SeniorNet Huddinge

Säkerhet på nätet
2020-01-09

1

Vi måste genomskåda osanningarna

- Idag är alla dagar som första april. På sociala medier sprids information som är falsk och ibland medvetet lögnaktig. Nu efterlyser forskaren Emma Frans en folkbildningskampanj för att inte fler ska låta sig luras av falska nyheter och påståenden.
- Inte bara sociala medier, du kan bli uppringd eller kontaktad på annat sätt av personer som försöker lura av dig pengar eller värdesaker.

Insidan DN 2019-01-08

2

SeniorNetHuddinge

TÄNK SÄKERT!

Det är lätt hänt att värdefull information hamnar i fel händer. Det tråkiga är att konsekvenserna kan bli allvarliga.

- **Ingen** som är seriös ringer upp dig och ber dig att använda e-legitimationen inte för något syfte. Avsluta samtalet direkt, oavsett vad det handlar om.
- Genom att tänka på hur du agerar på nätet och genom enkla åtgärder så kommer du långt i vårt uppkopplade liv med smarta saker.
- Tänk också på att uppgradera operativsystem och virusprogram regelbundet

3

SeniorNetHuddinge

Dagens innehåll

- Bedrägerier – Någon ringer upp (Vishing)
- Investeringsbedrägeri
- Hur känner man igen bluffarna?
- Falska mejl (Phishing)
- Bedrägeri via SMS (Smishing)
- Bluffakturor
- Romansbedrägeri
- Skydda dina pengar
- ID stöld
- Digital brevlåda
- Länkar

4

SeniorNetHuddinge

Vad kan man råka ut för

Numera är det vanligare att bedragarna ”hackar” sig in i din hjärna. Dom låter trovärdiga och vederhäftiga, men …

- Du blir uppringd av ”polisen” eller ”banken”, målet är att lura dig att logga in på ”din bank” med ditt BankId för att komma åt dina pengar.

Om du blir uppringd av ”polis” eller ”bank” eller någon annan som uppmanar dig att loga in med BankID – Lägg på, avsluta samtalet och kontakta polisen

- Det har också förekommit att ”polisen” ringt och sagt att man ska plocka fram smycken och kort och att det kommer en uniformerad polis …. – **Plocka inte fram något! Avsluta samtalet direkt! Om/när en ”uniformerad polis” kommer; begär att få se fotolegitimation!**

5

SeniorNetHuddinge

Falska finansbolag ringer upp om fejkade lån – sen länsas kontot

- De lurade blir uppringda av falska finansbolag som meddelar att ett lån de aldrig sökt är beviljat.
- När kunden påtalar att något måste ha blivit fel erbjuder sig personen från finansbolaget som egentligen är en bedragare att koppla samtalet till den uppringda personens bank. Efter att ha kopplats till det som uppfattas som banken uppmanas den uppringda att knappa in uppgifter och logga in på sitt bank ID.
- Detta öppnar upp för bedragarna att länsa kontona.

Källa: https://www.svt.se/nyheter/lokalt/vasternorrland/polisen-varnar-for-ny-bedrageriform-lanet-man-aldrig-ansokt-om-beviljat-sen-lansas-kontot

6

Pensionsmyndigheten utnyttjas för bedrägerier

Vad händer?

- Sponsrade inlägg på Facebook lockar med saker som bostadstillägg eller högre garantipension – men är bara ute efter nya pensionärer att lura
- Om man klickar på länken till sitens ”räknekalkyl” (el. likn.) fungerar den inte men sedan ringer någon upp och det är då bedrägeriet börjar.
- Eller också finns en steg-för-steg guide där man fyller i sina uppgifter, men i slutändan behövs ett personligt samtal. Det är också där bedrägeriet börjar

Detta är bara två exempel, det finns många sätt så det gäller att vara vaksam och misstänksam.

Källa: DN Ekonomi 2019-11-12

Från DN Ekonomi 2019-11-19

Upp till en miljon svenskar kan ha nåtts av bitcoin-bedragarna. Detta är ett investerings-bedrägeri. De kändisar som förekommer i denna typ av annonser är inte vidtalade och inte medvetna om att deras namn utnyttjas.

Bluffannonser som använder sig av H&M:s ordförande Stefan Persson och TV4:s "Nyhetsmorgon". Foto: Skärmdumpar

SeniorNetHuddinge

Var skeptisk! Satsa aldrig pengar på något du inte vet säkert vad det är eller bolag du inte känner till!

9

SeniorNetHuddinge

Gör en polisanmälan!

Anmäl till **polisen**

Gör en polisanmälan genom att **ringa** 114 14 eller gå till en polisstation . Det kan du göra oavsett om du hunnit betala in pengar, redan vet att du förlorat pengarna eller endast är utsatt för ett försök till **bedrägeri**.

Om du har drabbats – Finansinspektionen
https://www.fi.se › konsumentskydd › investeringsbedragerier › om-du-har-...

Beroende på hur långt du kommit med att göra en investering i något som du misstänker är ett bedrägeri har du olika handlingsmöjligheter:

- Om du ännu inte gjort någon affär är ännu ingen skada skedd och du kan bara avbryta kontakten.
- Har du precis skickat iväg en betalning via din bank kan du försöka stoppa den. Kontakta din bank omgående.

10

SeniorNetHuddinge

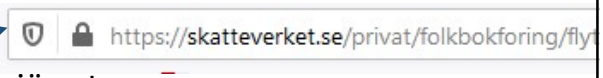
Råd från banken

- Använd aldrig din kortläsare eller Mobilt BankID på uppmaning av någon annan oavsett orsak.
- Logga aldrig in på Internet- eller Mobilbanken på uppmaning av någon annan.
- Lär dig helst bankkoderna utantill och lämna aldrig ut kort eller några som helst uppgifter om ditt kort, exempelvis kortnummer, CVC/CVV- eller PIN-kod eller de svarskoder som genereras av din kortläsare.

Du skulle väl inte heller lämna ifrån dig dina hemnycklar?

SeniorNetHuddinge

Hur kan man då känna igen bluffarna?



1. Kolla alltid att webbadressen ser seriös ut.
2. Kontrollera att påståenden om samarbeten med välkända företag eller myndigheter stämmer.
3. Ett annat varningstecken kan vara att sidan saknar kontaktuppgifter – telefonnummer och/eller mejladress
4. Om organisationen uppger en postadress, kontrollera att det verkligen finns ett kontor på adressen
5. Sök efter organisationen i Finansinspektionens företagsregister. Där listas alla företag och personer med tillstånd att erbjuda finansiella tjänster i Sverige.

Källa: DN Ekonomi 2019-11-12

SeniorNetHuddinge

Falska mejl

Det förekommer ett antal olika falska mejl

- Ett mejl som ser ut att vara skickat från din egen mejladress. Men avsändaradress går att fejka så betala inga pengar.
- Ett mejl som påstår att dom filmat dig när du besökt en vuxenwebbplats. – Om du verkligen besökt en sådan plats och tror att det kan finnas en film du inte vill ska spridas, be om bevis.
- Det förekommer också mejl som är en kontaktförfrågan. Man bör inte svara på en sådan förfrågan.
- Mejl om att du har vunnit stora pengar.
- Mejl från vänner som säger sig sitta fast någonstans i världen utan pengar. (Be den/dom genast byta lösenord på sitt mejlkonto!) – Är du osäker kontakta vännen och kontrollera om detta verkligen stämmer.
- Fler exempel?

SeniorNetHuddinge

Falska mejl – ett exempel!

Jag är en hacker som har tillgång till ditt operativsystem.
Jag har också full tillgång till ditt konto.
Jag har sett dig i några månader nu.
Faktum är att du smittades av skadlig programvara via en vuxenwebbplats som du besökte.

Om du inte är bekant med det kommer jag att förklara.
Trojan Virus ger mig full åtkomst och kontroll över en dator eller annan enhet.
Det betyder att jag kan se allt på din skärm, sätta på kameran och mikrofonen, men du vet inte om det.

Jag har också tillgång till alla dina kontakter och all din korrespondens.

Varför ditt antivirus inte upptäckte skadlig programvara?
Svar: Min malware använder drivrutinen, jag uppdaterar dess signaturer var fjärde timme så att ditt antivirus är tyst.

Jag gjorde en video som visar hur du tillfredsställer dig i den vänstra halvan av skärmen, och i den högra halvan ser du videon som du tittade på.
Med ett musklick kan jag skicka den här videon till alla dina e-postmeddelanden och kontakter på sociala nätverk.
Jag kan också publicera åtkomst till alla dina e-postkorrespondenser och meddelanden som du använder.
Men oroa dig inte för mycket, det finns ett sätt vi kan åtgärda denna sekretessproblem.
Allt vi behöver är en Bitcoin-betalning på **£8,960.00 GBP**, vilket jag tror är ett rimligt pris med tanke på omständigheterna.

SeniorNetHuddinge

Falska mejl – ett exempel till

Jag hoppas att detta når dig i tid. Jag gjorde en resa till Donetsk, Ukraina och min väska blev stulen med mitt internationella pass och mina kreditkort inuti. Ambassaden är villig att hjälpa mig att ta ett flyg utan mitt pass, jag behöver bara betala för biljetten och hotellräkningarna. Till min förfäran kan jag inte få tillgång till mina pengar utan mitt kreditkort och kontakt med min bank, men de behöver mer tid för att kunna ge mig ett nytt kort. I den här olyckliga situationen tänkte jag fråga om ett lån som jag kan betala tillbaka så fort jag kommer tillbaka. Jag behöver verkligen vara med på nästa flyg. Jag behöver 19,587 kr. Berätta om du kan hjälpa mig genom Ria Penningöverföring eftersom det är det bästa alternativet jag har.

15

SeniorNetHuddinge

Bedrägeri via SMS

Bedragare kan också kontakta dig via SMS. Syftet är ofta att få dig att klicka på en länk och fylla i personliga uppgifter som bedragarna sen kan använda.

Tips:

- Klicka inte på länkar från okända avsändare.
- Lämna inte ifrån dig ”hemlig”(dvs koder och annan) information.

16

SeniorNetHuddinge

Bluffakturor

En bluffaktura skickas ofta via mejl och är ett krav på betalning för en vara eller tjänst som du aldrig har beställt eller fått levererad. Det kan också hända att en säljare, via telefon, försöker hävda att ni har ingått ett avtal och kräver dig på pengar.

Tips:

- Är fakturan rimlig? Har vi köpt den här varan/tjänsten?
- Står det någonstans att fakturan egentligen är ett erbjudande av något slag?
- Hävdas att du ingått ett avtal via telefon – be om bevis.
- Om du har haft affärer med företaget: Är bank- eller plusgironumret samma som förra gången?

17

SeniorNetHuddinge

Romansbedrägeri

Kärlek eller Romans-bedrägerier inleds vanligtvis på nätet, till exempel på Facebook eller dejtingsida. Inte sällan är bedragaren ”en militär på uppdrag utomlands”.

Bedragaren kontaktar en person och man börjar chatta, byta e-post och prata i telefon / Skype.

Den här kontakten kan ofta pågå i månader och bedragaren bedyrar snabbt sin kärlek och pratar om en gemensam framtid.

Efter ett tag, börjar bedragaren att begära pengar under olika förevändningar, till exempel sjukhuskostnader och resor.

18

SeniorNetHuddinge

Romansbedrägeri – Tips

- Se upp för "soldater" och kvinnor som ber dig skicka pengar
- Kontrollera personens uppgifter från siten där kontakten togs – det går ofta att se att personen inte är verklig (på vänlista, inläggshistorik, …)
- Räkna med att personen först har arbetat för att vinna ditt förtroende
- Skicka aldrig pengar till någon som ber om det via internet.
- Om du har blivit lurad, rapportera det. *Du är inte ensam*.

19

SeniorNetHuddinge

Säkerhet på nätet

Om du inte har köpt en lott på nätet, har du inte vunnit något heller.

Om någon vill ha ditt kort och inloggningsuppgifter – tro inte på det. Man behöver inte kort och inloggning för att sätta in pengar!

Ingen bank frågar efter ditt kontonummer, de har det ju redan.

Om du får epost från någon du inte vet vem det är, klicka aldrig på några länkar i mailet.

Källa: e-legitimation.se

20

SeniorNetHuddinge

Skydda dina pengar

Använd e-legitimation

- E-legitimation en personlig elektronisk ID-handling som du använder för att legitimera dig och godkänna handlingar på Internet(motsvarar ditt ID-kort eller körkort).

Källa: e-legitimation.se

SeniorNetHuddinge

Din e-legitimation är en värdehandling

- Din e-legitimation är en personlig id-handling, precis lika mycket som pass, körkort och id-kort.
- Du ansvarar för allt som din e-legitimation används till och du får inte använda den till att släppa in någon annan (alltså logga inte in någonstans på någon annans uppmaning)
- Låt inte någon annan använda din e-legitimationen (lika lite som du låter någon använda dina andra legitimationshandlingar)
- Se till att mobiltelefonen, surfplattan eller datorn där du har e-legitimationen är säkra och att du spärrar e-legitimationen om du tror att någon annan har kommit åt den.
- Välj en kod som är svår att gissa sig till.
- Berätta inte koden för någon, inte ens om det är en familjemedlem.

SeniorNetHuddinge

Din legitimation är personlig!

- Det blir allt vanligare att personer och företag vill ”hjälpa dig att samla information om dig på ett ställe”. Till exempel kan det på deras webbplats stå ”Legitimera dig så att vi kan hämta din information”. **Gör inte det!**
- Både du och de personer eller företag som du släpper in kan göra sig skyldiga till ett brott som kallas missbruk av urkund.
- Tänk på att om du loggar in åt någon annan, genom att du använder din e-legitimation – till exempel BankID, kan dessa företag eller personer t.ex. flytta över pengar från dina konton och enkelt hämta alla uppgifter om dig från andra webbplatser.

SeniorNetHuddinge

Att tänka på

- Lämna **aldrig** ut lösenord och koder! – Det finns ingen som av legitima skäl frågar efter det.
- Var restriktiv med att lämna ut kontonummer. Lämna bara till mottagare du litar på. (*Banken har ju redan dina*.)
- Logga aldrig in med BankId på någon annans uppmaning..
- Ha olika lösenord.
  - Ett säkrare till bankid, e-posten och till ställen som rör din ekonomi.
  - Till Aftonbladet, DN och andra informationskanaler kan man ha samma (eller liknande) lösenord.

SeniorNetHuddinge

ID kapning, identitetsintrång, identitetsstöld

… är när någon obehörig använder din legitimation, dina lösenord, ditt personnummer eller ditt mobila BankID. – Det är en form av bedrägeri.

- 2019 ökade antalet försök till ID-kapningar

Om du upptäcker att någon obehörig har ändrat din adress?

- Kontakta Skatteupplysningen på telefon 0771-567 567 för att få hjälp. Du ska även anmäla det till Polisen så att du kan skicka en kopia på anmälan till Skatteverket.

SeniorNetHuddinge

Skatteverkets tips för att skydda dig

- Spärra ändringar av din adress via blankett så att du bara kan ändra den med hjälp av BankID. Det gör du i Skatteverkets tjänst ”Spärra obehörig adressändring”.
- Komplettera med adresslåset så skyddar du dig mot att någon obehörig adressändrar, lagrar eller eftersänder din post. Det gör du i tjänsten ”Adresslåset” som finns hos Svensk adressändring.
- Skaffa en digital brevlåda så du får ett meddelande om din folkbokföringsadress ändras.

Källa: https://skatteverket.se/privat/folkbokforing/identitetsintrang.4.35c34f651660af3747c3178.html

SeniorNetHuddinge

Mer att tänka på

Tips

- Använd BankId där det erbjuds
- Använd så ofta som möjligt unika lösenord
- Använd starka lösenord som innehåller små och stora bokstäver, siffror och specialtecken. Aldrig ord som ingår i ordlistan
- Använd tvåstegsautentisering (t.ex. ett lösenord plus en engångskod som skickas med SMS). Det går då till så, att efter att man har matat in sitt lösenord så får man (automatiskt) ett textmeddelande med en kort teckenserie att mata in. Nyttan med det här är att det är mycket svårare för någon att komma åt ens konto. För att lyckas bryta sig in måste de komma åt både vårt lösenord och vår mobiltelefon.
- Ha olika lösenord.
  - Ett säkrare till bankid, e-posten och till ställen som rör din ekonomi.
  - Till Aftonbladet, DN och andra informationskanaler kan man ha enklare lösenord.

SeniorNetHuddinge

Mer att tänka på

Håll bedragarna borta

- Det är vanligt att bedragare hör av sig och säger att de representerar någon som man litar på, exempelvis Polisen eller banken. De kan till exempel säga att det har hänt något akut och att du genast måste logga in med din e-legitimation. Om du gör det finns det risk för att du släpper in dem (i stället för dig själv) så att de kan komma åt dina pengar eller känsliga uppgifter.
- Använd aldrig ditt e-id om du blir uppringd
- Ingen som är seriös ringer upp dig och ber om dina koder eller säger att du ska använda e-legitimationen. Avsluta samtalet direkt om det händer, oavsett vad det handlar om.
- Låt inte någon annan använda din e-legitimation
- Du får inte använda din e-legitimation för att ge någon annan tillgång till dina uppgifter. Till exempel kan ett företag skriva "Legitimera dig så att vi kan hämta din information". Gör inte det. Du har ingen kontroll på vad de samlar in och både de och du begår kanske ett brott.

SeniorNetHuddinge

Digital brevlåda

Skaffa en digital brevlåda så får du post från myndigheter digitalt i stället för på papper. Till skillnad från vanliga mejl är den digitala brevlådan säker eftersom inloggning sker med e-legitimation, till exempel Mobilt BankID. En digital brevlåda är gratis, miljövänlig och tillgänglig var du än är.

SeniorNetHuddinge

Digital brevlåda

Kivra

Digimail

E-Boks

Min myndighetspost

Gemensamt för dessa digitala brevlådor är att man loggar in med Mobilt bankid.

SeniorNetHuddinge

Om vi har tid kvar – lite om säkerhet

- En liten film om avtal via SMS (14 dagar ångerrätt gäller fortfarande): https://www.youtube.com/watch?v=a9oSP409R58
- En lite längre film om bedrägeri via BankID: https://www.youtube.com/watch?v=A3hBZnxdg0s
- En liten film med bra tips Bedrägerier på internet: https://www.youtube.com/watch?v=53OxsoJFV-Y
- En liten film om hur du skyddar dig https://www.youtube.com/watch?v=qhPCXn2c4c4

SeniorNetHuddinge

Presentation om BankID och digitala brevlådor

Här är länk som ger dig tips som ger dig tips

- om hur du installerar Mobilt BankID
- Hur du skaffar dig digital brevlåda

Det är en presentation från Öppet Hus 2019-10-10:

https://huddinge.seniornet.se/wp-content/uploads/sites/38/2018/03/BankID-o-Dig-brevl%C3%A5dor-2019-10-10.pdf

SeniorNetHuddinge

Länkar

Internetkunskap från Internetstiftelsen: https://internetkunskap.se/

Webbplats för Myndigheten för digital förvaltning: https://www.digg.se/

Checklistor för olika händelser som har med säkerhet att göra finns på DinSäkerhet.se: https://www.dinsakerhet.se/checklistor/?category=9

Kolla med din bank. Många banker har sidor som ger tips och råd.

På seniornet Sweden under studiematerial:
https://seniornet.se/studiematerial/sakerhet/

I kampanjen "Tänk säkert" får du tips om hur du kan använda internet på ett säkrare sätt https://www.dinsakerhet.se/tank-sakert
https://www.dinsakerhet.se/mediagalleri/?category=9