Cybercrime

Mänskliga misstag i en digital värld

Anmälda bedrägeribrott

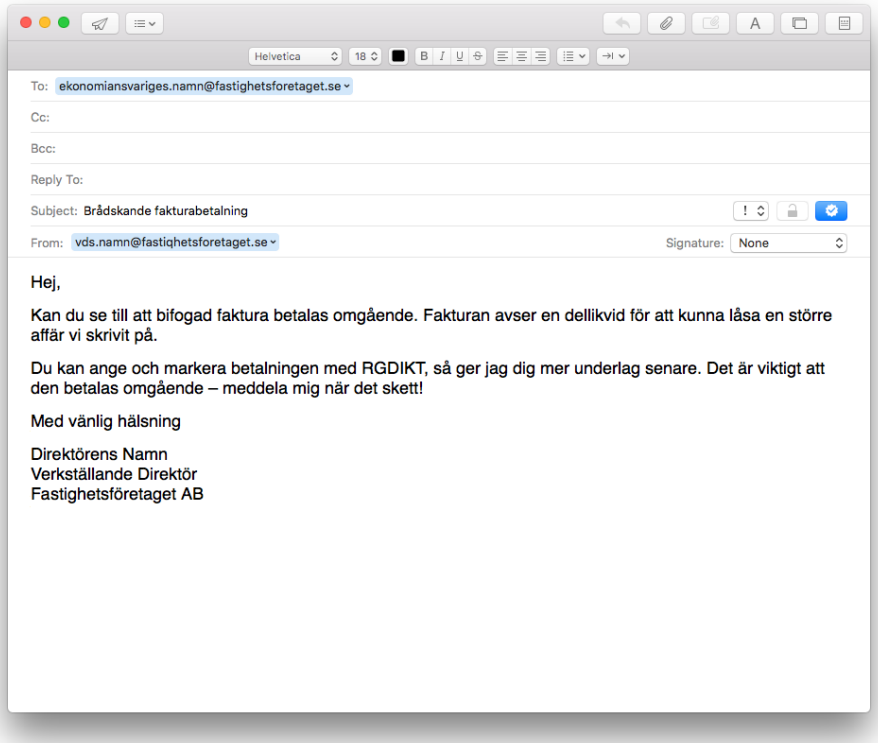
- Förra året anmäldes över 200 000 brott
- Ökningen under 2018 ligger på omkring 25%
- Varje dag anmäls det närmare 700 bedrägeribrott
- 90 % av alla bedrägerier sker idag på nätet
- 60-70% av alla bedrägerier inleds med ett identitetsintrång

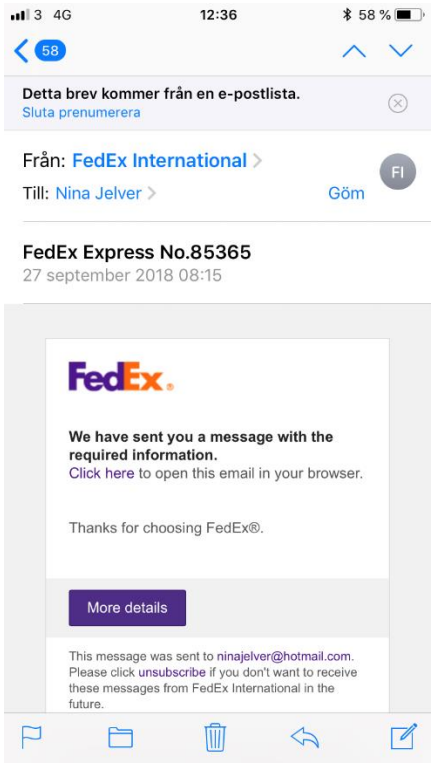
Företagskapningar

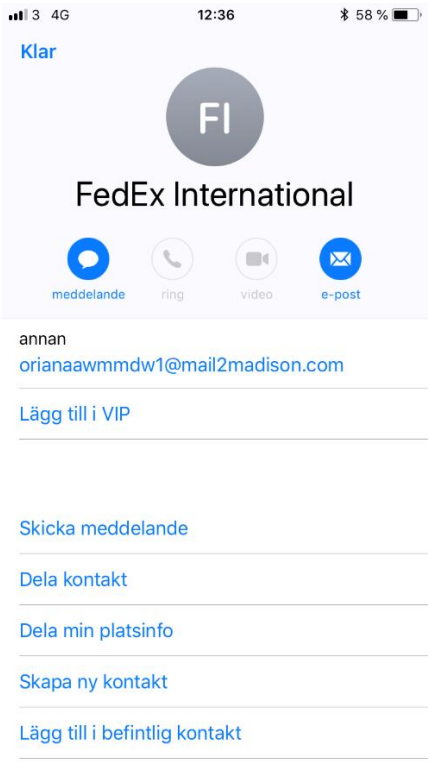
- *Modus 1:* Kapar befintliga företag genom att skicka in anmälan om ändring av styrelse till Bolagsverket. Därefter ansöker man ofta om lån och genomför beställningar av varor i företagets namn.
- *Modus 2:* Registrerar en liknande domän eller använder ”spoofad” mejladress. Skickar därefter mejl från den som brukar ha kontakt med exempelvis banken om att man vill byta utbetalningskonto.
- *Modus 3*: Utger sig via mejl för att vara VD i företaget. Kontaktar ekonomiansvarig och försöker på så sätt få igenom betalningar och överföringar.

Som visningsnamn för en domänadress, tillåter de flesta mailklienter att du skriver en annan e-postadress, så den skickande adressen är pahittad@accountant.com, men det mottagaren ser är istället ulf.kristersson@moderaterna.se och det är först när man hovrar över visningsnamnet med markören som man ser den egentliga mailadressen.

Med andra ord kan man genom fel visningsnamn utge sig för att vara någon man inte är.







- *Modus 5:* Phisingmejl med bifogad trojan. Genom att klicka på den bifogade länken infekteras inte bara mottagaren av mejlet utan mejlet vidarebefordras dessutom till samtliga på dennes kontaktlista.

postnord

Du har lösta paket

Vi har fått ditt paket **CT429586028SE** på **2015/09/22**. Courier kunde inte leverera det här paketet till dig.

Få och skriva ut fraktsedel, och visa den på närmaste postkontor för att få det här paketet.

Få fraktsedel

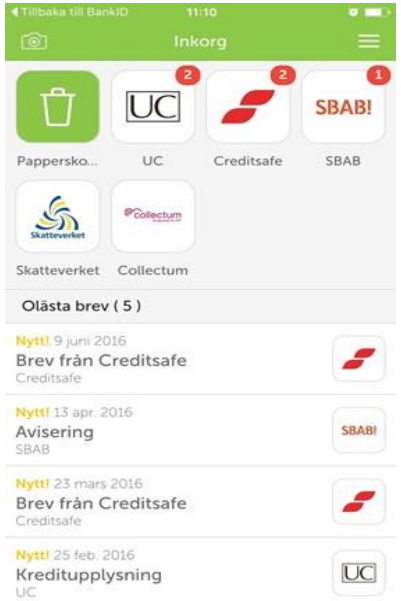
Om paketet inte tas emot inom 20 arbetsdagar, kommer Postnord har rätt att kräva ersättning från dig - 60 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste Postnord kontoret.

Detta är ett automatiskt meddelande. Klicka här för att avregistrera

Varningssignaler

- Meddelande om styrelse- eller adressändring som ni inte har anmält
- Utebliven post, helt eller delvis
- Utebliven leverans av varor
- Kreditupplysning som ni inte känner till
- Orderbekräftelse eller faktura på saker ni inte har beställt

Så minskar du risken för att drabbas



- Använd en digital brevlåda, på så sätt får du ett meddelande direkt från Bolagsverket om det har kommit in en anmälan om ändring av styrelse eller ny adress.
- Det går även bra att ladda ner Bolagsverkets app och följa ditt eget företag.
- Se över vilka rutiner ni har vid anmälan om nytt konto för utbetalning

Om du drabbas…

- Agera snabbt om något verkar konstigt och du misstänker att felaktiga uppgifter blivit registrerade
- Kontakta Bolagsverket som kontrollerar vem som har skickat in anmälan om ändrade uppgifter på telefon 0771-670 670 eller via e-post bolagsverket@bolagsverket.se
- Gör en polisanmälan och skicka en kopia på anmälan till Bolagsverket
- Om felaktiga uppgifter har registrerats ska ni snabbt anmäla de riktiga uppgifterna på verksamt.se
- Kontakta er bank, era leverantörer, kunder och samarbetspartners och berätta vad som har hänt.

Telefonbedrägerier - Vishing

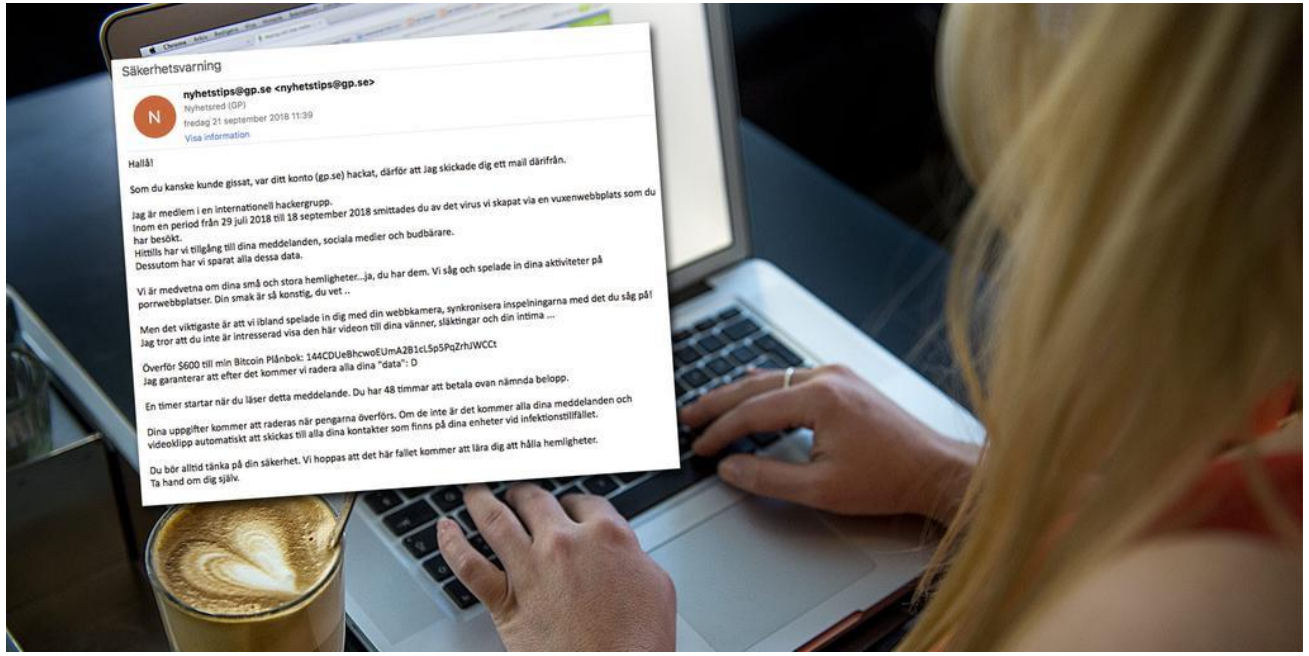
- Gärningspersoner vilseleder, i huvudsak äldre personer att det är ”polisen/banken” som ringer.
- I majoriteten av fallen kommer samtalet från ett ”spoofat” nummer.
- Hela syftet med samtalet är att förmå bankkunden att lämna ut koder till sin elektroniska e-legitimation, bankdosa eller godkänna inloggningar till sitt Mobila BankID.

Så minskar du risken att drabbas

- Lämna aldrig ifrån dig dina svarskoder eller logga in på uppmaning av någon annan.
- Lägg på luren och motring

Ransomware - utpressningsvirus

- Utpressningsvirus, så kallad ransomware, är en skadlig programvara som låser datorer och mobila enheter eller krypterar elektroniska filer.
- För att återfå kontrollen krävs att du betalar en lösensumma, oftast i bitcoin.



Så minskar du risken för att drabbas

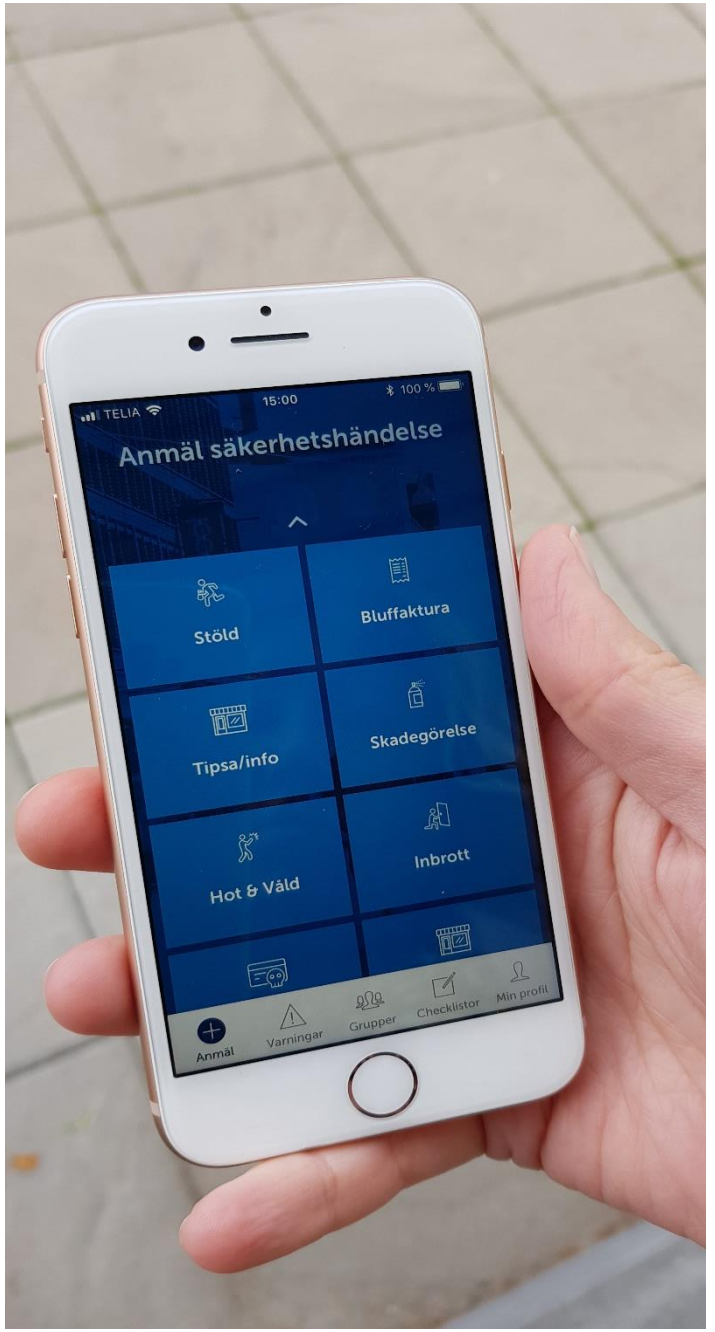
- Håll dina programvaror uppdaterade.
- Använd ett antivirusprogram.
- Klicka inte på bilagor, reklam och länkar om du inte vet var de kommer ifrån
- Installera inte mobilappar från okända leverantörer/källor
- Undvik att surfa på publika nätverk
- Ta backup regelbundet på den information du inte kan vara utan.

Om du drabbas

- Skulle du drabbas finns det en mängd officiella webbplatser och bloggar som innehåller instruktioner om hur du på ett säkert sätt kan ta bort skadlig programvara från dina enheter.
- Besök alltid www.nomoreransom.org för att kontrollera om din enhet har blivit smittad av ett av de utpressningsvirus för vilka det finns gratis tillgängliga dekrypteringsverktyg.
- Och till sist – betala inte!

Svensk Handel Säkerhetscenter

- Databas för säkerhetshändelser
- Enklare polisanmäla brott
- Varningar till företagare
- Checklistor för säkerhetsarbete i butik
- Samverkan med andra butiker i närområdet
- Överblick över händelser runt butiken
- Kommunikationsplattform
  - Krisgrupp
  - Ledningsgrupp
  - Personalgrupp



Kontakt

- Svensk Handels växel:

  Telefon 010 – 471 85 00 Mejl: info@svenskhandel.se

- Varningslistan:

  Telefon: 010 – 471 86 30 Mejl: varningslistan@svenskhandel.se

- Säkerhetsenheten

  Telefon: 010-471 86 80 Mejl: sakerhet@svenskhandel.se

- Nina Jelver

  Telefon: 010-471 85 16 Mejl: nina.jelver@svenskhandel.se