Kan man skydda sig mot attacker?

Är dina medarbetare oavsiktliga insiders?
Och hur kan man skydda organisationen mot det?

Marie Louise Arendt

IT-säkerhetschef, Region Skåne

Agenda

1. Vad ska vi skydda?
2. Var finns den största risken?
3. Vilka blir konsekvenserna?
4. Vad kan man göra för att minska risken?

1. Vad ska vi skydda?

Digitalisering ett måste, men skapar nya risker

- I dag arbetar i stort sett alla organisationer med digitalisering
- Det är ett måste för många **företag**, för att öka produktiviteten och behålla konkurrenskraft
- ... och för **offentliga myndigheter** som måste leverera mer välfärdsservice till fler människor, baserat bland annat längre livslängd
- Men digitaliseringen medför fler risker för att data ska bli röjda, otillgängliga eller förvanskade

FOI

Forskning Kurser Rapporter Jobba hos oss **Nyheter och press**

Totalförsvarets forskningsinstitut

21 november 2023

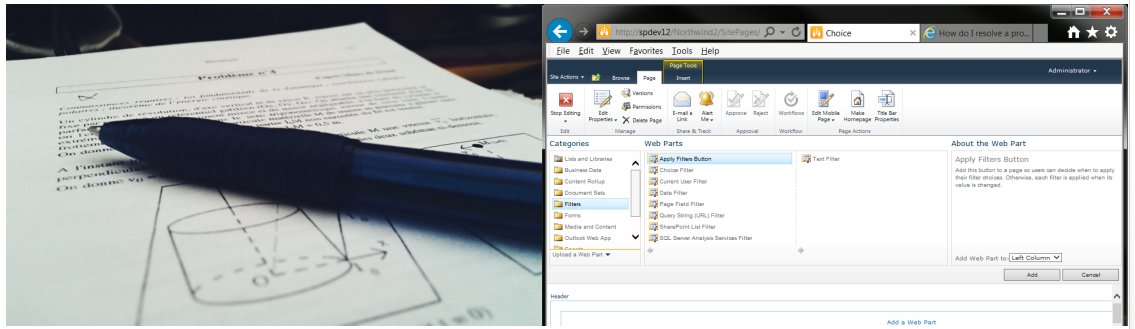
Digitalisering i vården skapar nya risker

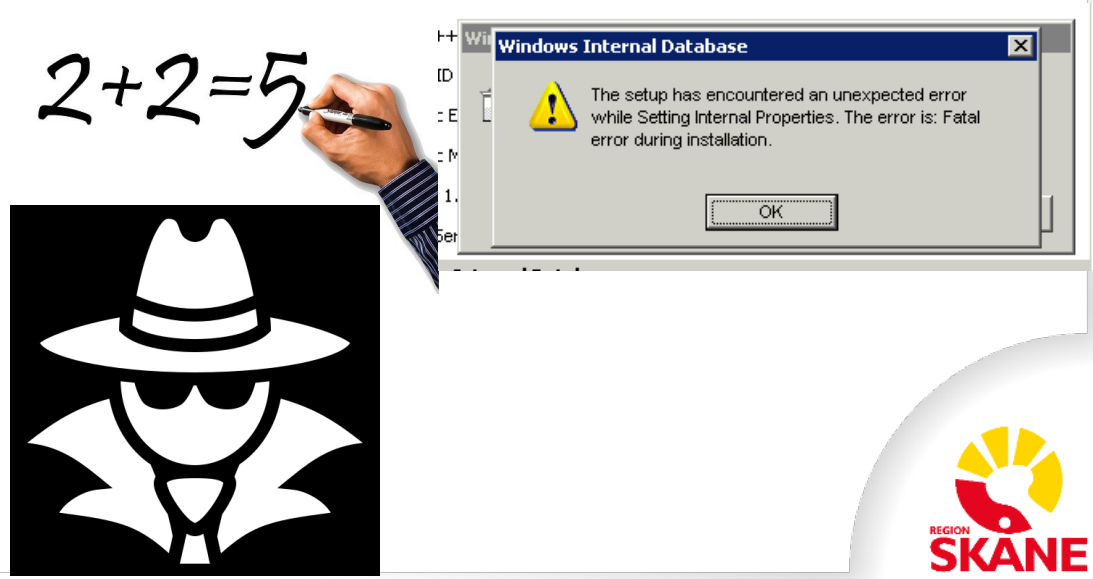
It kan göra vård enklare och mer effektiv. Men med it-systemen kommer risker, för intrång och för vård som inte fungerar överhuvudtaget. Forskare på FOI har kartlagt riskerna med hälso- och sjukvårdens digitalisering.

De senaste åren har hälso- och sjukvård har i hög grad digitaliserats. Bild: Andrey Suslov/Shutterstock.

Information och -säkerhet

- Informationssäkerhet är ett samlingsbegrepp som innebär att vi skyddar all vår information:
  - **analog** såväl som
  - **digital** ...
- ...mot **alla typer av hot**, som kan innebära påverkan vad gäller
  - **Konfidentialitet** (ej hamna i orätta händer)
  - **Tillgänglighet** (vi når den när vi behöver den)
  - **Riktighet** (informationen är korrekt, har inte förvanskats)



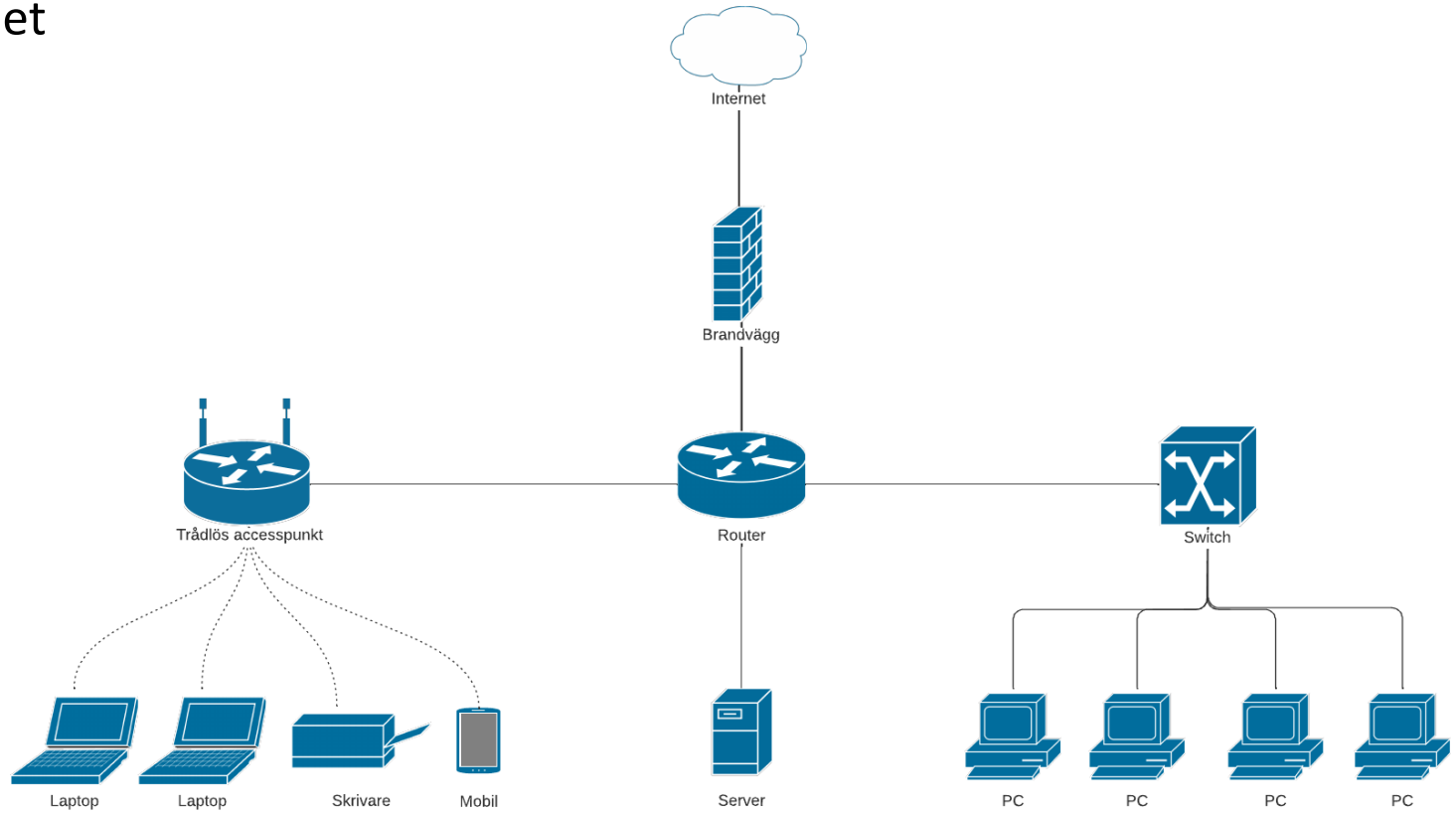


Digitala system

- De flesta av oss använder dagligen en rad olika **digitala system**, privat och yrkesmässigt, för
  - diarieföring
  - tidrapportering
  - ekonomiuppföljning och bokföring
  - bankärenden
  - journaler
  - med flera

Digital infrastruktur

- **Digital infrastruktur** är benämningen på ”vägstrukturen” som knyter ihop olika enheter, t ex datorer, skrivare, servrar, mobiler etc, med varandra och med internet

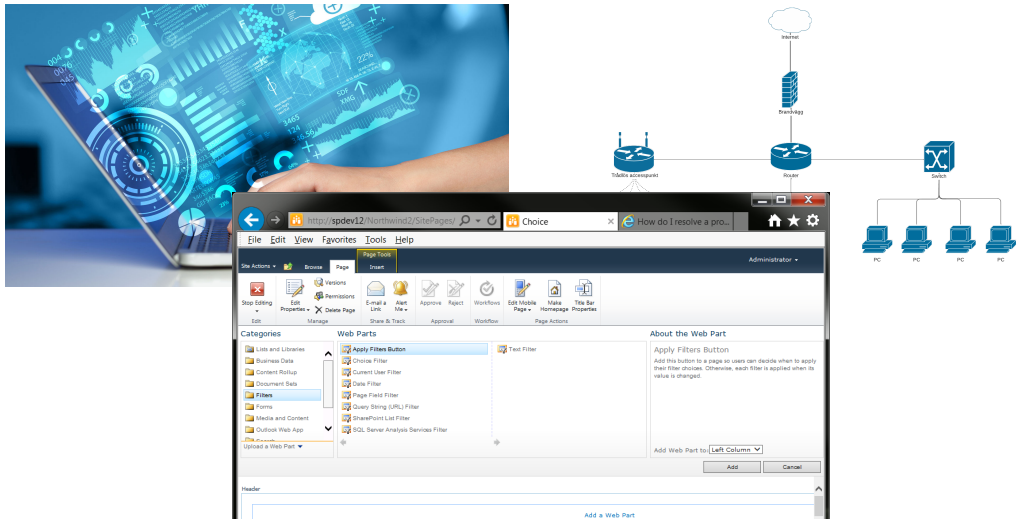


IT-säkerhet

- IT-säkerhet innebär att vi skyddar våra
  - **digitala** system inklusive
  - **digital infrastruktur** men även
  - tillhörande **anläggningar** ...
- ... mot **alla typer av hot** som kan innebära påverkan vad gäller **tillgänglighet, t ex**
  - **Inbrott**
  - **Sabotage**
  - **Brand**
  - **Översvämning**

Cybersäkerhet

- Cybersäkerhet innebär att vi skyddar våra
  - **digitala system**
  - inklusive **infrastruktur** samt
  - vår **digitala information** ...
- ... mot **antagonistiska** hot:
  - **Konfidentialitet** (ej hamna i orätta händer)
  - **Tillgänglighet** (vi når den när vi behöver den)
  - **Riktighet** (informationen är korrekt, har inte förvanskats)
- En **antagonist** är någon som **med flit** försöker inhämta, påverka eller förstöra information eller system/infrastruktur



2. Var finns den största risken?

Många säger ”externa hot”

Frågar man vem som helst om vad man tror är den främsta orsaken till dataintrångsincidenter, säger många att **externa hot** toppar listan

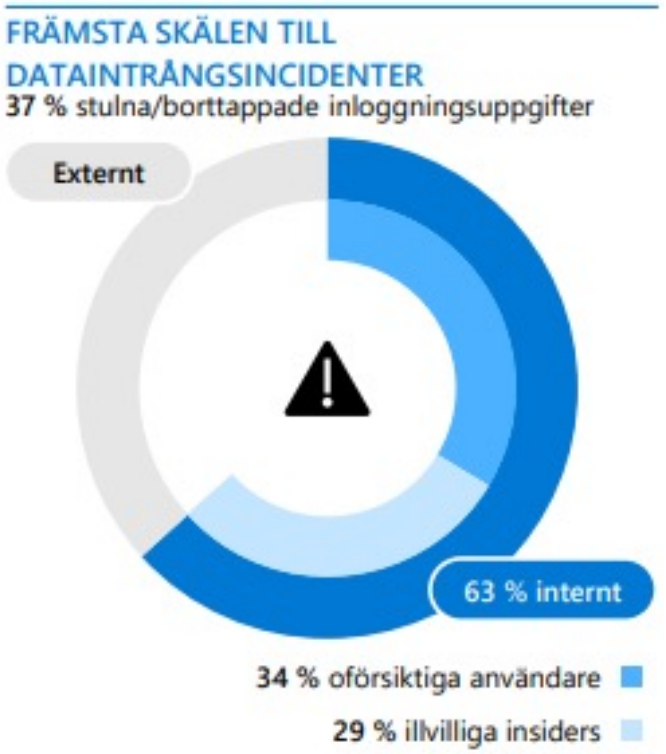
Begreppen nedan:

- **Främmande makt** (Ryssland, Kina och Iran),
- **Hackare** (Akira, Revil, Conti m fl)
- **Hacktivister** (Anonymous)

... nämns ofta som de främsta bovarna bakom tappad dataintegritet

Insiderrisker en av de främsta intrångs-orsakerna

- Men det är bara **37 % härrör från externa hot**
- Microsoft skriver i sin rapport från mars 2024 att nästan två tredjedelar **(63 %)** av dataintrångsincidenterna härrör från **insider**
- Majoriteten av dessa är sk **oavsiktliga** eller **omedvetna insiders**



Källa: Microsoft, ”Ompröva säkerheten inifrån och ut”, mars 2024

Företagsledare i Sverige håller med

- I en rapport som genomförts under 2022 bland **75 företagsledare i Sverige**, ges en inblick i hur vanligt det är med dataförluster, stölder och intrång hos de svenska företagen
- Närmare **hälften** av företagsledarna uppger att de **drabbats av dataintrång** under det senaste året
- En stor del av dessa, 74 procent, anser att **stöld av inloggningsuppgifter** är den största orsaken till dataintrång
- De vanligaste bristerna som anställda visar upp är just att **ladda ner skadliga bilagor** eller **filer** samt att **klicka på skadliga länkar**

SÄKERHET 2022-10-03 06:30

Därför ökar insiderhotet i hybrida arbetsmiljön – ”anställda inte lika vaksamma”

PRO Nästan hälften av svenska företagsledare uppger att de drabbats av dataintrång senaste året. Vanligaste orsaken är att inloggningsuppgifter blivit stulna – något som Proofpoints nya Nordenchef Annika Westlund tror hänger ihop med distansarbetet.

Vi kan dela in dessa i **medvetna** respektive **omedvetna** insiders

Den *medvetne* insidern

...

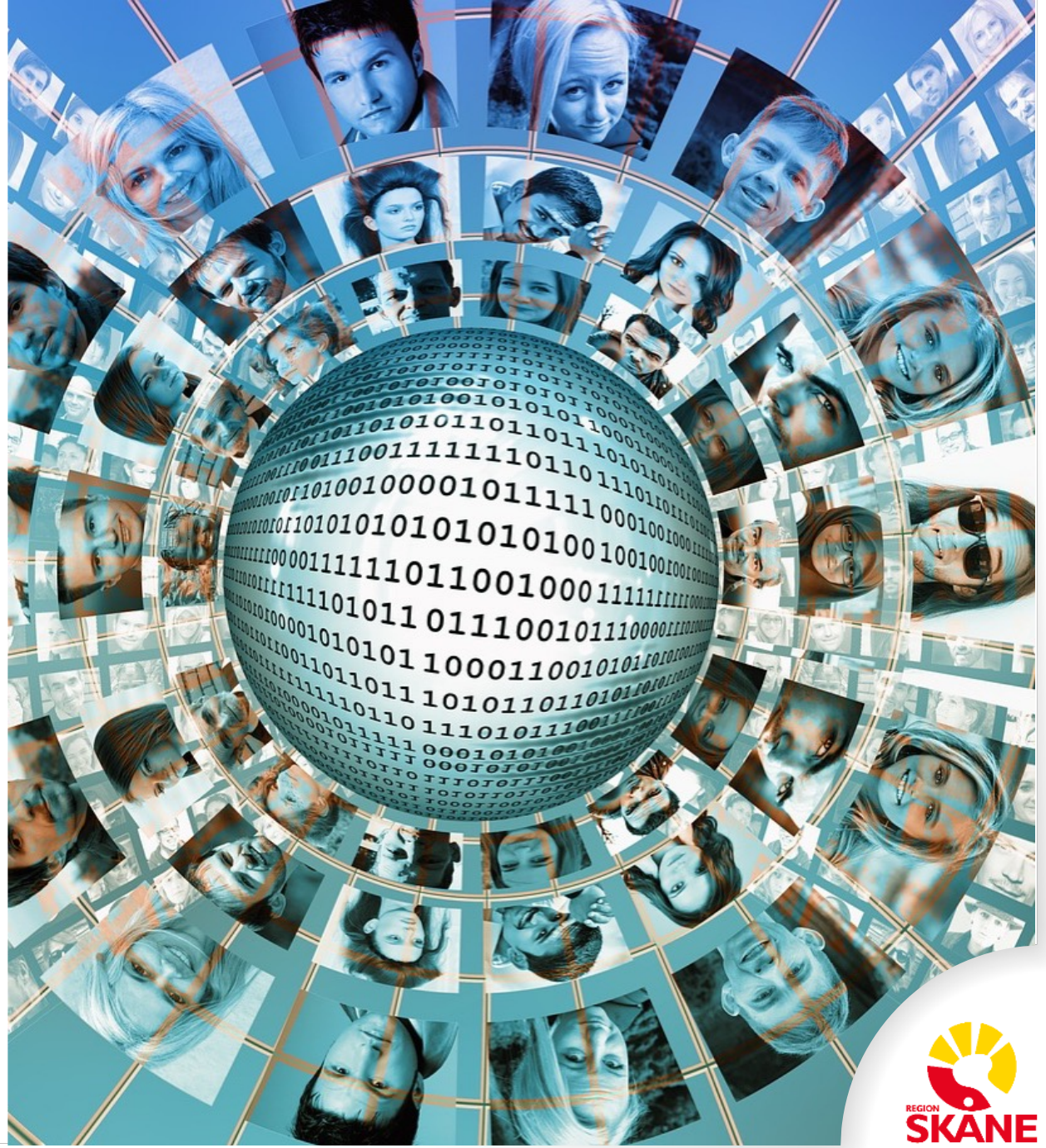
- läcker **medvetet** känslig information
- eller **orsakar andra problem med avsikt**
  - ibland för att **hämnas** på arbetsgivaren som man anser har sårat insidern på något sätt, exempelvis genom brist på uppskattning eller utebliven löneförhöjning,
  - ibland av **ideologiska** eller **politiska** skäl
- kan vara **motiverad** och **stimulerad** genom antingen **betalning**, **hot** eller **andra påtryckningsmedel** från en hotaktör såsom organiserad brottslighet eller en statsaktör

Hur finner antagonisten den medvetne insidern?

- genom **målsökning**
- genom **vänner och kontakter**
- genom att ta reda på vad som **motiverar en person** och vad som är **viktigt i den personens liv**

Ju **fler kontaktytor** till personen som finns eller kan skapas, desto fler gemensamma nämnare som finns med personen eller kan skapas

Och **ju fler sårbarheter** det går att hitta eller skapa hos personen, desto större är chansen att lyckas få personen att hjälpa till



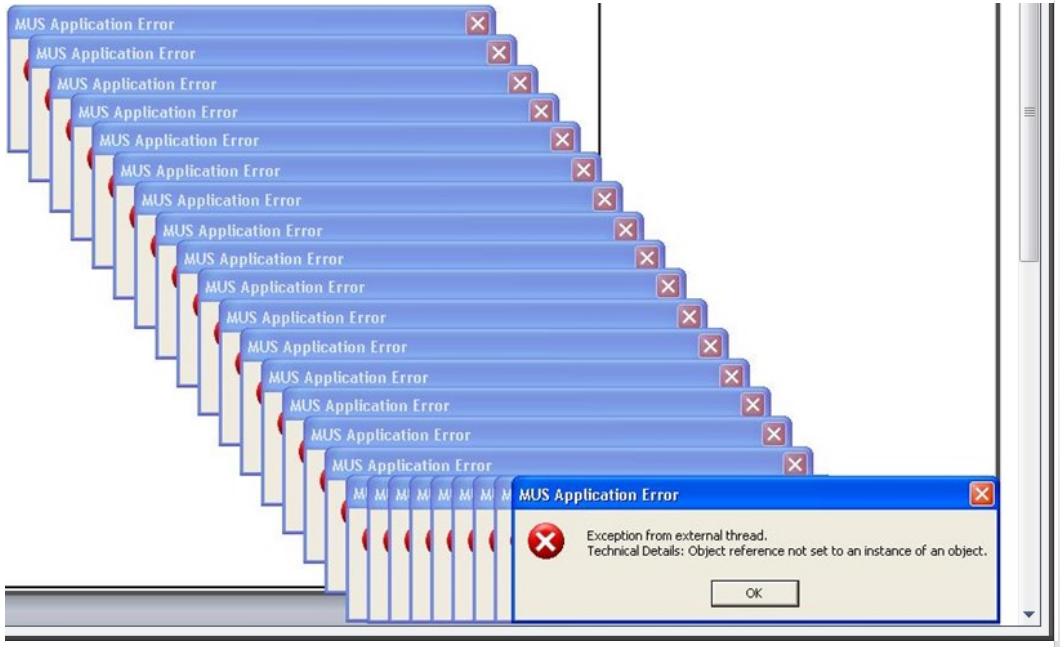
Den *omedvetne* insidern

- är **slarvig** och kan lämna en dörr öppen, datorn inloggad och/eller obevakad
- tillåter en okänd eller obehörig att ”**ta rygg**” vid inpassering
- **blir av med** eller glömmer sitt **passerkort**, **dator**, **mobiltelefon** etc
- **delar med sig av lösenord, koder och e-tjänstekort** till kollegor för att vara ”smidig”
- är medveten om säkerhetsrutiner och liknande, men tycker **inte** de känns **viktiga**, upplever dem som **krångliga** och väljer att ta genvägar eller helt strunta i dem, eftersom **rutinerna bara gäller andra**
- riskerar att **bli manipulerad** att hjälpa någon få tillträde till information eller system genom att exempelvis falla för en riktad så kallad ”spear phishing*)”-attack

*) Spear-phishing, även kallat spjutfiske, är en **riktad form av nätfiske** (phishing). Det innebär att skräddarsydda och målinriktade e-postmeddelanden skickas till noga utvalda offer. E-postmeddelandena är svåra att upptäcka utan noggrann kontroll, och det kan vara svårt att stoppa attackförsöken.

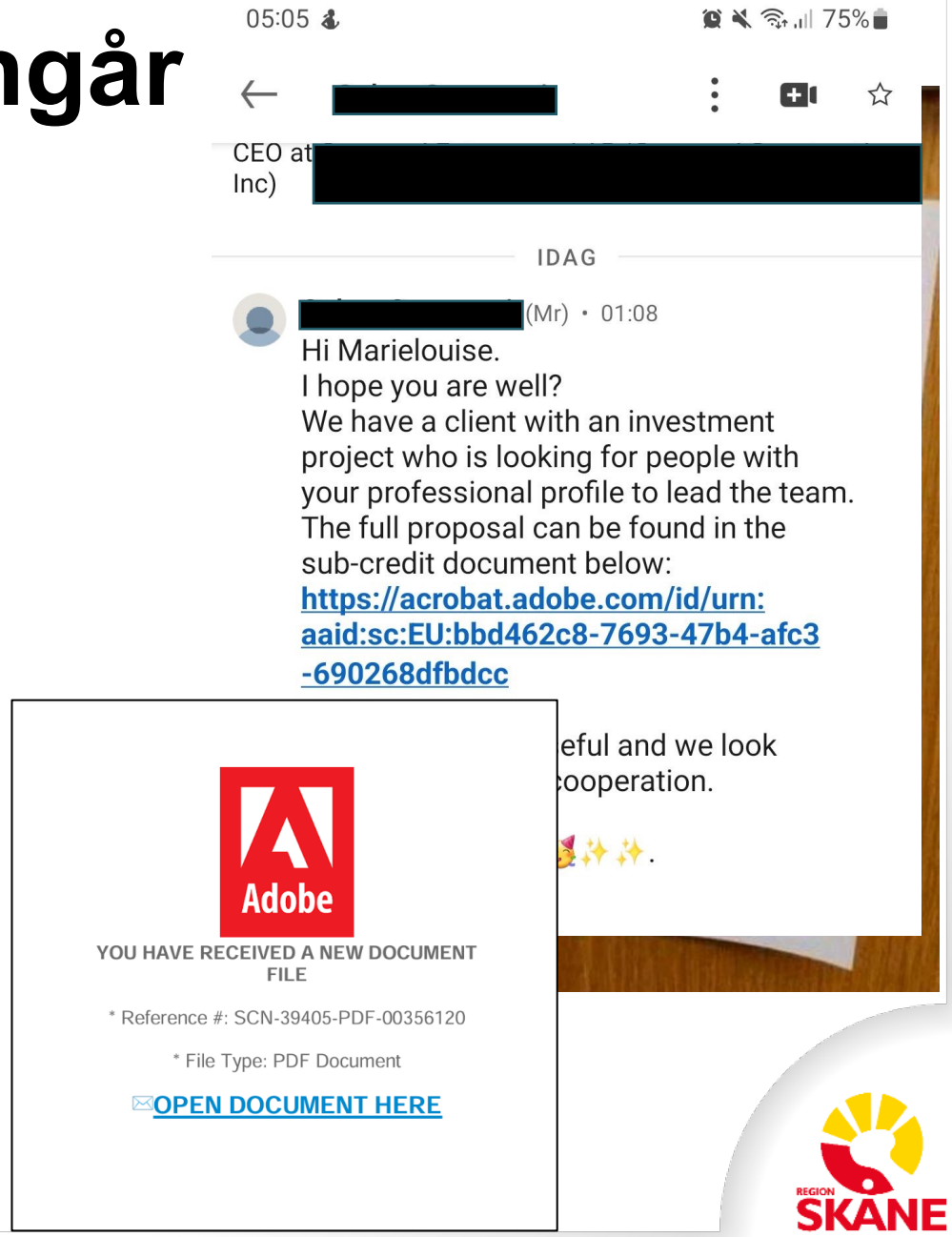
Den omedvetne insidern har två huvudorsaker

1. Användaren gör något av **misstag** eller **frångår rutiner** pga stress
2. **Kompetensbaserade fel**, man gör fel utan att veta om det eller av slarv/bristande engagemang



1. Exempel på misstag/frångår rutiner

- Är **slarvig med lösenord**, t ex väljer för enkla eller har samma lösenord på flera tjänster, vilket gör det enklare för antagonister att ta sig in i organisationens nätverk
- I en stressad situation där någon annan är inloggad på datorn, använder man den inloggningen för att det **går snabbare**
- Man får ett **jobberbjudande** via Linkedin och blir nyfiken på erbjudandet och klickar på länken



Avancerad (spear-)phising

SÄKERHET 2022-11-03 06:10

Kartlägger sina offer i sociala medier – ”mer avancerade attacker”

Nätfiske har varit ett enkelt sätt för angripare att stjäla inloggningsuppgifter som sedan används i cyberattacker. Samtidigt har det varit ett trubbigt vapen. Nu varnar cyberexperter för att kriminella lägger mer kraft på att kartlägga offren i detalj på sociala medier, var de är och har varit, och sedan skicka skadliga mejl riktade till särskilda individer baserat på den informationen.

Fejkad bemanning

Attackerna riktar in sig mot arbetssökande, och bedragaren tar kontakt vid Linkedins chattfunktion och utger sig för att komma från ett bemanningsföretag. Därefter påbörjar förövaren en mejlkonversation med offret och länkar till webbsidor som fejkar legitima bemanningsföretag, men som i själva verket är fyllda med skadlig kod.

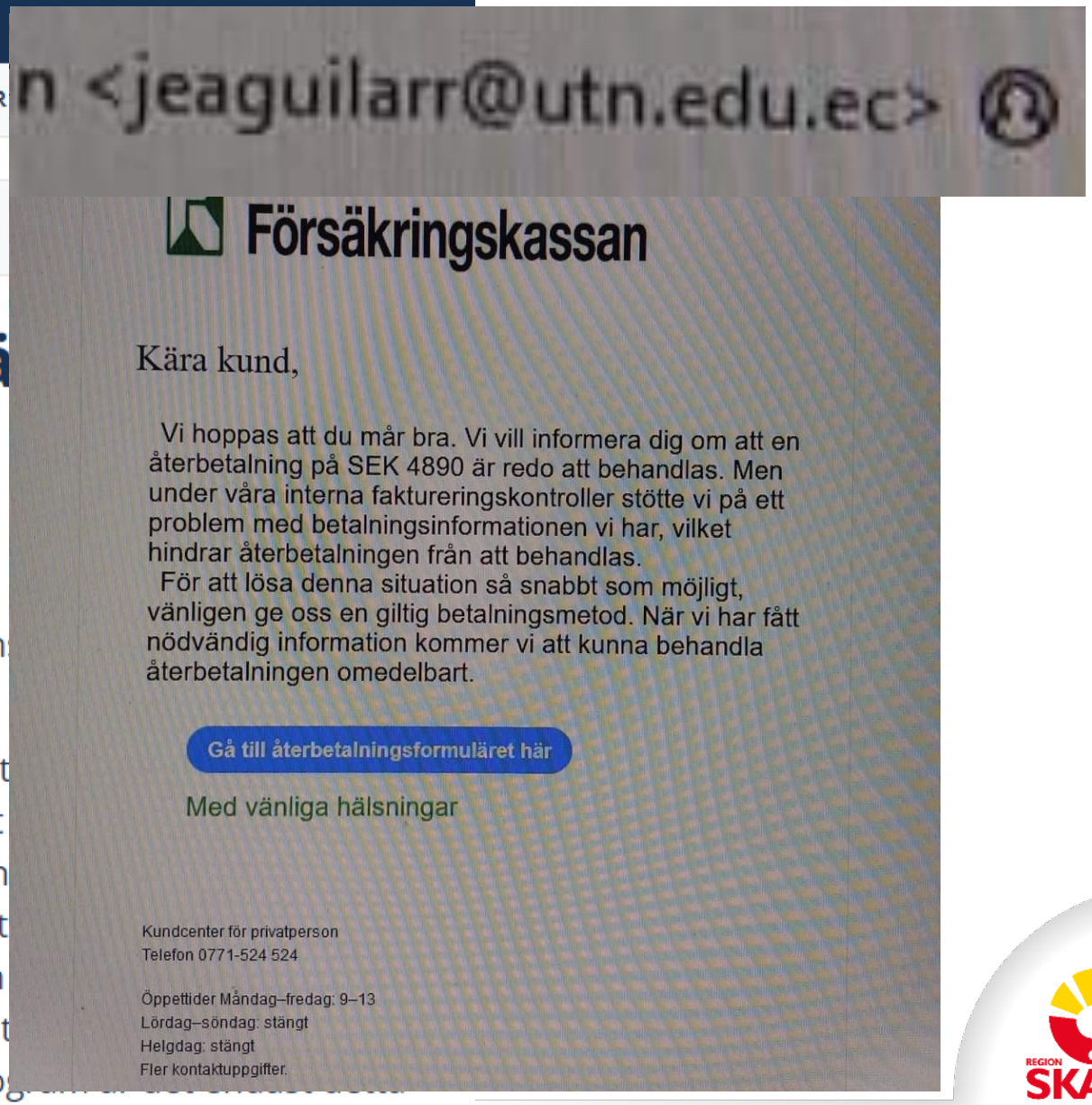
Publicerad: 2023-06-15 14:02

Nätfiske med falska avsä PDF-bilagor

NÄTFISKE PDF PHISHING SPOOFING

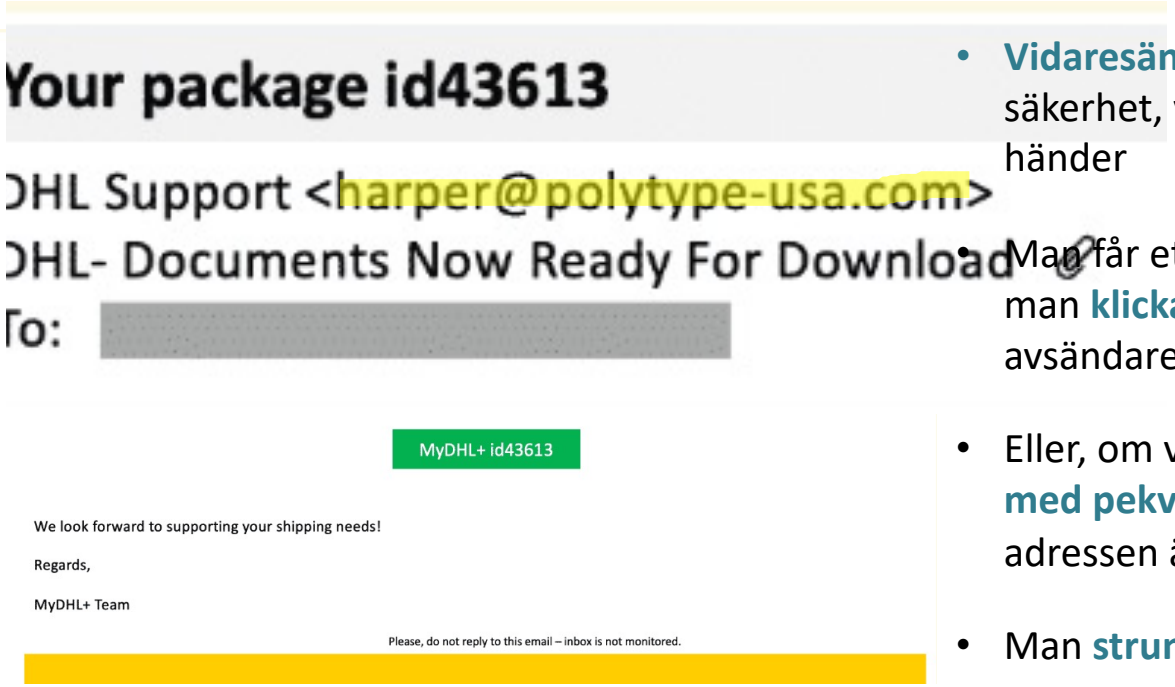
CERT-SE har observerat flera fall av nätfiske med gemen avsändarnamn och PDF:er.

I denna nätfiskekampanj ser e-postmeddelandena ut att organisationen, sk. e-post spoofing. E-postmeddelandet som mottagaren uppmanas klicka på. E-post spoofing in ändrar sitt namn i e-postmeddelandets avsändarnamn t organisations eller individs namn i syfte att utge sig från görs genom att ändra i e-postmeddelandets header. Det mottagare att upptäcka detta eftersom i vissa e-postpro namn som visas och inte avsändaradressen.



REGION SKÅNE

2. Exempel på kompetensbaserade fel



- **Vidaresändning** av organisationens epost till privat epostkonto med lägre säkerhet, vilket kan innebära att känslig information kommer i orätta händer
- Man får ett mail med information om att man har ett paket att vänta, och man **klickar på länken för att se vad det är,** utan att tänka på att avsändaren inte har en DHL-adress
- Eller, om visningsadressen är manipulerad och ser äkta ut, **utan att hovra med pekverktyget över avsändarens epostadress** för att säkerställa att adressen är korrekt
- Man **struntar i att genomföra uppdateringar**
- Använder sig av s k **skugg-IT**, som inte uppdateras eller där sårbarheter inte åtgärdas vilket ökar möjligheterna för den som vill nästla sig in

Falska mejl tar dina inloggningsuppgifter

- Du får ett mail med en länk som kanske innehåller ett jobberbjudande eller något annat som lockar dig
- Du klickar på länken och blir iom det uppmanad att logga in på Linkedin
- Du loggar in = ger i samma ögonblick bort dina inloggningsuppgifter

Falska LinkedIn-webbplatser

Enligt Check Point Research sker det typiska phishing-försöket genom att ett falskt mejl innehåller en länk som till synes är avsedd för exempelvis LinkedIns inloggningssida.

FALSK: Ett exempel på en falsk inloggningssida till LinkedIn som du kan landa på efter att ha klickat på en länk i ett mejl.

När du sedan klickar på länken kommer du till en sida som visas ovan. Sidan liknar LinkedIns inloggningssida. När du kommit så långt är du mycket nära att ge bort dina inloggningsuppgifter till personerna bakom nätfisket, som i sin tur till exempel kan ta över ditt LinkedIn-konto.

SÄKERHET 2022-06-21 06.15

Rapport: 24 miljarder användarnamn och lösenord till försäljning på dark web

Det populäraste lösenordet är "123456".

Säkerhetsföretaget Digital Shadows, via Venture Beat, har räknat ut att hela 24 miljarder användarnamn och lösenordskombinationer finns ute till försäljningen på dark web. De tillgängliga användarnamnen och lösenordskombinationerna skulle kunna användas för att få åtkomst till eller ta över ett offers konto.

Av dessa lösenord ska 6,7 miljarder ha en unik användarnamn- och lösenordskombination, vilket är 1,7 miljarder fler än när Digital Shadows gjorde samma undersökning 2020. Av dessa 6,7 miljarder användarnamn och lösenordskombinationer ska det vanligaste lösenordet varit "123456" som utgjorde 0,46 procent av helheten.

För att skydda sig online när det kommer till användarnamn och lösenord rekommenderar Digital Shadows användningen av verktyg som multifaktorsautentisering, lösenordshanterare och unika, snarare än återanvända, lösenord.

”Aktuell” händelse *eller* länkar till falska webbsidor

- Du får ett mejl om att du ska få skatteåterbäring och avsändaren påstår sig vara Skatteverket
- Avsändarens mejladress kan vara:
  - refund@skatteverket.se
  - skatt@skatteverket.se
  - eller liknande
- Du blir ombedd att klicka på en länk som ser ut att gå till Skatteverket

- Du uppmanas att kontakta polisen genom att klicka på länken www.polisens.se
- Titta noga på webbadressen. Den ser rätt ut, men i slutet av ordet polisen har bedragarna lagt till ett extra s och plötsligt hamnar du någon annanstans än på www.polisen.se
- Den falska länken går till en sida som är identisk med eller snarlik den riktiga
- Du kan enkelt tro att det är den rätta webbadressen, men är helt i händerna på bedragare

Källa: Polisen.se

3. Vilka blir konsekvenserna?

Vilka blir konsekvenserna?

Enligt IBM:s rapport ”Cost of a data breach”

- ligger den mänskliga faktorn bakom 19 av 20 cyberintrång
- uppgår den genomsnittliga kostnaden för cybersäkerhetsincidenter orsakade av den mänskliga faktorn till 4,35 miljoner dollar (ca 51 MSEK)

Cybersäkerhetsintrång innebär inte bara stora ekonomiska kostnader för verksamheten utan skadar även organisationens anseende

Från handhavandefel till angrepp

Charlotte Petri Gornitzka berättar att de flesta it-incidenter i samhället som rapporterades in till och med 2022 hade med handhavandefel eller systemfel att göra. Men 2023 ändrades det.

– Då blev den vanligaste incidenten ett angrepp. Det innebär att vi måste höja den grundläggande nivån för att skydda informationssystem och tjänster.

MSB-chef om svensk it-säkerhet: ”Lite pinsamt att vi inte kommit längre”

– Sju av tio organisationer saknar de mest grundläggande delarna i ett systematiskt informations- och säkerhetsarbete. Väldigt många av dessa är kommuner, säger MSB:s generaldirektör Charlotte Petri Gornitzka.

4. Vad kan man göra för att minska risken?

”Vi har tekniska lösningar som skydd, det räcker!”

- Gör det?
- Nej, antalet cyberattacker blir fler och vi kan inte enbart förlita oss på de tekniska lösningar och skydd som finns implementerat
- Om människan gör ett oavsiktligt misstag spelar det ingen roll hur bra tekniken är
- Varje medarbetare spelar en viktig roll för att förhindra intrång i organisationens IT-miljö
- Det är viktigt att ständigt arbeta med att öka medvetenhet inom områdena IT- och cybersäkerhet, genom att ge utbildning och tips för hur man kan tänka i en alltmer uppkopplad värld


Aktuell Säkerhet

DIGITAL SÄKERHET TRADITIONELL SÄKERHET I FOKUS EVENEMANG PERSONALNYTT KRÖNIKOR

Nyheter

Mänskliga faktorn sätter käppar i hjulet för cybersäkerhet

Av Linda Kante - 2019-11-08

Kunskap är ett steg på vägen …

Man måste se till att alla förstår vad man får och inte får göra, och varför

Erbjud era medarbetare regelbundna utbildningsinsatser, om handhavande, lösenord, cybersäkerhetshot samt hur man hanterar hoten

Det är ingen engångsföreteelse, skapa en utbildningsplan som består av flera delar:

- Digital utbildning i IT- och cybersäkerhet
- ATP-material där man diskuterar frågorna
- Be er informationssäkerhets- eller IT-säkerhetssamordnare/-chef komma och informera på APT om hur ni jobbar med frågorna hos er
- Nanolearning är ett bra sätt att hålla kunskaperna vid liv

Men i mars kunde Aftonbladet a
Bergström – trots allt hemlighetsn
hanterat sekretessbelagd informat
privata Gmail-adress vid upprepad

Bedömningen: Kan skada Sverig

Mejl som omfattas av utrikessekre
skickades både till och från den pr
adressen och var direkt kopplade t
vaccinsamordningen.

Det rörde sig om ett stort antal mejl. Bara tre av mejlen som Bergström skickade till sin privata mejl innehöll totalt över 80 A4-sidor.

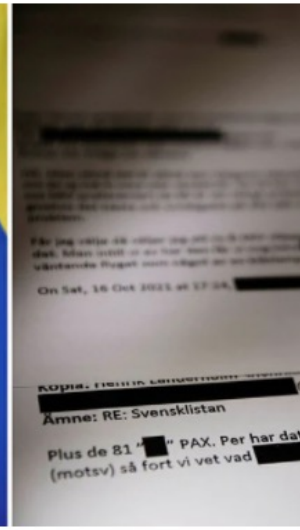
Alla sidor var helt sekretessbelagda.

Ämnesraderna i två av de mejlen kopplades

SVERIGE

Generaldirektör skickade hemliga uppgifter till privata mejlkonton

UPPDATERAD I GÅR 09:45 PUBLICERAD I GÅR 06:25



Henrik Landerholm, generaldirektör vid Myndigheten för psykologiskt försvar. Foto: Lars Schröder/TT, Nicklas Thegerström

Generaldirektören för Myndigheten för psykologiskt försvar, Henrik Landerholm, har skickat sekretessbelagda uppgifter till privata e-postkonton, kan DN avslöja.

Uppgifterna bedöms vara så känsliga att de skulle kunna skada Sverige om de röjs.

– Att hantera uppgifter på det här sättet innebär att de är lättare att inhämta av främmande makt, säger Kim Hakkarainen, expert på säkerhetsskydd vid

Informationsklassning, riskanalys och DPIA är ett annat

I allt vi gör; förändrar befintliga system eller utvecklar/köper in nya system, bör **informationsklassning**, **riskanalys** och i vissa fall **konsekvensbedömning** (DPIA = Data Protection Impact Assessment) ligga som grund

– *Vilken information kommer att hanteras, hur flödar informationen, handlar det om personuppgifter eller patientuppgifter, vad säger lagstiftningen?*

– *Och vilka risker finns, på vilken nivå och om vi mitigerar (reducerar) riskerna, vilken nivå hamnar vi på då?*

Inget **driftgodkännande** ges utan att ovanstående finns på plats och endast om riskerna är acceptabelt höga

Höga risker måste mitigeras, exempelvis genom:

- autentisering
- kryptering
- rutiner och tydlig information om säkerhet till systemets användare
- logg över vem som använder personuppgifter
- stöd för säkerhetskopiering
- pseudonymisering av personuppgifter
- öppen redovisning av personuppgifternas syfte och behandling
- möjlighet för den registrerade att övervaka uppgiftsbehandlingen
- reducering av antalet personer som har tillgång till uppgifterna
- begränsning av sökbegreppen så att det inte går att söka på känsliga personuppgifter
- unförande av automatisk borttagning av personuppgifter som inte längre ska behandlas
- utformning av it-systemen så att inte fler personuppgifter än nödvändigt behandlas, det vill säga inbyggt dataskydd och dataskydd som standard

REGION SKÅNE

Ytterligare tips ...

- **Undersök:** Och identifiera vilka faktorer som kan innebära ett hot mot cybersäkerheten hos er, vad har ni för svagheter och sårbarheter?
- **Ta fram en plan:** Utarbeta en handlingsplan för vad ni bör göra för att förstärka säkerheten och håll er till den
- **Stark lösenordshantering är aldrig fel**: Genom att stärka systemet för lösenordshantering inom organisationen förhindrar ni cyberintrång som beror på dålig lösenordshygien
- **E-postfilter:** Det finns speciella program som förbättrar filtreringen och fångar upp nätfiskemeddelandena innan de når mottagaren
- **Undvik usb-minnen:** Och måste man använda sådana, se till att de scannas först, gärna i en fristående ”tvättdator”

Slutligen: Utsatt för nätfiske eller bluff-sms?

Nätfiske som även kallas phishing är när bedragare på olika sätt "fiskar" efter dina uppgifter. Var misstänksam om du exempelvis får mejl med uppmaning om att klicka på en länk och fylla i dina bankuppgifter. Följ aldrig sådana uppmaningar.

Om du misstänker att du blivit utsatt för nätfiske, gör en polisanmälan och kontakta din bank.

Gör en polisanmälan

Det finns två sätt att göra en polisanmälan på:

- ring polisen på 114 14
- besök en polisstation.

Ring 112 om brottet händer nu, eller om polisen behövs på plats snabbt.

Polisanmälan – allt du behöver veta

Rapportera misstänkta bluff-sms till 7726

Har du fått ett misstänkt bluff-sms? Vidarebefordra meddelandet till **7726**. Siffrorna motsvarar ordet SPAM på knappsatsen i telefonen och är globalt etablerat för att rapportera bluff-sms.

Det är ett operatörsoberoende nummer som alla kan använda. På så sätt får teleoperatörerna veta vilka bluff-sms du får.

Frågor?