kortet kan sedan bara användas en gång. Vanligtvis anger du ett maxbelopp på kortet, så företaget inte kan dra mer än utlovat.

Det är ett bra skydd om du vill ta en risk och köpa någon billig pryl på en skum sajt.

Om sajten är ett bedrägeri och försöker dra tusentals kronor fungerar det inte och du slipper lägga timmar på att anmäla till banken och få betalningen hävd. För att inte tala om hur mycket bättre du kommer sova.

Om du inte vill eller kan använda virtuella engångskort kan du använda betalning med Paypal eller Klarna istället, eftersom företaget du handlar hos i så fall inte får reda på några kortuppgifter och måste tala om för betalningstjänsten vad beloppet är. Företaget kan inte heller använda några lagrade uppgifter för att utföra fler betalningar vid ett senare tillfälle.

Använd fejkade svar på säkerhetsfrågor

Jag vill också passa på att upprepa ett tips från min guide till kontosäkerhet.
En del sajter vill att du fyller i säkerhetsfrågor som vad din mamma hette innan hon gifte sig. Fyll i påhittade svar istället för äkta!

Förutom att det följer det första tipset om att inte dela några personuppgifter i onödan minskar det risken att få kontot kapat, då hackare inte kan luska ut vad svaren är utifrån verkliga uppgifter om dig.

Bestrid falska fakturor och polisanmäl bedrägeriförsök

Har du drabbats av ett bedrägeriförsök eller fått en bluffaktura är det viktigt att du inte är passiv och skickar korrespondensen i papperskorgen.

Felaktiga eller renodlade bluffakturor är det bäst att så snabbt som möjligt bestrida.
Skicka ett brev eller mejl med en kopia av fakturan i fråga och gör klart att du bestrider den och att du inte är betalningsansvarig eftersom du inte har lagt någon beställning (eller vad som passar för just den fakturan, anpassa brevet till den aktuella fakturan).
Det rekommenderar både Polisen och organisationer som Konsumenternas.

Riktiga bluffakturor bör du, precis som bedrägeriförsök, även polisanmäla.
Även om sannolikheten att polisen sättet dit just dessa bedragare är liten hjälper anmälningar till att ge polisen korrekt statistik över den här typen av brottslighet och kan bidra till ökade resurser för att bekämpa problemet.