Bli säkrare på nätet

Seniornet Lidingö
Okt-2023

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. **Se till att dina kortbetalningar är säkra**

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 det.

➢**Lösenordet bör vara någorlunda komplext**

- Det blir svårare för hackaren att knäcka lösenordet om det innehåller många olika typer av symboler, som specialtecken, siffror och stora och små bokstäver.

1.1 Lösenord forts…

➢**Generera lösenordet och spara det i en lösenordshanterare**

- Du kan även välja att generera ett lösenord. Då blir lösenordet helt slumpvis valt och ofta består det av många olika symboler. Ett sådant lösenord är omöjligt att komma ihåg och därför kan du spara det i en lösenordshanterare och lätt logga in via den.
  En mycket bra lösenordshanterare är Bitwarden.

➢**Sätt ihop olika ord till lösenordsfraser**

- Om du inte vill generera ditt lösenord slumpmässigt kan du istället välja att sätta ihop flera olika ord till en fras. Tänk dock på att frasen inte ska vara logisk och orden bör vara så slumpmässiga som möjligt. “tigerköksöartellerimarinbiologlyktstolpe” är ett exempel på det. Undvik också att ha med ord som rör personlig information om dig, som namn på dig, din familj eller ditt husdjur, födelsedatum etc.

Kan ditt lösenord ha hamnat i orätta händer?

Kolla här: https://haveibeenpwned.com/

2. Håll koll på/skydda dina enheter

- Installera aldrig program i onödan och avinstallera de du inte använder. Det är också viktigt att installera nya uppdateringar direkt eftersom det kan finnas säkerhetslösningar i uppdateringarna som fixar eventuella säkerhetshål i programmet.

- Ladda inte heller ned programvara som du blir uppmanad att ladda ned 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. Det är alltså ett viktigt skydd och du bör ha en sådan för att hackare inte ska komma åt din privata information. Microsoft Defender har en brandvägg. Om du är osäker på om den är påslagen, kontakta SNL på handledningen, vi hjälper dig.

- **Använd VPN eller antivirus (eller båda):** Det är bra att ha ett VPN och antivirus installerat på din enhet eftersom att de jobbar för att hålla din enhet säker. Ett antivirusprogram skannar din enhet och tar bort skadlig programvara som trojaner eller spionprogram.
  Med ett VPN krypteras din trafik och du surfar privat.

3. Se upp för bedrägerier

- Om du surfar på nätet är det även viktigt att du känner till vilka bedrägerier som är de vanligaste och hur du ska skydda dig från dem.

- 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.

- **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.

3.2 Se upp för bedrägerier

Hur man identifierar ett smishing-meddelande

Ibland är det ganska lätt att identifiera ett smishing-meddelande, medan det i andra fall är väldigt svårt. Ofta finns det dock ganska många gemensamma nämnare för dessa meddelanden, varav nedanstående är ypperliga exempel:

- **De vill att du ska agera snabbt.**

- **De vill ha något av dig.** Detta kan vara att du ska klicka på en länk, bidra med din personliga information eller föra över pengar.

- **Inkluderade länkar.** Många av dessa meddelanden inkluderar någon typ av länk som du ska klicka på.

  Klicka ALDRIG på länkar som du får via SMS, meddelande, mail eller liknande.

- **Erbjudanden som verkar för bra för att vara sanna.**

3.3 Se upp för bedrägerier

- Det är oftast mycket lättare att få dig att själv lämna ut de uppgifter en bedragare behöver för att kunna stjäla från dig, än att exempelvis hacka din dator eller göra inbrott.

- Att lura dig på det sättet sker genom så kallad ”social ingenjörskonst”. Det handlar helt enkelt om att veta vilka knappar man ska trycka på för att få dig att frivilligt lämna ut information.

- Uppgiftsfisket kan ske på en rad olika sätt – till exempel genom mejl, sms eller telefonsamtal. Grundläggande är att bedragaren låtsas vara någon du skulle kunna tänka dig att lämna ut den eftersökta informationen till.

3.4 Phishing

- Nätfiske, på engelska phishing (uttalas ’fishing’), är ett samlingsbegrepp för de olika försök till uppgiftsfiske som sker över internet.

- Det vanligast nätfiskeförsöket sker via ett mejl, som utger sig från att vara från ett företag du är kund hos. Du uppmanas besöka en hemsida för att uppdatera dina uppgifter. Sajten är i sin tur en skickligt utförd kopia av det riktiga företagets webbplats. Bedragaren skickar sitt mejl till alla e-postadresser denne kommer över. I det slumpvisa urvalet träffar alltid några mejl rätt.

- Nätfiskeförsök kan till exempel utge sig vara från banker eller betaltjänster som påstår att ditt konto är utsatt för bedrägeri och ber dig verifiera inloggningsuppgifter eller streamingtjänster som varnar för att tjänsten avslutas om du inte uppdaterar dina kortuppgifter, eller från Skatteverket som vill ha dina uppgifter för att betala tillbaka skatt.

3.4.1. Phishing

- Ytterligare en variant är att locka med hög ersättning om du svarar på en kundnöjdhetsundersökning.
- Det är också vanligt att bedragaren fiskar efter inloggningsuppgifter till ditt e-postkonto, eller dina konton i sociala medier. Dessa kan sedan användas i andra bedrägerier som drabbar dina vänner och bekanta.
- Misstänker du att ett mejl är ett nätfiskeförsök ska du aldrig klicka på länkar i det, aldrig öppna det så att bilder laddas ned, och aldrig öppna bifogade filer. Gör du det riskerar du att bekräfta för bedragaren att din e-postadress är aktiv och därmed värd att sälja eller utsätta för fler bedrägeriförsök. Öppnar du bilagor eller besöker bedragarens webbplats riskerar du att skadlig kod installeras på din dator.
- Är du osäker på om mejlet är ett bedrägeriförsök ska du aldrig använda uppgifterna i det för att kontakta företaget det utger sig komma från. Dessa kan vara falska. Skriv i stället webbadressen ur minnet, eller slå upp telefonnumret i nätkatalogen.

https://internetstiftelsen.se/guide/skydda-dig-mot-bedragare/bedragerier-pa-natet/

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. För att vara säker är det därför bättre att berätta så lite som möjligt om ditt privatliv på sociala medier och se till att vara så privat som möjligt. Det må vara svårt i den digitala eran, men det minskar risken att drabbas av cyberattacker eller liknande.

Om du har barn bör du även informera dem om hur de ska bete sig och om säkerhet på nätet. Många barn förstår inte vad som är farligt och inte och därför måste du som förälder informera dem om hur de ska förhålla sig till internet och hur säkerheten på nätet fungerar.

7. Se till att dina kortbetalningar är säkra

Att betala med kort på nätet kan vara något av de osäkraste du kan göra online eftersom du självmant ger ifrån dig väldigt privata uppgifter.

Om du väljer att göra ett kortköp är det viktigt att du bara handlar på sidor som erbjuder 3D Secure. Det innebär att det krävs ett godkännande från BankID utöver dina kortuppgifter för att få handla på sidan. Men det är viktigt att inte bara lita på det utan också se till så att sidan är säker i övrigt. T.ex. att den har en säker och krypterad anslutning.

Om du väljer att handla med kort på nätet kan det även vara en god idé att enbart handla med ett specifikt kort på nätet.
Kortet bör inte vara ett kreditkort eller kopplat till ditt lönekonto. Då håller du både alla internetköp samlade på ett och samma kort och minskar den ekonomiska risken. Om du inte har ett sådant kort så stäng alltid kortet du handlar med för internetköp när du handlat färdigt, då blir det omöjligt för en hackare att använda kortet på nätet.

På många hemsidor kommer det även upp en fråga om du vill spara kortet för framtida köp. Välj alltid nej på det.
Det är bättre att inte ha ditt kort sparat alls.

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

Publicerad 31 mars 2023

Att bedragare ringer upp främst äldre människor, utger sig för att vara ett barnbarn och kräver 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.

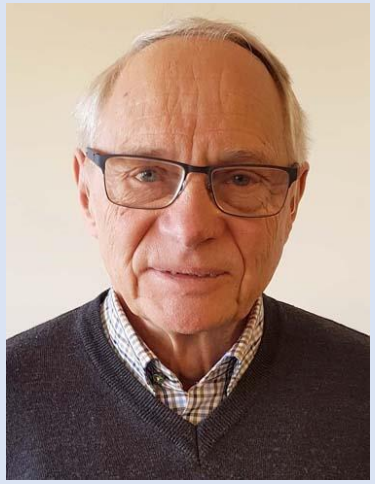
Hur många sekunder långt klipp räcker för att kunna klona någons röst? Och hur bra funkar det egentligen på svenska?

Åtgärd:
RING och kontrollera

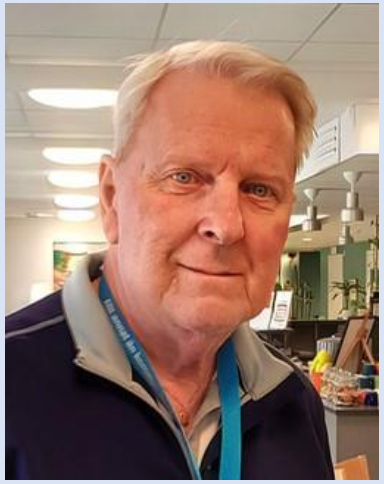
Artificiell Intelligens (AI)
är inte smartare
än den data
vi människor matar den med.

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

Tack för oss!



Jan Ekberg



Stefan Ternvald