SeniorNetHuddinge

SeniorNet 2019-03-20

Säkerhet på nätet

SeniorNetHuddinge

Säkerhet på nätet

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

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

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

Källa: e-legitimation.se

SeniorNetHuddinge

Vad kan man råka ut för

Nätfiske och den okända avsändaren.

Virus, trojaner och maskar

Trådlösa nätverk

E-post är som vykort

Skydda dina pengar

Källa: e-legitimation.se

Surfa säkert

Skanna webbsidor innan du öppnar dem
Säkerhetsföretaget Trend Micro har gjort en smidig webbtjänst som kontrollerar webbsidor direkt.
Skriv in adressen till webbsidan och klicka på **Check Now**, så får du direkt veta om webbsidan är farlig, säker eller misstänkt.

Länk till hemsidan :

https://global.sitesafety.trendmicro.com/

Källa: e-legitimation.se

Nätfiske

På senare år har dock många nätfiskare blivit mer sofistikerade. Framförallt de phishing-mejl som forsöker komma över inloggningsuppgifter till banker har blivit svårare att skilja från äkta vara. Genom att använda logotyper, text och bilder stulna från bankens verkliga webbplats går det att få till mejl som ser ut att vara äkta. Inte sällan ber avsändaren dig logga in för att bekräfta exempelvis din adress, eller installera en säkerhetsuppdatering. I själva verket smusslas dina inloggningsuppgifter undan och används sedan av angriparen för att länsa ditt konto

Källa: [e-legitimation.se]

SeniorNetHuddinge

Telia – Varning för bluffmejl och SMS

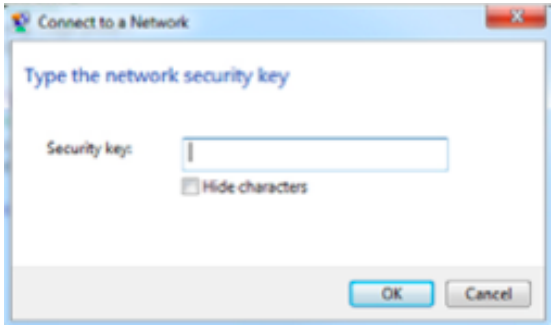
- Har du fått ett mejl eller sms som ber dig att bekräfta en återbetalning eller ange kontouppgifter? Är Telia den påstådda avsändaren? Då handlar det om ett bluffmejl. **Telia skickar aldrig ut fakturor eller återbetalningsärenden via mejl.** Skulle du får en faktura eller ett besked om återbetalning i ett mejl som har Telia som påstådd avsändare, ska du radera det.

- Finns fakturan inte på Mitt Telia, är det en bluff.
- Tänk på att Telia och Telias samarbetspartners aldrig begär att våra kunder ska lämna ifrån sig sina uppgifter via e-post eller sms. Det är viktigt att inte låta sig luras, utskicken kan se förhållandevis professionella ut, i vårt fall med Telias logotyp och Telia-liknande e-postadresser som avsändare.

Trådlösa nätverk

I huvudsak behövs två sorters skydd för trådlösa nätverk: Dels ska nätverket förses med lösenord och dels ska det krypteras.

Så här ser inloggningen till ett nätverk som skyddas med WPA2- kryptering ut på en Mac



Och så här ser inloggningen till ett nätverk som skyddas med WPA2- kryptering ut på en PC.

E-post är som vykort

Att skicka ett mejl kan mest av allt liknas vid att skicka ett vykort – utan kuvert – på posten. Faktum är att vykort förmodligen är ett bättre val om du har hemligheter att förmedla i text, för de passerar betydligt färre snokande ögon än ett genomsnittligt mejl.

Källa: [e-legitimation.se]

SeniorNetHuddinge

Främsta tecknen på bluffmejl
Se upp om du får e-post om utbetalning av pengar, brådskande meddelanden och dokument.

Varningsklockorna bör ringa för fullt om du får e-post med ämnen som handlar om pengar, efterfrågningar, hjälp eller dokument.
Dessa fyra typer av ämnen är nämligen de som kriminella oftast använder när de försöker lura av oss personlig information eller installera skadliga program i datorn. Det visar en undersökning från säkerhetsföretaget Proofpoint efter att de har gått igenom miljontals med bluffmejl som har skickats under årets första sex månader.
18 procent av den falska e-posten handlar om utbetalningar från exempelvis Skatteverket eller betalningstjänsten PayPal.
I hela nio av tio fall försöker avsändaren se ut att vara en välkänd källa, till exempel Skatteverket. Källa: e-legitimation.se

Skydda dig och ditt privatliv på internet

Kontrollera inställningarna på sociala medier
Du bör noggrant gå igenom alla inställningar för sekretess och privatliv på sociala medier som Facebook, Instagram och andra sociala medier som du använder.
Om du använder standardinställningarna delar du med dig av betydligt mycket mer information än du kanske tror och vill göra.

Skydda telefonnummer och e-postadress
Att lägga ut sitt telefonnummer och sin e-postadress på olika webbplatser kan resultera i olidliga mängder telefonsamtal från allt från försäljare till bedragare, och en inbox full med skräppost. Var därför noga med att i största möjliga mån aldrig lägga ut sådan information där obehöriga kan se dem.
Eventuellt kan du skapa ett extra e-postkonto som du enbart använder för nyhetsbrev, reklam och liknande.

Skydda dig och ditt privatliv på internet

Använd kraftfulla lösenord
Varje år publiceras listor med de populäraste, och därmed också de mest osäkra, lösenorden. Och det finns nästan ingen gräns för hur lata och fantasilösa användare det finns.
Du skyddar dina konton - och därmed även informationen på kontona - med unika lösenord som är minst tolv tecken långa men gärna ännu längre.

Några av de vanligaste lösenorden

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom

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

E-legitimation / BankID

Vad är e-legitimation

- E-legitimation behövs för att, över internet, enkelt och säkert ha kontakt med myndigheter, organisationer och företag
- E-legitimation kan i många fall användas för att ingå avtal och signera handlingar
- BankID är en vanlig typ av e-legitimation

Källa: e-legitimation.se

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.

SeniorNetHuddinge

E-legitimation / BankID

- Vad kan man göra med e-legitimation?
  - Deklarera
  - Anmäla flyttning
  - Inloggning på Pensionsmyndigheten
  - Adressändring
  - ”Mina vårdkontakter”
  - M.m. (listan tenderar att bli längre och längre)
- BankID kan man ladda ner genom sin bank
- BankID laddas på egen dator, surfplatta och/eller mobiltelefon.
- Telia E-legitimation kan man få via Skatteverket och Skatteverkets ID-kort (kräver också en kortläsare)

Källa: e-legitimation.se

BankID

- Du beställer BankID via din Internetbank. Vid din beställning kommer du att installera BankID säkerhetsprogram om du inte redan har det installerat.
- Hur du beställer ett BankID skiljer sig åt mellan olika banker. Hos vissa banker krävs ett personligt besök på bankkontoret där du legitimerar dig med godkänd ID-handling, medan du hos andra kan logga in på din Internetbank och beställa ditt BankID direkt.

Läs mer på: support.bankid.com

SeniorNetHuddinge

BankId säkerhetsapp

BankId säkerhetsprogram eller säkerhetsapp är ett program som du måste ha i din dator eller mobila enhet för att kunna beställa och använda BankId. BankId säkerhetsprogram kan du installera från install.bankid.com , medan du hämtar BankId säkerhetsapp från App Store , Google Play-butiken respektive Microsoft-store , beroende på vilken typ av mobil enhet du har.

Mobilt BankID

För att komma igång med mobilt BankID behöver du skriva under ett avtal på internetbanken, ladda ner BankID-appen till din telefon och få en aktiveringskod.

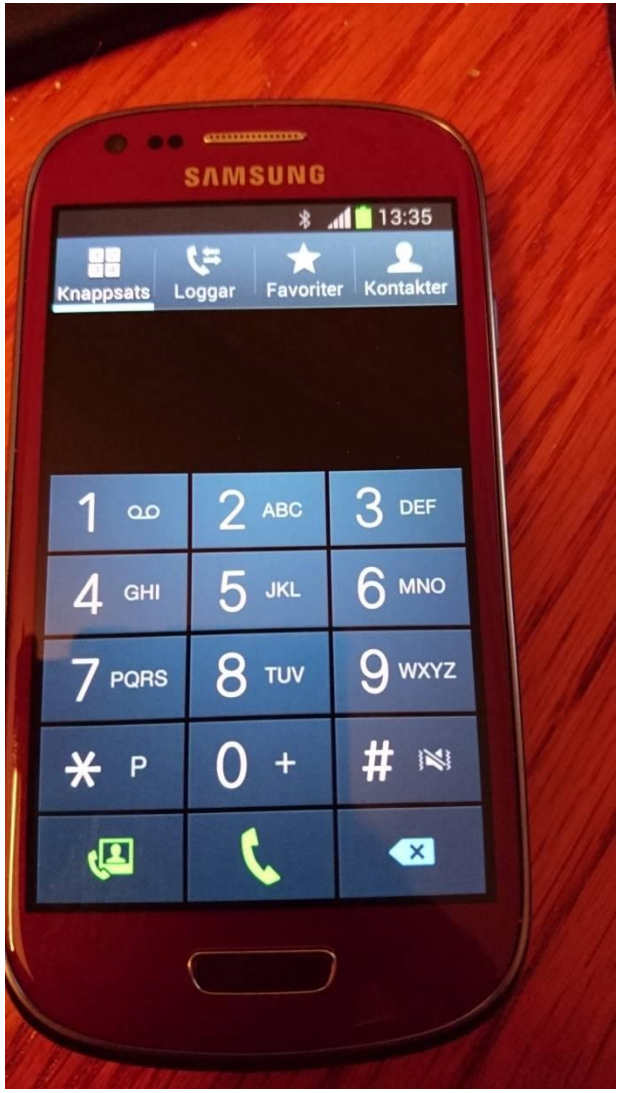
1. Ladda ner och installera BankID säkerhetsapp på den enhet där du vill ha ditt Mobila BankId. Beroende på vilken enhet du har laddar nu ner från App Store, Google Play eller Windows Store (länkar till resp. webbplats hittar du på din banks webbplats eller på BankID:s webbplats)

Mobilt BankID

2. Beställ Mobilt BankId via din bank
   a) logga in på banken som vanligt
   b) någonstans finns att välja att ansöka om Mobilt BankID.
   c) Notera aktiveringskoden du ser på skärmen
3. Aktivera Mobilt BankId.
   a) Öppna BankId appen på din enhet och klicka på Hämta BankID
   b) skriv in ditt person-nummer och aktiveringskoden.
   c) Välj en ny säkerhets-kod 6-8 siffror
      (det är bara du som har din säkerhetskod, glömmer du den får du ladda nytt Mobilt BankID)

Tips för säkerhetskod till Mobilt BankID

- 6-8 siffror kan vara svårt att komma ihåg, eftersom man inte kan ta siffror (ex. födelsedata, telefonnummer) som någon kan gissa sig till
- Eftersom knappsatsen på telefonen har både siffror och bokstäver kan man välja ett ord eller namn man kan komma ihåg.
- Exempel: VolvoV70 som blir siffrorna 86586870
- Eller: Missan10 som blir 64772610



2019-03-20

SeniorNetHuddinge

Att använda Mobilt BankID

Första gången du loggar in på Internetbanken med Mobilt BankId behöver du verifiera på samma sätt som du hittills verifierat betalningar på internetbanken.

Det är **inloggning och signering** av betalningarna som skiljer allt annat med räkningarna gör du på samma sätt som med annan inloggning.

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 di*na.)
- 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 lösenord.

SeniorNetHuddinge

Skimning

Skimning är en form av kontokortsbedrägeri där en bedragaren använder en avläsare för att stjäla kortuppgifterna på ett kontokort. Bedragaren kan sedan använda kortuppgifterna till att betala med på internet.

Tekniken som används heter RFID

.

Radio-frequency identification (**RFID**) är en teknik för att läsa information på avstånd från transpondrar och minnen

Det finns en typ av skyddskort som stoppar trådlös skimning. Skyddskortet innehåller en störsändare som stör ut skimningsutrustning och förhindrar avläsning. Det finns även speciella plånböcker i metall som blockerar kommunikationen mellan det kontaktlösa betalkortet och avläsaren. Det finns inget sätt för kortanvändare att skydda sig mot skimning när bedragare har monterat avläsningsutrustning i en kassaterminal.

Skimning

Kreditkortsskydd till plånboken eller handväskan. Blockerar skimming av kreditkorten. Skydda era kort från att bli skimmade. RFID från korten blockeras via störningssignaler. Skyddar kort i en radie av 2,5 cm från rfid-blockeraren. I de flesta fall räcker det alltså med ett sådant här kort i plånboken

Det finns flera olika tillverkare av detta skydd.

Bla Kjell& Co säljer ett kort i tvåpack för 129,90

Länkar

It säkerhet för privatpersoner:
https://www.iis.se/lar-dig-mer/guider/it-sakerhet-for-privatpersoner/

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

https://www.dinsakerhet.se/tank-sakert

https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Nu-startar-Informationssakerhetsmanaden/

https://skatteverket.se/privat/sjalvservice/allaetjanster/tjanster/sparraobehorigadressandring.4.361dc8c15312eff6fd123f5.html(Skatteverket spärra obehörig adressändring)

https://adressandring.se/private/watch (Adresslås

SeniorNetHuddinge

Mer att tänka på

Har ni blivit något klokare?

Tack för idag!