Svenskarnas syn på IT-säkerhet **2018**

sentor

Innehållsförteckning

Inledning

2017 kantades av flera uppmärksammade säkerhetsrelaterade händelser. Få missade skandalen hos Transportstyrelsen som än idag skapar rubriker i media. Fjolåret präglades även till stor del av förberedelser inför det nya regelverket GDPR som trädde i kraft i maj i år vilket har inneburit stora och påkostade förändringar för många organisationer.

Dessa händelser avspeglar sig i vår syn på IT-säkerhet. Hur har egentligen skandalen på Transportstyrelsen påverkat vårt förtroende för myndigheter när det gäller behandling av data? Vilken inställning har vi till vad som räknas som person-uppgifter eller inte, och vad förväntar vi oss av företag och organisationer när det kommer till hanteringen av uppgifterna?

Dessa frågeställningar lägger grunden för den tredje upplagan av Sentors årliga rapport ”Svenskarnas syn på IT-säkerhet”. I år bygger undersökningen på svar från 1002 svenskar i åldrarna 18-75 år som tillsammans utgör ett riksrepresentativt och statistiskt säkerställt urval. Syftet med rapporten, som har tagits fram tillsammans med undersökningsföretaget Ipsos, är att kartlägga svenskarnas inställning till IT-säkerhetsrelaterade ämnen.

Målet med rapporten är att leverera bättre insikter kring hur svenskar känner och agerar i frågor kopplade till säkerhet. Något som kan användas för att på ett bättre sätt informera och kommunicera med dessa grupper.
Valår och GDPR gör frågor rörande personliga uppgifter extra intressanta. Personuppgifter som namn, politiska åsikter och sexuell läggning anses i högre utsträckning vara känslig data i år jämfört med i fjol. Nytt för i år är att vi har tagit tempen på huruvida säkerhetsincidenter på banker påverkar kundernas förtroende. Nästan samtliga, oavsett grupp, skulle överväga att byta bank ifall det skulle framkomma att de har missbrukat ens personuppgifter.

Lågt förtroende är ett återkommande ämne i årets undersökning. Bland annat har svenskarnas förtroende för e-han-delsföretag minskat sedan 2017. Även förtroendet för hur sociala medier hanterar känslig information är fortsatt lågt, redan innan skandalen om Facebook och Cambridge Analytica uppdagades.

Detta och mycket mer finns att ta del av i rapporten i sin helhet.
Vid frågor kring rapporten, maila oss på info@sentor.se.

Trevlig läsning!

Anders Söderström, CEO

Definition av känslig data

Vilken typ av information anser du är känslig data?

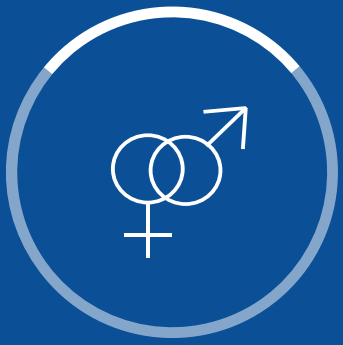
När svenskarna får ange vad de anser vara känslig data, så varierar svaren. De flesta är dock överens om att kreditkortsuppgifter och personnummer är känslig data. Noterbart i årets rapport är att fler uppger att politiska åsikter är känslig data. 44 procent uppger detta i år, att jämföra med 35 procent i fjol.

96%
anser att kreditkortsnummer är känslig data

83%
anser att personnummer är känslig data

68%
anser att IP-adress är känslig data

44%
anser att politiska åsikter är känslig data



36%
anser att sexuell läggning är känslig data

28%
anser att telefonnummer är känslig data

28%
anser att adress är känslig data

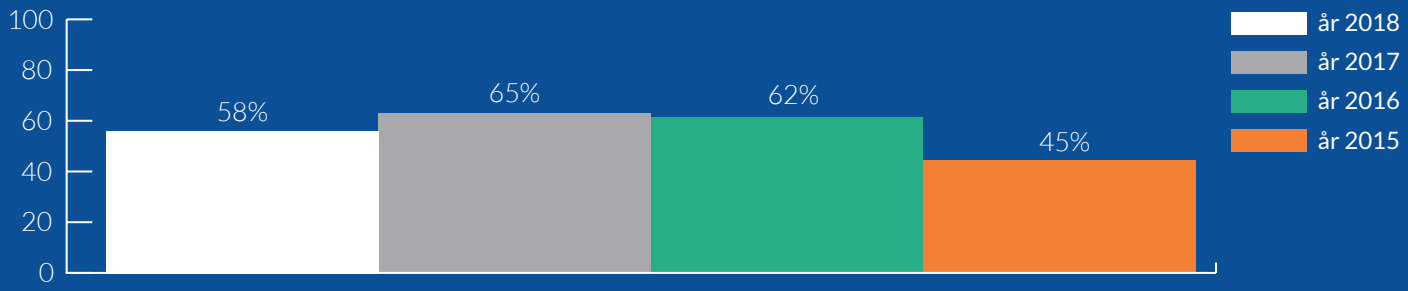
26%
anser att e-postadress är känslig data

13%
anser att namn är känslig data

Inställning till IT-säkerhet

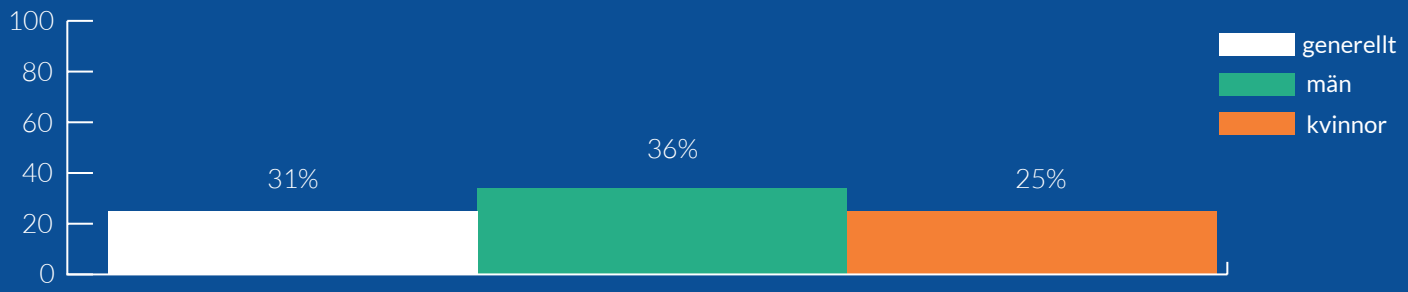
Är du orolig för att någon form av dataintrång eller IT-säkerhetsattack ska drabba dig (virus, bedrägeriförsök eller liknande)?

Över hälften av svenskarna känner en rädsla för att drabbas av ett dataintrång eller en IT-säkerhetsattack. Undersökningen visar att närmare 6 av 10 svenskar är oroliga för att drabbas.



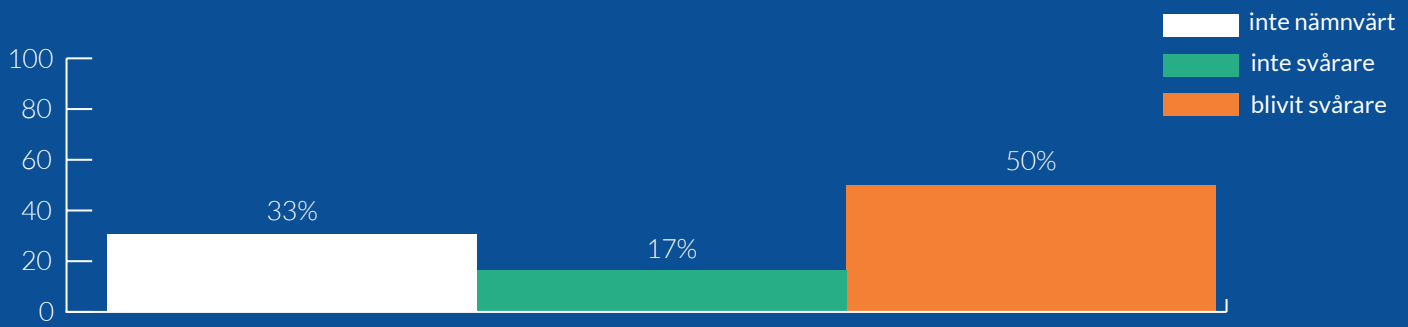
Har du utsatts för någon form av dataintrång eller IT-säkerhetsattack privat eller på jobbet(virus, bedrägeriförsök eller liknande)?

3 av 10 svarar att de har utsatts för någon form av dataintrång (privat eller på jobbet) under det gångna året. Bland männen uppger 36 procent att de har utsatts medan siffran bland kvinnor är 25 procent.



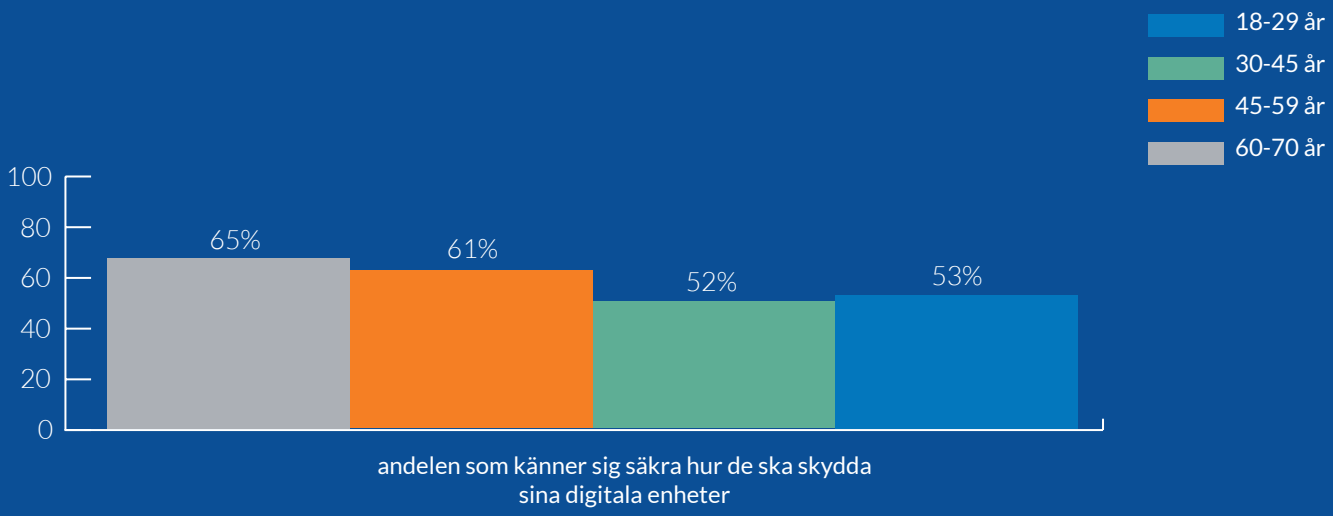
Upplever du att det har blivit svårare att ta hand om din egna IT-säkerhet i takt med att antalet digitala tjänster som används har ökat?

Hälften av svenskarna uppger att det har blivit svårare att ta hand om den egna IT-säkerheten i takt med att antalet digitala enheter och tjänster ökar.



Vet du hur du ska skydda dina digitala enheter från dataintrång?

7 av 10 svenskar är säkra på hur de ska skydda sina digitala enheter. Män känner sig mer säkra jämfört med kvinnor. Dessutom uppger fler äldre personer (60-75 år) att de känner sig säkra på hur enheterna ska skyddas jämfört med de yngre åldersgrupperna.



69%

av männen känner sig säkra på hur de ska skydda sina digitala enheter.

46%

av kvinnorna känner sig säkra på hur de ska skydda sina digitala enheter.

Förtroende för statliga och privata organisationer

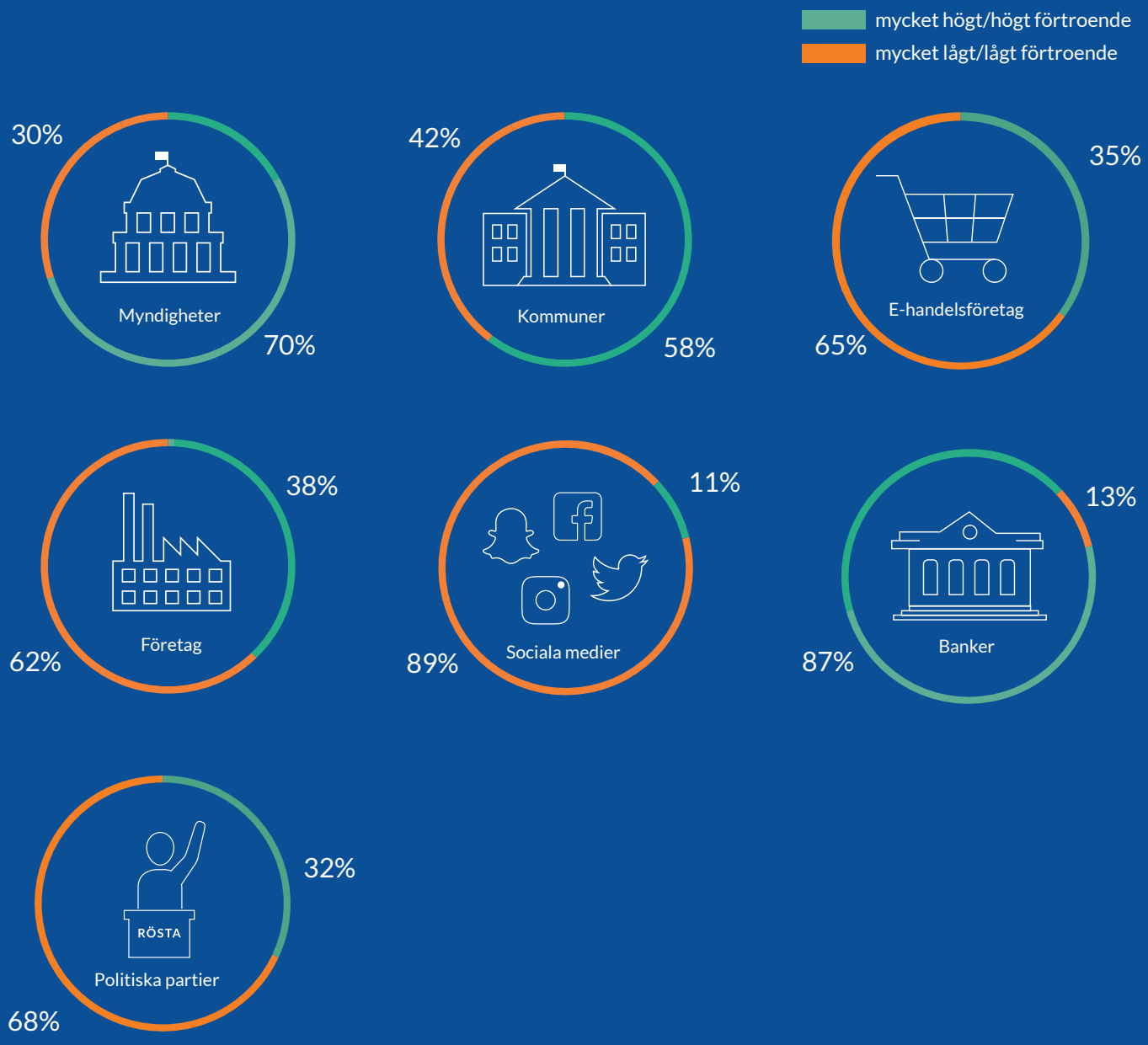
Hur ser ditt förtroende ut för att följande aktörer, som hanterar din känsliga data, skyddar informationen från missbruk och intrång?

Både statliga och privata organisationer har tillgång till svenskarnas känsliga data. I årets rapport har vi undersökt hur den svenska befolkningens förtroende ser ut för dessa aktörer när det kommer till att skydda deras information från missbruk och intrång.

Svenskarna har stort förtroende för bankernas hantering av känslig data, medan företag i allmänhet, och e-handelsföretag i synnerhet, brottas med ett svagare förtroende.

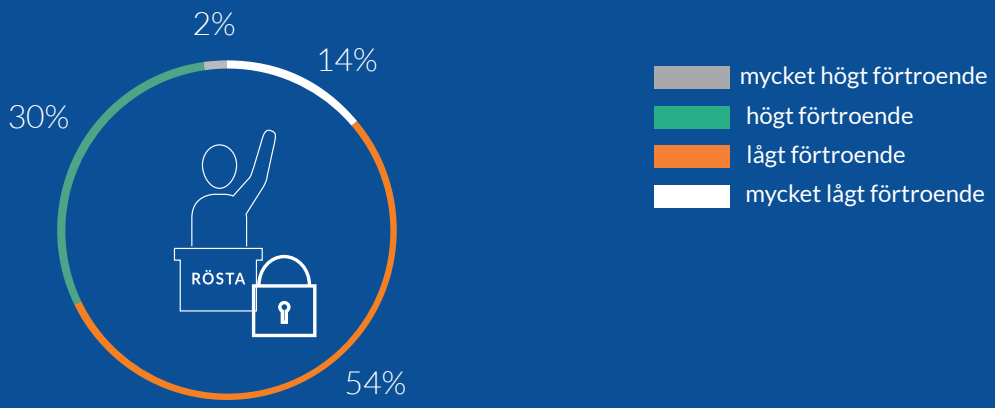
Trots förra årets uppmärksammade IT-säkerhetsincidenter inom offentlig sektor är förtroendet för dessa aktörers förmåga att skydda medborgares känsliga data orubbat. Förtroendet för myndigheter ligger på exakt samma nivå som i fjol, innan IT-skandalen hos Transportstyrelsen uppdagades.

Företag inom sociala medier placerar sig återigen lägst i vår förtroendebarometer, där endast 11 procent av svenskarna säger sig ha högt, eller mycket högt förtroende för dessa företags förmåga att skydda känslig data.



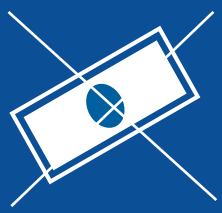
Hur ser ditt förtroende ut för att politiska partier, som hanterar din känsliga data, skyddar informationen från missbruk och intrång?

2 av 3 svenskar har lågt, eller mycket lågt, förtroende för politiska partiers kapacitet att skydda känslig data. Politiska partier har ofta medlemsregister där exempelvis personuppgifter och politiska åsikter kan finnas registrerade. De är också intressanta måltavlor för många cyberkriminella med anledning av detta.



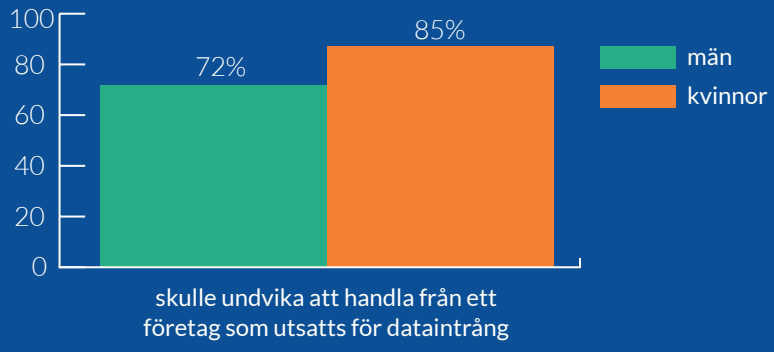
Skulle du undvika att handla från ett företag om du kände till att företaget utsatts för dataintrång?

Har IT-säkerhetsattacker blivit vardagsmat? I år svarar 78 procent att de skulle undvika att handla från ett företag som utsatts för dataintrång, att jämföra med 83 procent 2017. Kvinnor är mer benägna att undvika att handla från ett företag som utsatts för dataintrång (85 procent), jämfört med män (72 procent).



78%

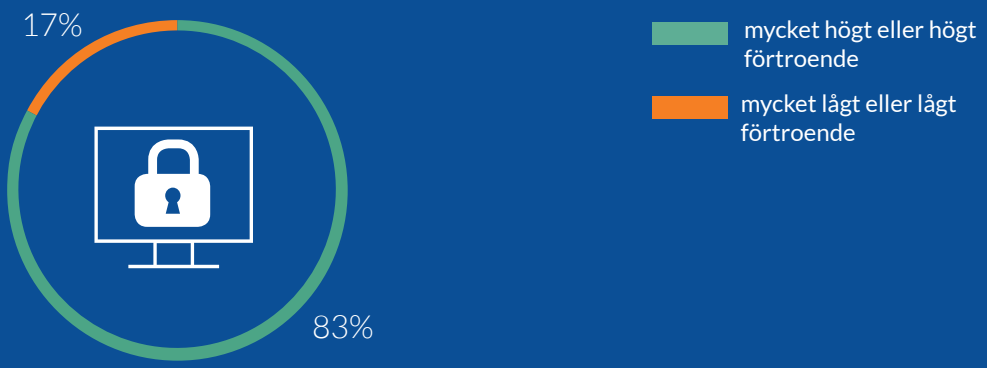
skulle undvika att handla från ett företag som utsatts för dataintrång



Säkerhet på arbetsplatsen

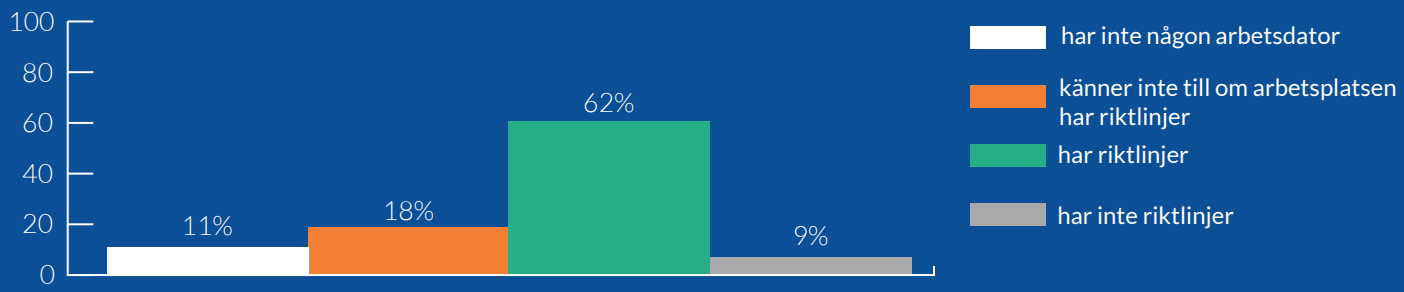
Hur stort förtroende har du för IT-säkerheten på din arbetsplats?

8 av 10 svenskar uppger att de har förtroende för IT-säkerheten på den egna arbetsplatsen. Förtroendet bland åldersgruppen 18-29 har ökat mest – från 66 procent 2017 till 88 procent 2018.



Har din arbetsplats riktlinjer för säkert användande av din arbetsdator?

4 av 10 svenskar med arbetsdator uppger att arbetsplatsen inte har riktlinjer för säkert användande. 2 av 10 känner inte till om deras arbetsplats har riktlinjer.

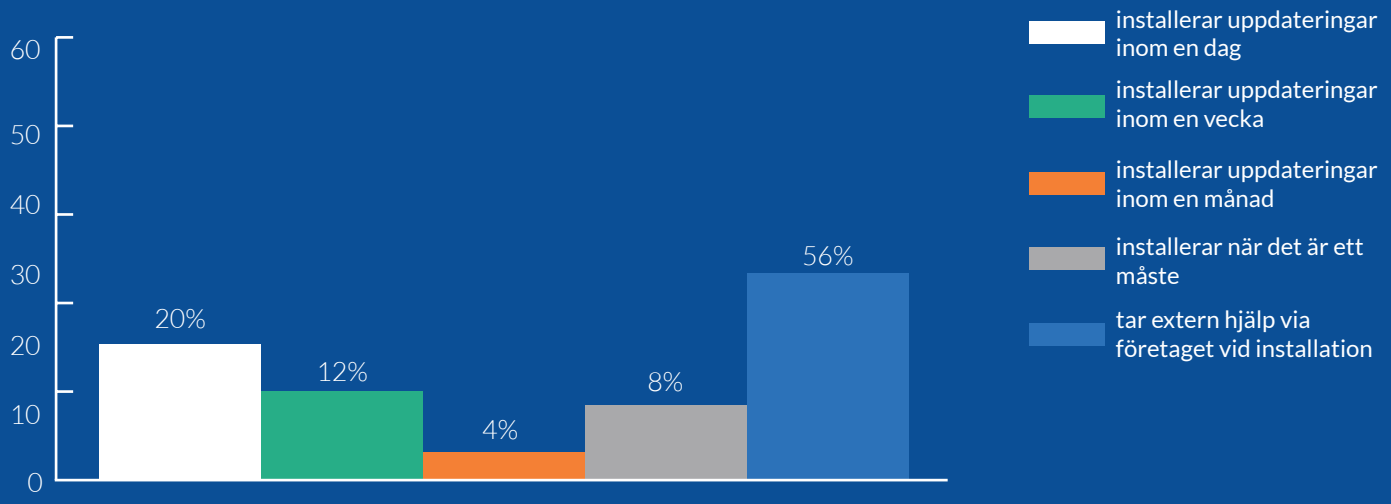


Hanterar du känslig eller hemlig information på din arbetsdator?

Att hantera känslig data på arbetsdatorn kan vara riskfyllt, något 6 av 10 svenskar uppger att de gör.

Hur hanterar du uppdateringar till din arbetsdator (ex. uppdateringar av operativsystem, Office-paketet och insticksprogram till din webbläsare)?

Över hälften av svenskarna svarar att de får extern hjälp via företaget när det kommer till att uppdatera arbetsdatorn.



Har din arbetsdator använts av någon annan än dig själv?

Över hälften av svenskarna har lånat ut sin arbetsdator till någon annan. Vanligast är att man lånar ut den till en kollega.

41%
uppger att de har lånat ut arbetsdatorn till en kollega

8%
uppger att de har lånat ut arbetsdatorn till en familje-medlem

2%
uppger att de har lånat ut arbetsdatorn till någon annan än kollega och familjevän

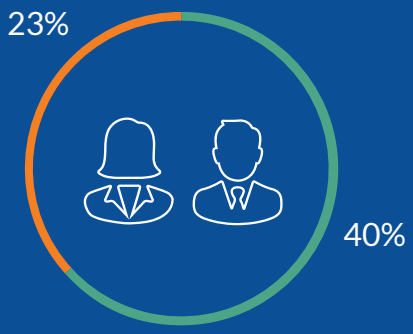
49%
uppger att de inte lånat ut sin arbetsdator

Har du kopplat in en privat USB-sticka eller extern hårddisk i din arbetsdator?

Att koppla in en privat USB-sticka eller extern hårddisk i sin arbetsdator kan orsaka omfattande skador. Trots att det är riskfyllt uppger 1 av 3 svenskar att de gjort just detta.

har kopplat in en USB-sticka eller extern hårddisk i sin arbetsdator

har ej kopplat in en USB-sticka eller extern hårddisk i sin arbetsdator



män

kvinnor

har kopplat in en USB-sticka eller extern hårddisk i sin arbetsdator

Känner du till säkerhetsriskerna med att koppla in en privat USB-sticka eller extern hårddisk i din arbetsdator?

Hela 40 procent svarar att de inte känner till säkerhetsriskerna med att koppla in en privat USB-sticka eller extern hårddisk i arbetsdatorn.

60%
uppger att de känner till säkerhetsriskerna

46%
kvinnorna uppger att de inte känner till säkerhetsriskerna

40%
uppger att de inte känner till säkerhetsriskerna

74%
uppger att de känner till säkerhetsriskerna

Har du kopplat in en privat telefon eller dator på arbetsplatsens nätverk?

Närmare 3 av 10 svenskar har kopplat in en privat telefon eller dator på arbetsplatsens nätverk.

29%
har kopplat in en privat telefon eller dator på arbetsplatsens nätverk

71%
har ej kopplat in en privat telefon eller dator på arbetsplatsens nätverk

Har du någon gång fått virus eller misstänkt att du har fått virus på din arbetsdator?

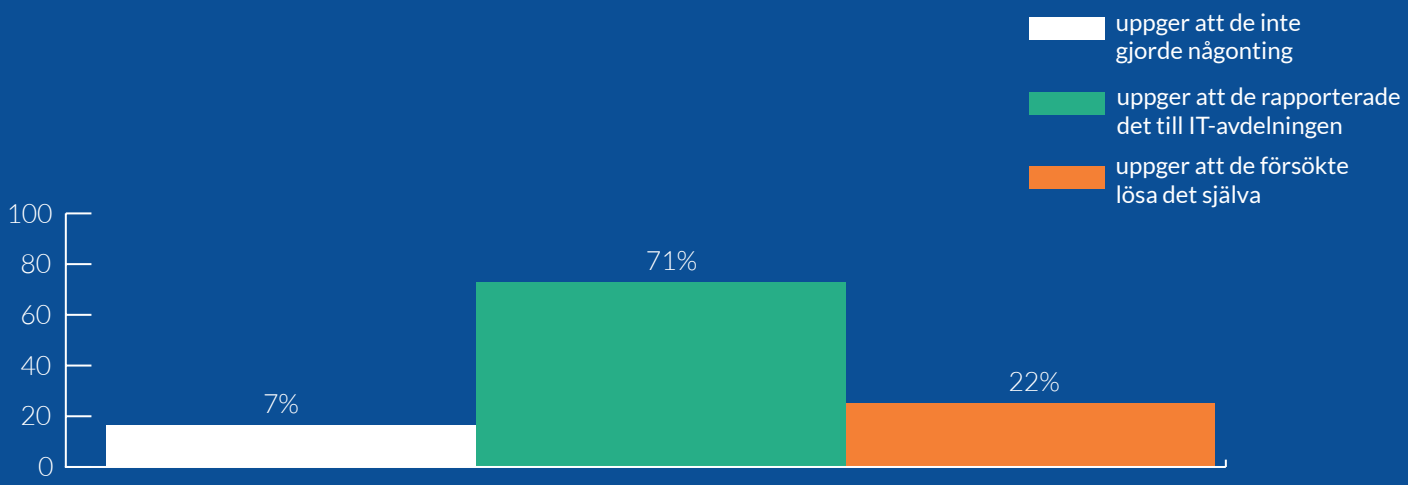
1 av 10 har fått eller misstänker att de har fått virus på arbetsdatorn.

88%
uppger att de varken har fått eller misstänker att de har fått virus på sin arbetsdator

12%
uppger att de har fått eller misstänker att de har fått virus på sin arbetsdator

Hur hanterade du den situationen?

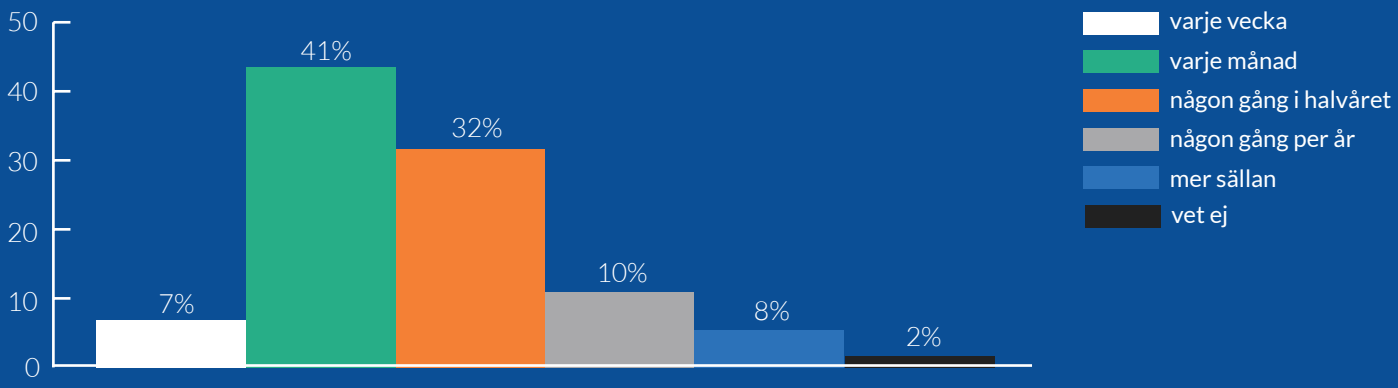
3 av 10 svenskar som har drabbats av virus på sin arbetsdator försökte antingen lösa problemet själva eller ignorerade det helt.



Säkerhet och e-handel

Hur ofta e-handlar du?

Närmare hälften av svenskarna e-handlar varje månad eller oftare.



Har du handlat något (ex. kläder, biljetter, hemelektronik) över nätet under tiden du var uppkopplad mot ett offentligt/publikt trådlöst nätverk?

2 av 10 av de som e-handlar har någon gång gjort det via ett offentligt nätverk.

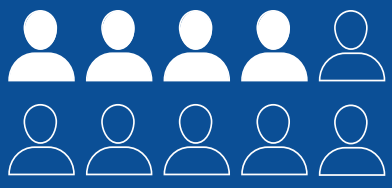
11%
vet inte om de har varit uppkopplade mot ett offentligt/publikt trådlöst nätverk när de e-handlat

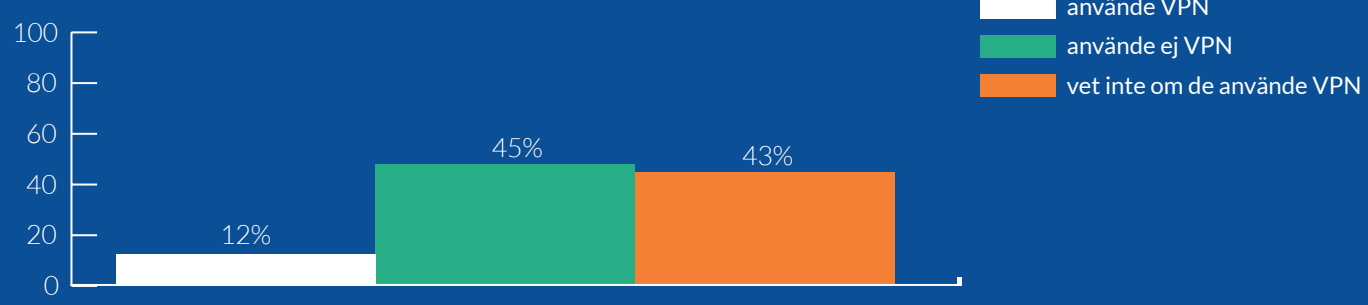
67%
har inte varit uppkopplade mot ett offentligt/publikt trådlöst nätverk när de e-handlat

22%
har varit uppkopplade mot ett offentligt/publikt trådlöst nätverk när de e-handlat

Använde du VPN vid detta köp?

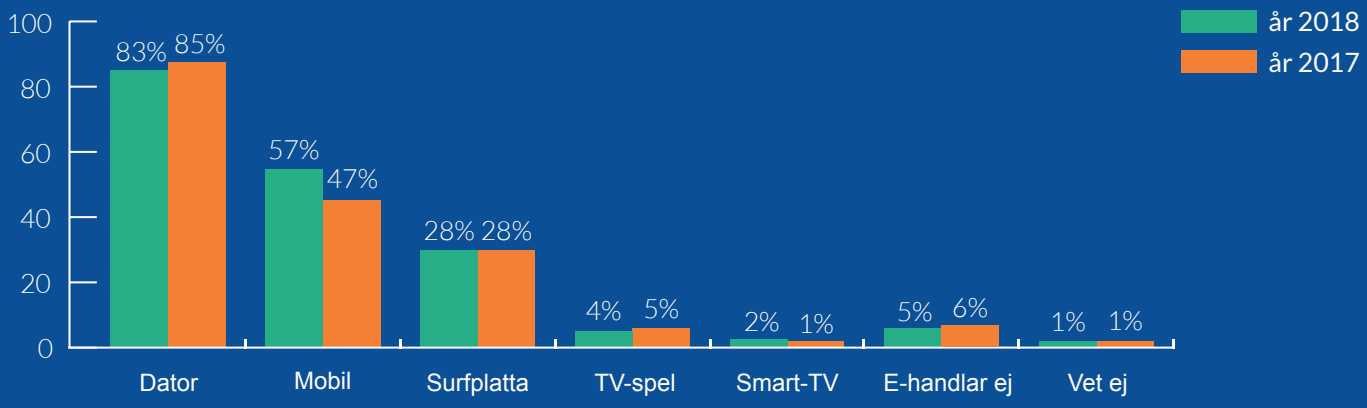
VPN är en teknik som används för att skapa en säker förbindelse i ett icke-säkert datanätverk. Vetskapen om att denna teknik existerar är däremot liten. Fler än 4 av 10 svarar att de inte vet om de använde VPN vid köptillfället.





Vilken/vilka enheter använder du för att genomföra dina e-handelsköp?

Trots den digitala utvecklingen är datorn fortfarande den mest använda enheten för att genomföra e-handelsköp. Samtidigt blir det allt vanligare att genomföra e-handelsköp via mobilen.



Vad av följande skulle få dig att avbryta en transaktion på en för dig ny e-handelswebbplats?

8 av 10 anser att språket på hemsidan påverkar deras köpbeslut och kan leda till att de väljer att avbryta köpet.

82%
hävdar att en hemsida med språkliga fel får dem att avbryta en transaktion

81%
avbryter ett köp om de får en varning i webbläsaren om att företagets säkerhetscertifikat ej är tillförlitligt

74%
avbryter ett köp om företaget fått tveksamma referenser/omdömen i sociala medier

52%
uppger att de avbryter ett köp om de använder ett publikt/offentligt nätverk

51%
avbryter ett köp om företaget saknar en trovärdig om-oss-sida

50%
avbryter ett köp om företaget inte använder HTTPS (dvs. det saknas ett grönt hänglås i adressfältet i webbläsaren)

42%
avbryter ett planerat köp om de måste uppge sitt personnummer

39%
avbryter ett köp om företaget utannonserar ett väsentligt lägre pris än branschstandard

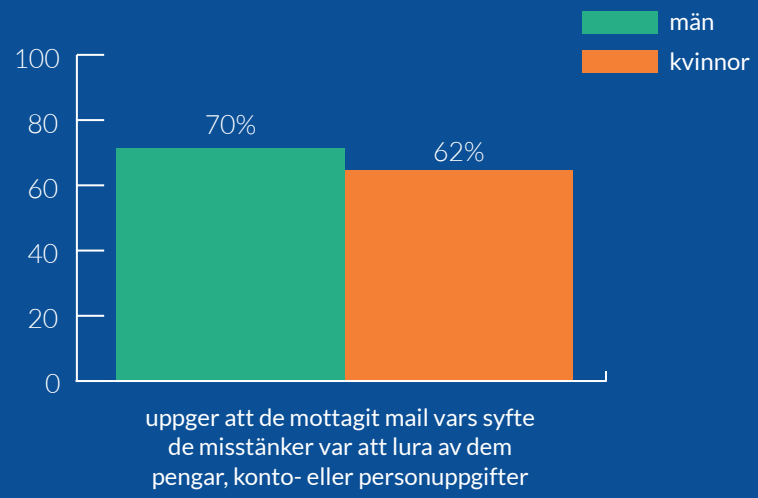
Nätfiske och bedrägerier

Har du (under de senaste 12 månaderna) mottagit mail vars syfte du misstänker var att lura av dig pengar, konto- eller personuppgifter?

Fler svenskar svarar att de mottagit mail med bedrägerisyfte i år (66 procent) jämfört med förra året (62 procent).

66%

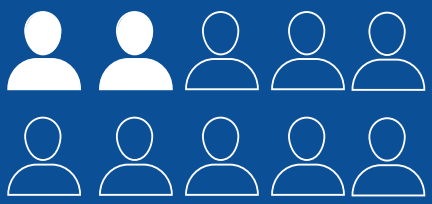
uppger att de mottagit mail vars syfte de misstänker var att lura av dem pengar, konto- eller person-uppgifter

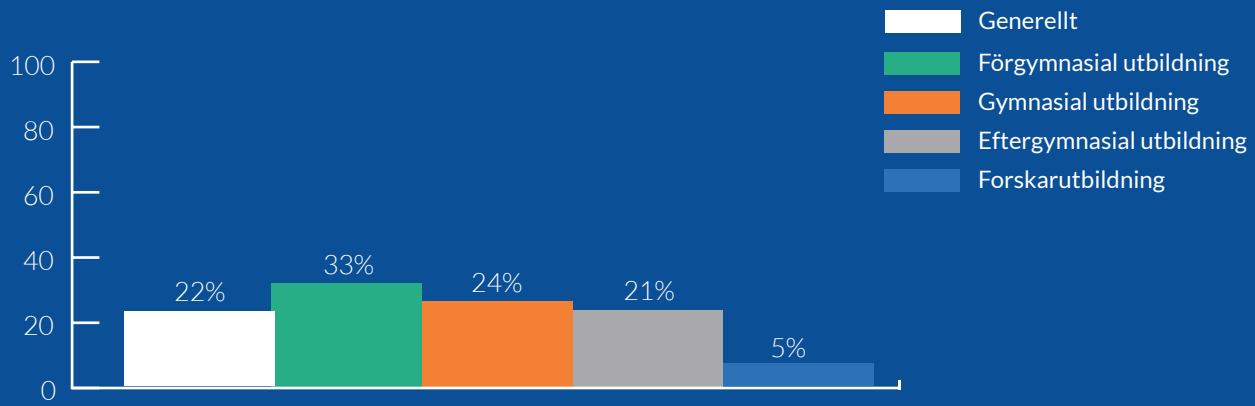


uppger att de mottagit mail vars syfte de misstänker var att lura av dem pengar, konto- eller personuppgifter

Har du svårt att avgöra om mail är legitima från en verklig avsändare eller om de är bluffmail från en falsk avsändare?

2 av 10 svenskar har svårt att avgöra om mail kommer från en verklig avsändare eller ej.

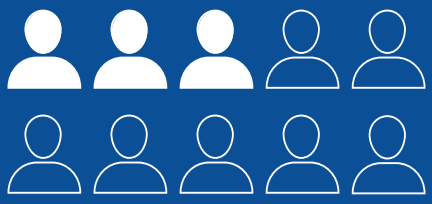




tycker det är svårt att avgöra om mail är från en verklig avsändare eller ej

Har du någon gång blivit kontaktad av en person via sociala medier som du misstänker är ute efter din känsliga information?

3 av 10 svarar att de har blivit kontaktade av en person via sociala medier som var ute efter känslig information.



30%
har blivit kontaktade

70%
har inte blivit kontaktade

Skulle du låna ut pengar om någon kontaktar dig över internet? (flera val är möjliga)

Att låna ut pengar över internet kan vara riskabelt, trots det hävdar 1 av 10 att de skulle låna ut pengar om en bekant kontaktade dem.

88%
skulle inte låna ut pengar till en bekant

8%
skulle låna ut pengar till en bekant

1%
skulle låna ut pengar om mailet var tillräckligt trovärdigt

3%
vet inte hur de skulle göra

Hackare utnyttjar e-post för attacker

Nätfiske eller phishing som det också kallas handlar om att någon utger sig för att vara exempelvis en bank, myndighet eller kanske ett företag i syfte att få tillgång till känsliga uppgifter såsom inloggningsuppgifter eller kreditkortuppgifter. Det har på senare år blivit vanligare med nätfiske riktat till utvalda grupper av mottagare som får anpassat textinnehåll. Ibland förekommer rentav personligt adresserade mejl som ser ut att komma från ens kontakt på företaget eller en bekant.

I år uppger fler att de mottagit mail vars syfte de misstänker var att luras på pengar eller känsliga uppgifter än förra året. Ser du en ökning av den här typen av nätfiske även bland företag?

Vi ser en klar ökning av epost som angreppsvektor, både för nätfiske och för att infektera datorer med virus. Vi ser också trender över året där det förekommer fler försök runt tider där det skickas mycket mail och mailreklam, värst brukar det vara runt jul.

Fyra procent av svenskarna uppger att de har drabbats av skadlig kod som krypterat filer på datorn. Andelen som skulle vara beredd att betala 1000 kronor för att få tillgång till sina filer igen om de har blivit krypterade har ökat jämfört med 2017. Ska man betala för att få tillbaka sina filer, eller finns det några risker med det?

Jag avråder alltid från att betala då det inte finns någon garanti för att man faktiskt får tillbaka sina filer. Det finns dessutom rent moraliska betänkligheter med att betala, vi vet att vissa grupperingar som sysslar med den här typen av IT-brott också ägnar sig åt andra typer av organiserad brottslighet.
Om man trots allt känner sig tvungen att betala så är det viktigt att komma ihåg att datorn fortfarande är virusinfekterad även efter det att du fått tillbaka kontrollen. Installera om datorn från grunden och ta hjälp med att flytta filer från din infekterade dator på ett säkert sätt, annars finns det risk att du blir av med allt igen.

2 av 10 har svårt att avgöra om mail är från en verklig avsändare. Finns det några kännetecken man kan leta efter för att avgöra om avsändaren är den den utger sig för att vara eller inte?

Först och främst är det bra att fundera över rimligheten i det mottagna mailet. Hur är mailet formulerat och utformat? Om mailet verkar komma från ett företag bör man fundera på om det är troligt att avsändaren skulle välja att kontakta dig på det här sättet och be om den typen av uppgifter. Om du är det minsta osäker så ring till avsändaren, eller kundtjänsten hos avsändarföretaget (hitta deras telefonnummer på den officiella hemsidan, inte i mailet), för att kontrollera riktigheten i mailet.
Rent tekniskt så går det absolut att göra ett antal kontroller för att kontrollera att avsändaren är riktig, men en avancerad avsändare kan manipulera väldigt mycket för att undgå att bli upptäckt. För vanliga användare rekommenderar jag helt enkelt att man plockar upp telefonen och ringer avsändaren vid minsta misstanke.

Hanna Eldmar
SOC Manager

Lösenordsanvändning

Anser du att ditt lösenord till din mail är säkert?

1 av 5 tycker inte att de har ett säkert lösenord till sin mail.

78%
anser att lösenordet till deras mail är säkert

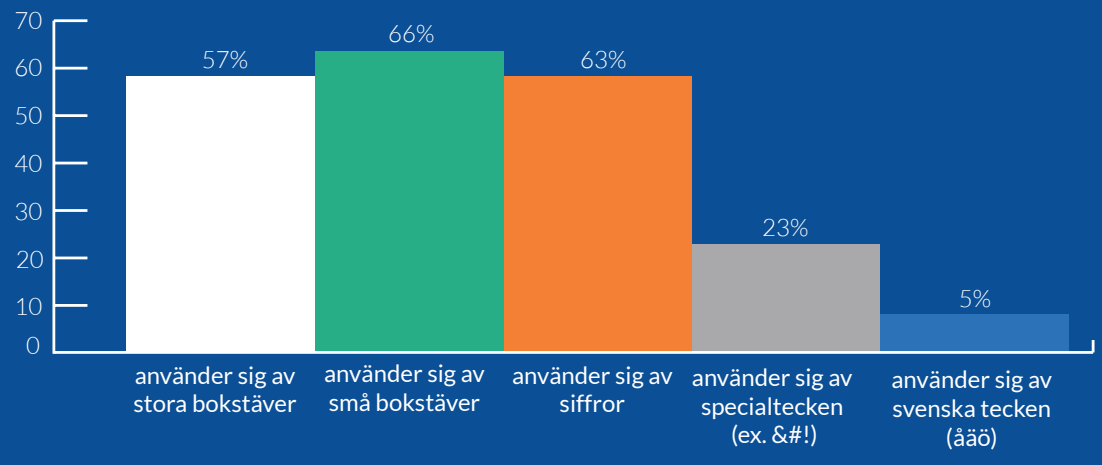
22%
anser inte att lösenordet till deras mail är säkert

Hur många tecken består ditt maillösenord av?

Vanligast är att svenskarna använder 9-12 tecken i sitt maillösenord. Näst vanligast är det att använda 1-8 tecken i sitt lösenord (24 procent).

Inom IT talar man om olika sorter av tecken. Vilka av dessa teckentyper använder du dig av i ditt lösenord till din mail?*

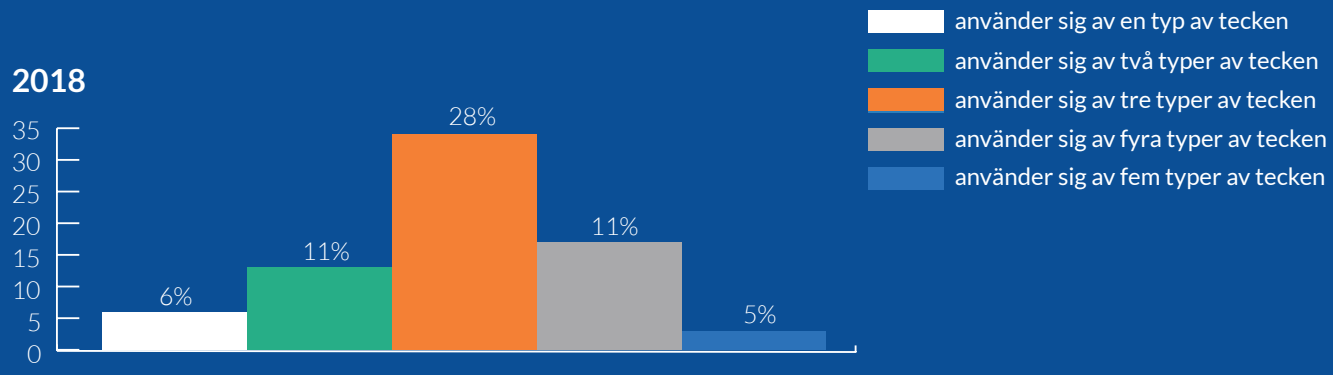
Endast 5 procent av svenskarna använder sig av svenska tecken i sitt lösenord.



*Flervalsfråga, därav över 100% i resultatet.

Hur många av dessa typer av tecken använder du i ditt lösenord?

Det vanligaste är att maillösenordet består av tre typer av tecken.



Använder du samma lösenord till din mail som till andra tjänster på Internet (ex. till sociala medier, e-handelssajter)?

Närmare 1 av 4 uppger att de använder samma lösenord till mailen som till andra tjänster på Internet.

22 %
uppger att de använder samma lösenord till mailen som till andra tjänster på Internet

78 %
uppger att de inte använder samma lösenord till mailen som till andra tjänster på Internet

Ransomware och lagring

Har någon krypterat dina filer (så att du inte kan använda datorn) och använt sig av utpressning där de krävt pengar i utbyte mot att låsa upp de krypterade filerna?

Det är få svenskar som utsatts för en krypteringsattack. Undersökningen visar att 4 procent utsatts, jämfört med 96 procent som inte har utsatts.

4%
uppger att de blivit utsatta för krypteringsattacker

96%
uppger att de inte blivit utsatta för krypteringsattacker

Om du skulle få dina filer låsta/krypterade så att din dator inte gick att använda. Skulle du då vara beredd att betala 1000 kronor i lösensumma för att få tillgång till dessa igen?

Förra året uppgav 12 procent att de skulle betala 1000 kr för att få tillbaka sina filer, i år har siffran ökat till 16 procent.

16%
skulle betala för att få tillgång till sina filer

84%
skulle inte betala för att få tillgång till sina filer

Gör du backup/säkerhetskopior av din viktigaste information på datorn (ex. dokument, bilder)?

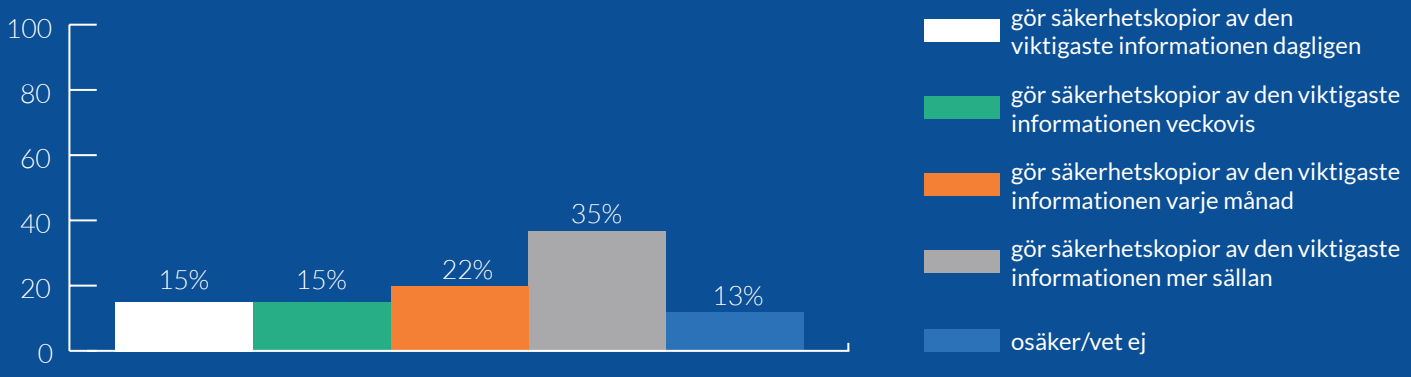
7 av 10 gör säkerhetskopior av den viktigaste informationen på sin dator.

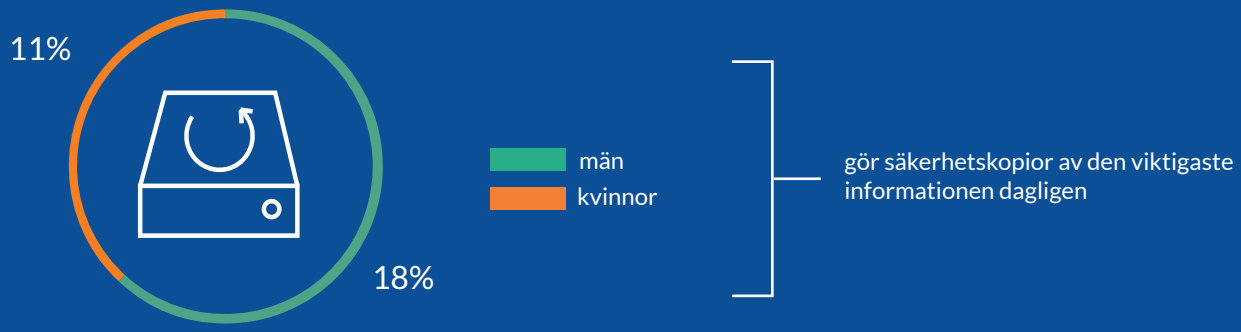
71%
gör säkerhetskopior av den viktigaste informationen på sin dator

29%
gör inte säkerhetskopior av den viktigaste informationen på sin dator

Hur ofta gör du backup/säkerhetskopior av din viktigaste information?

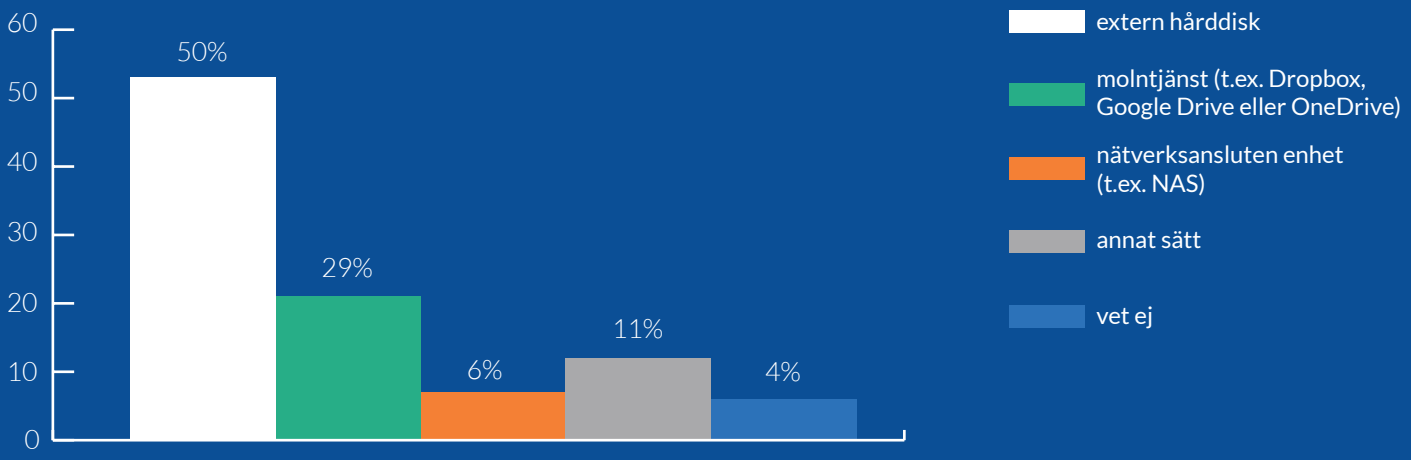
Att säkerhetskopiera innehållet i datorn är relativt vanligt. Fler än hälften säkerhetskopierar viktig information minst en gång i månaden.





På vilket sätt gör du primärt backup/säkerhetskopior på din viktigaste information? (flera val är möjliga)

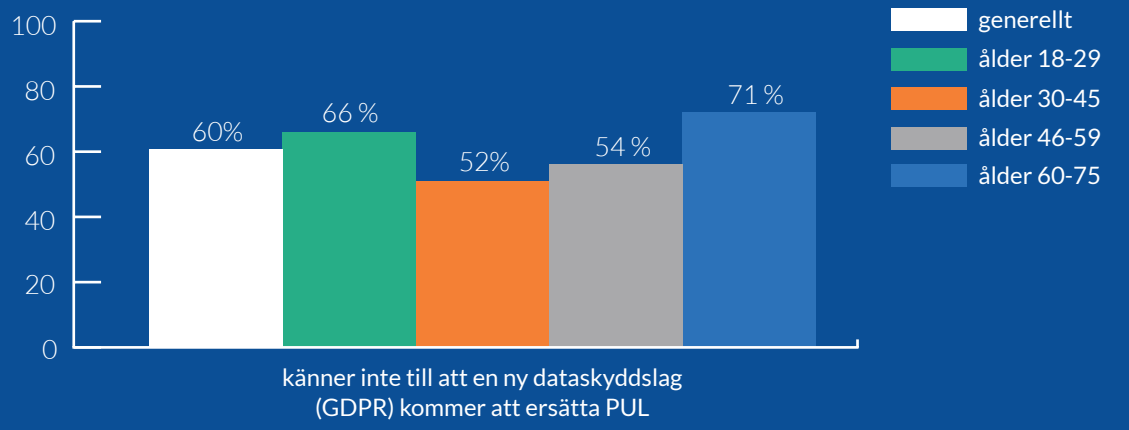
Användandet av molntjänster som backuprutin har ökat från 21 procent 2017 till 29 procent 2018.



Personuppgifter och integritet

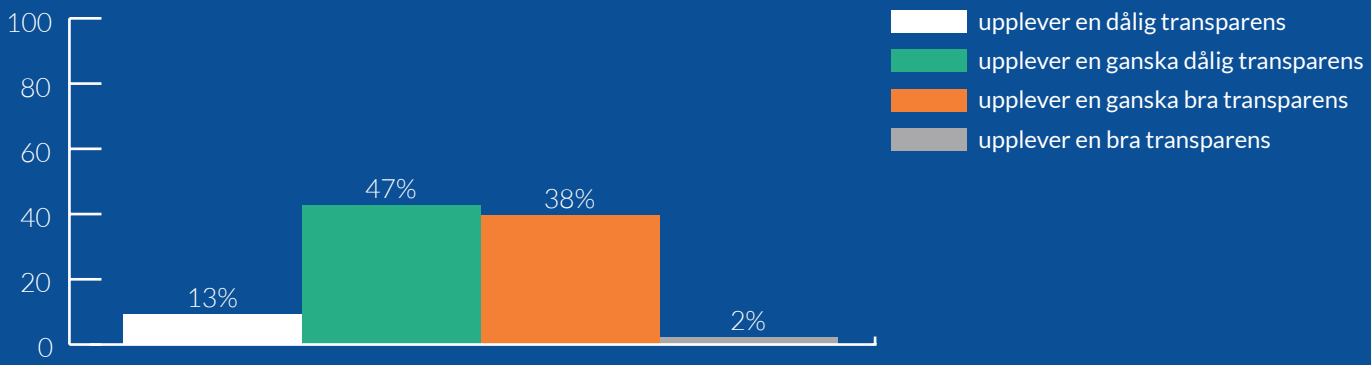
Känner du till att en ny dataskyddslag, General Data Protection Regulation (GDPR), kommer att ersätta Personuppgiftslagen (PUL) från och med maj 2018?

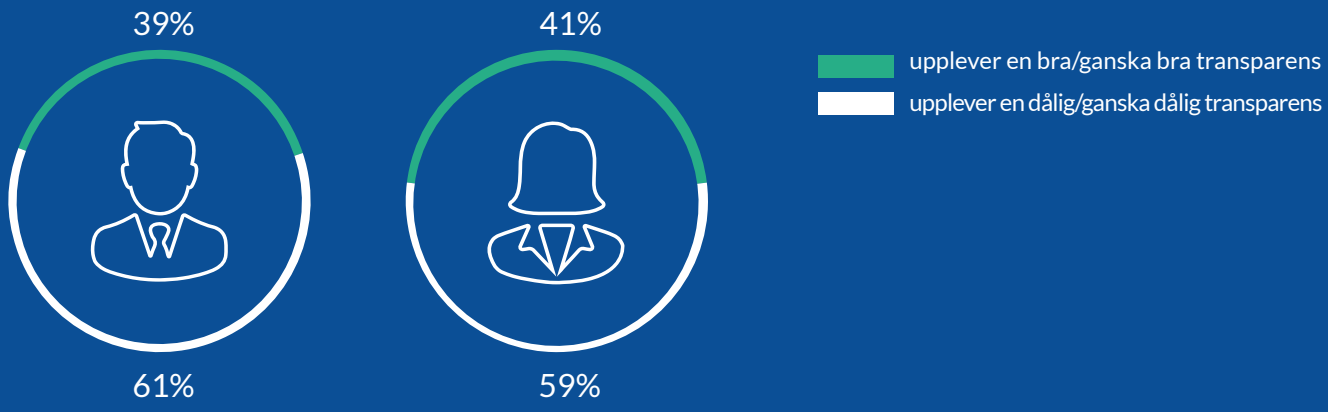
60 procent uppger att de inte känner till att PUL kommer ersättas av en ny dataskyddslag (GDPR), jämfört med 2017 då 87 procent svarade att de inte kände till den nya dataskyddslagen.



Hur transparenta tycker du svenska organisationer är på sina webbsidor gällande datainsamling och hur data används (exempelvis när du fyller i ett formulär på en webbplats)?

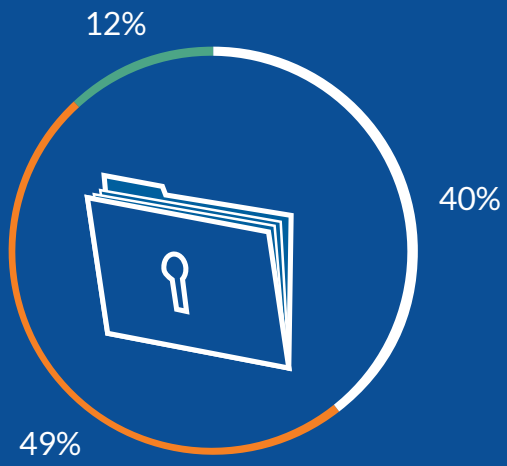
Närmare 6 av 10 anser att svenska organisationer brister i transparens gällande hur data används. Fler män än kvinnor upplever en bristande transparens.





Hur uppfattar du möjligheten att återkalla ditt samtycke (att be dem ta bort information om dig i sina system) hos organisationer som fått möjlighet att lagra din information?

Det är generellt låg kännedom om möjligheten att återkalla information. 40 procent vet inte vilka möjligheter de har att återkalla information och 49 procent menar att det är ganska, eller mycket svårt att återkalla information.



- uppger att det är enkelt/mycket enkelt att återkalla information
- uppger att det är svårt/mycket svårt
- vet ej vilka möjligheter de har att återkalla information

Skulle du samarbeta (till exempel handla av, stödja, använda deras tjänst) med en organisation som missbrukat personlig data (till exempel sålt vidare personlig information och/eller bilder)?

Nästan samtliga svenskar skulle inte samarbeta med en organisation som missbrukat personlig data.

5%
skulle samarbeta med en organisation som missbrukat personlig data

95%
skulle inte samarbeta med en organisation som missbrukat personlig data

Kännedomen om GDPR har ökat kraftigt

I maj i år trädde den nya dataskyddslagen GDPR i kraft. Förra året var den allmänna kännedomen om GDPR dock låg, endast 13 % kände till den. I år är motsvarade siffra 40 %.

Hur ser du på de siffrorna?

Det har varit mycket skriverier i media om GDPR och vad det innebär för individen. Det kombinerat med att många svenskar har fått ta emot e-post från organisationer som strävar efter att efterleva lagen, har förmodligen lett till att medvetenheten bland allmänheten har ökat.

GDPR ställer krav på transparens kring hur personuppgifter används. 60 % svarar att de upplever att svenska organisationer har dålig eller ganska dålig transparens på sina webbsidor gällande datainsamling och hur data används (exempelvis när du fyller i ett formulär på en webbplats). Hur bör företag arbeta för att vända de siffrorna?

GDPR tvingar företag att bli mer transparenta kring hur personuppgifterna används. Många har haft som prioritet att uppdatera sin integritetspolicy och uppdatera informationen i anslutning till formulär som man har på sin hemsida. Har man inte tagit tag i det här arbetet, ligger man efter och borde ta tag i det omgående för att efterleva lagen.
I grunden är GDPR något positivt i och med att det stärker skyddet för den enskilda individen. Genom att visa att man tar det här arbetet på allvar visar man också att man är en seriös aktör att göra affärer med.

Owe Strömbäck
Compliance Service Delivery Manager

Den generella kännedomen kring möjligheten att återkalla information är fortsatt låg under 2018. Bara 12 % upplever att det är enkelt att återkalla sitt samtycke till att lagra information om dem i sina system. Är det företagens skyldighet att tillhandahålla tydlig information om detta?

Ja, det ska tydligt framgå att det är möjligt att återkalla sitt, eller sina samtycken, och hur det kan göras. Enligt GDPR har varje individ rättighet att återkalla sitt samtycke, men också att få sina uppgifter rättade, raderade och flyttade.

Under fjolåret och de första månaderna 2018 har många organisationer kämpat med att förbereda sig inför GDPR. Vilka utmaningar skulle du säga att dessa organisationer står inför nu efter att lagen har trätt i kraft?

Det är lätt att stirra sig blind på att allt ska vara klart den 25 maj. Men det stora arbetet återstår, för nu ska alla organisationer efterleva GDPR över tid. Det ställer krav på andra arbetsmetoder och utan någon form av ledningssystem blir det svårt att säkerställa att arbetet sker på rätt sätt.

Vad innebär GDPR, och hur påverkar det individen och företagen?

GDPR (General Data Protection Regulation) trädde i kraft den 25 maj 2018 och ersatte därmed Personuppgiftslagen (PUL). Lagen gäller för alla medlemsländer i EU, samt för företag som behandlar EU-medborgares personuppgifter.

Vad är en personuppgift?

En personuppgift är en uppgift som på egen hand eller i kombination med andra uppgifter kan identifiera en person. Det kan till exempel vara namn, personnummer, e-mailadress, IP-adress, politiska åsikter eller sexuell läggning.

Vad innebär GDPR för individen?

GDPR är ett regelverk som är utformat för att stärka individens rättigheter och personuppgiftsskydd. I praktiken innebär det att lagen ger dig bättre insyn i hur, varför och när företag och organisationer behandlar dina uppgifter, samt mer kontroll över vilken information du vill ta del av genom krav på samtycke. Du kan när som helst upphäva ditt samtycke eller begära att få dina uppgifter:

- Rättade
- Raderade
- Flyttade
- Uttagna

Du har även rätt att bli informerad om dina uppgifter har eller riskerar att ha läckt vid en säkerhetsincident, exempelvis vid ett dataintrång.

Vad innebär GDPR för företagen?

För företag och organisationer innebär den nya lagen främst olika typer av skyldigheter. En av dem är att informera dig som individ om hur och varför dina uppgifter samlas in och behandlas, samt för vilket syfte.

Vid dataintrång eller dataförlust har företaget en skyldighet att rapportera händelsen till Datainspektionen inom 72 timmar efter det att incidenten har upptäckts. Om incidenten kan innebära en risk för individen, till exempel vid bedrägeri eller identitetsstöld, ska även den registrerade informeras om händelsen.

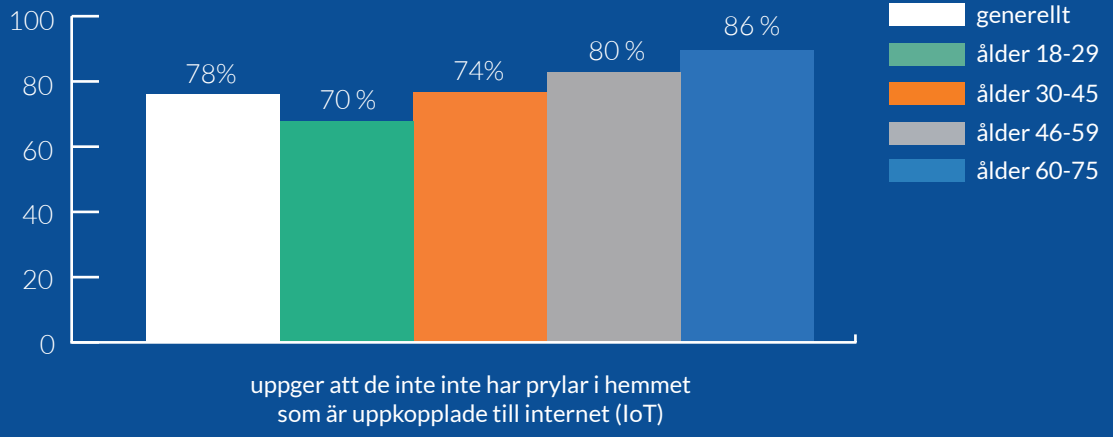
Vad händer om företagen bryter mot lagen?

Jämfört med den tidigare personuppgiftslagen hotar GDPR med avsevärt högre böter för de organisationer som inte efterlever den. Vid allvarliga brott riskerar företag böter på upp till 20 miljoner euro eller fyra procent av den globala årsomsättningen.

Internet of things

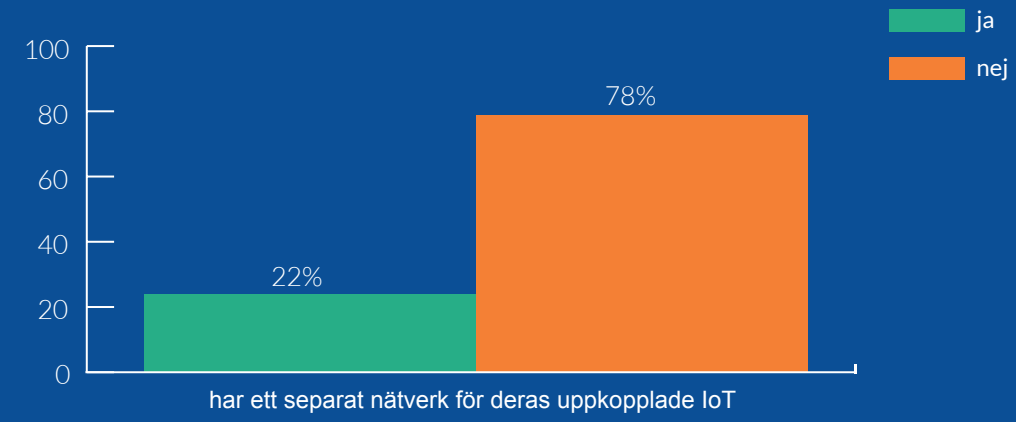
Innehar du prylar i ditt hem som är uppkopplade till internet (IoT), som ex. högtalare, övervakningskameror, termostater, hushållsapparater eller lampor?

1 av 5 svarar att de har uppkopplade prylar i hemmet.



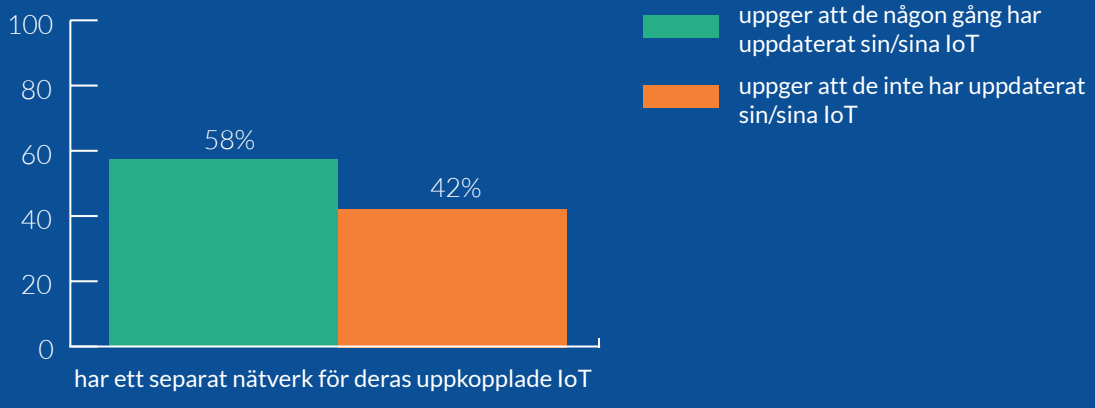
Har du ett separat nätverk för dessa uppkopplade IoT-enheter?

Var femte svensk har ett separat nätverk för deras uppkopplade IoT.



Har du någon gång uppdaterat din/dina IoT?

4 av 10 uppdaterar aldrig sina uppkopplade prylar.



IoT – Internet of Things

Internet of Things (IoT) handlar om anslutningen av vardagliga enheter till internet, alltifrån termostater och lampor till dörrklockor och larm. Tack vare att enheterna är anslutna till internet kan vi på olika sätt dra nytta av nya funktioner och underlätta vår vardag. Men precis som med andra enheter som är anslutna till internet så tillkommer också säkerhetsaspekter att ta hänsyn till.

Trenden med IoT, Internet of Things, ökar i de svenska hushållen. Var femte person har saker i hemmet som är uppkopplade till internet, som exempelvis högtalare, övervakningskameror, termostater, hushållsapparater eller lampor. Ser du några risker med att koppla upp dessa prylar?

Tyvärr har de flesta leverantörerna av dessa typer av enheter inte tagit säkerheten på allvar, utan tycks mest ha fokuserat på att snabbt få ut produkter på marknaden. De har även slarvat med att tillhandahålla säkerhetsuppdateringar till redan levererade enheter, vilket har resulterat i att Internet allt snabbare fylls med sårbara prylar. Detta utgör en risk både för konsumenten själv och resten av Internet, eftersom hackade prylar ofta används i attacker mot andra offer.

Enligt rapporten har bara en av fem som har IoT-enheter ett separat nätverk för dessa. Vad kan hända om man kopplar upp sakerna på sitt vanliga nätverk?

Många enheter försöker konfigurera öppningar i nätverkets brandvägg, i syfte att göra sig nåbara direkt från Internet. Om enheten exponerar någon tjänst med en allvarliga säkerhetsbrist så kan denna i värsta fall utnyttjas av en angripare för att få ett fotfäste i det interna nätverket. Angripare kan sedan nyttja denna åtkomst för att attackera andra enheter på nätverket.

Joel Rangsmo,
Teknisk säkerhetskonsult på Sentor

4 av 10 uppger att de inte har uppdaterat sina uppkopplade prylar. Varför är det viktigt att hålla sina prylar uppdaterade?

Även prylar med enkla arbetsuppgifter, såsom en smart glödlampa, bygger på komplex mjukvara och ett underliggande operativsystem. Nya sårbarheter upptäcks kontinuerligt i dessa typer av enheter, som ofta endast kan åtgärdas genom mjukvaruuppdateringar.

Vad ska man som privatperson tänka på om man har eller funderar på att koppla upp prylar i hemmet mot internet?

När man väljer prylar att köpa bör man försöka hålla sig till leverantörer som historiskt sett tagit säkerhet på allvar. När man väl har installerat en enhet är det viktigt att hålla koll på när nya uppdateringar släpps och att leverantören fortfarande underhåller enheten. Har man kunskap och möjlighet att sätta upp ett dedikerat nätverk för sina smarta prylar kan detta minska konsekvenserna av eventuella säkerhetsbrister.

Hantering av uppdateringar

Hur hanterar du uppdateringar av operativsystemet till din smartphone (ex. Android, iOS)?

Knappt en tredjedel använder automatiska uppdateringar av operativsystem till smartphone.

30%
uppger att de har automatiska uppdateringar/uppdaterar inom en dag

25%
uppger att de uppdaterar när applikationer eller annat säger att de måste för att telefonen ska fungera som den ska

21%
uppger att de uppdaterar inom en vecka från att de har meddelats

8%
uppger att de uppdaterar inom en månad från att de har meddelats

10%
uppger att de inte vet eller har ingen uppfattning

6%
uppger att de inte har en smartphone

Hur hanterar du uppdateringar av appar till din smartphone (ex. Facebook, Instagram, BankID m.m.)?

1 av 4 har automatiska uppdateringar av appar till smartphone.

39%
uppger att de har automatiska uppdateringar/uppdaterar inom en dag

24%
uppger att de uppdaterar när applikationer eller annat säger att de måste för att telefonen ska fungera som den ska

18%
uppger att de uppdaterar inom en vecka från att de har meddelats

5%
uppger att de uppdaterar inom en månad från att de har meddelats

9%
uppger att de inte vet eller har ingen uppfattning

5%
uppger att de inte har en smartphone

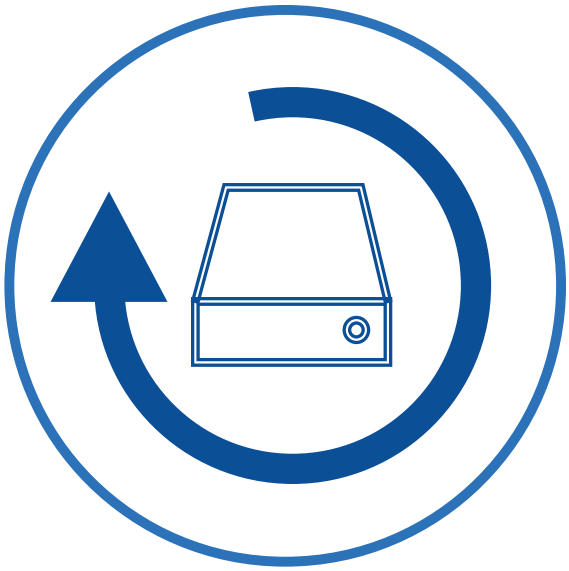
3 anledningar till att hålla sina enheter uppdaterade.

1. Täta till säkerhetshål

Det främsta skälet till att hålla sina enheter uppdaterade är att skydda dem mot säkerhetsbrister. När leverantörerna släpper nya uppdateringar är det inte ovanligt att de innehåller säkerhetsfixar på kända sårbarheter. Därför är det viktigt att alltid uppdatera operativsystem och applikationer när nya uppdateringar släpps.

2. Ökad funktionalitet

Nya uppdateringar innebär många gånger nya funktioner. Det kan handla om funkioner som gör enheten enklare att använda, så som kortkommandon. Men det kan också vara funktioner som ökar säkerheten, till exempel tvåfaktorsautentisering.



3. Bättre prestanda

När nya uppdateringar av operativsystem släpps förändras förutsättningarna för applikationerna. Det kan till exempel handla om att skärmen eller kameran kan få bättre prestanda eller att notifikationssystemet förändras. Då måste applikationerna vara anpassade efter de nya förutsättningarna för att kunna ta del av förbättringarna. Om man istället ignorerar uppdateringarna kan man tvärtom förvänta sig försämrad prestanda på sina applikationer.

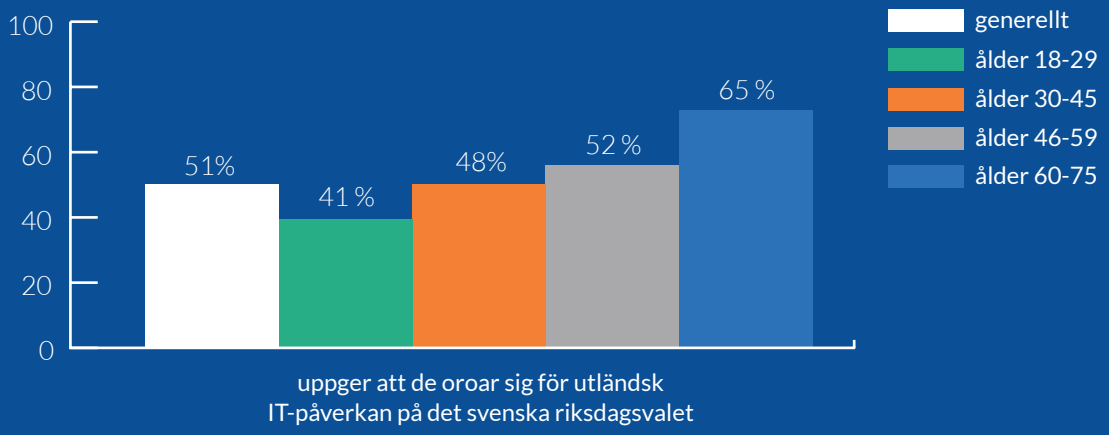
Vad bör uppdateras?

- Operativsystem
- Enskilda applikationer
- Webbläsare
- Insticksprogram till webbläsaren, till exempel Flash och Java.

Valpåverkan

Är du orolig för att andra länder med hjälp av IT-säkerhetsrelaterade åtgärder kommer att försöka påverka det svenska riksdagsvalet (likt det som ev. hänt i USA och Frankrike)?

Varannan svensk oroar sig för utländsk IT-säkerhetspåverkan kopplat till det svenska riksdagsvalet.



uppger att de oroar sig för utländsk IT-påverkan på det svenska riksdagsvalet

Cyberattacker och riksdagsvalet

I samband med det amerikanska presidentvalet har det varit mycket diskussion om huruvida utländska cyberattacker påverkade valet. Enligt en rapport från de amerikanska underrättelsetjänsterna FBI, CIA och NSA beordrade Vladimir Putin en större cyberattack i syfte att underminera den demokratiska processen, hjälpa Donald Trump att vinna och svartmåla Hillary Clinton.

I Sentors rapport uppger varannan svensk att de oroar sig för cyberattacker från andra stater i syfte att påverka det svenska riksdagsvalet. Vilka skäl skulle en främmande stat ha, när de i så fall skulle iscensätta cyberattacker i syfte att påverka valutgången i Sverige?

Dels har olika partier olika syn på utrikespolitiken, vilket innebär att Sveriges agerande mot andra länder påverkas av valutfallet i förlängningen. Såväl privata som statliga aktörer som har att vinna på vissa scenarion kan också tänkas ha intresse i att påverka valet med hjälp av tvivelaktiga medel för att öka sannolikheten för dessa situationer.

Därtill finns exempel på kampanjer med syfte att öka motsättningarna inom länder genom att öka polariseringen i debatten. Syftet bakom detta kan till exempel vara att destabilisera politiken för att försvaga landets politiska ställning internationellt.

Röstningen i Sverige sker idag fysiskt medan flera andra länder har digitaliserat röstningsförfarandet. Tror du att vi inom en närmare framtid kommer att gå över till e-röstning av något slag? Om inte, varför? Vilka är riskerna?

Beroende på vilken typ av system man talar om finns olika sorters problem. En av de centrala principerna i det svenska röstsystemet är att rösterna skall vara anonyma, för att förhindra att någon röstberättigad kan påverkas via hot eller belöning. Att garantera något sådant om medborgare tillåts rösta via internet är i stort sett omöjligt.

Skall man rösta via sina egna datorer eller telefoner blir det dessutom väldigt svårt att verifiera att dessa är fria från skadlig kod som skulle kunna manipulera rösterna.

Om man ser till ett system där man röstar elektroniskt i vallokaler så är vinsterna här begrän-

sade i jämförelse med dagens system, samtidigt som man öppnar upp för många nya risker. Förutom risken att delar av hård- eller mjukvara är avsiktligt manipulerad eller innehåller brister som en angripare kan utnyttja för att påverka resultatet, räcker det att misstankar om detta sprids för att underminera den demokratiska processen.

Därtill måste man hantera frågor om attacker mot infrastruktur som elnät och internet. Ett strategiskt strömavbrott i rätt vald del av Sverige skulle kunna tänkas påverka utfallet när ett sådant val måste tas om.

Så även om man kan lösa de rent IT-säkerhetsmässiga frågorna så tillkommer så många andra problem att jag har svårt att se att vinsten skulle väga upp detta på ett nationellt plan. Inom lokalpolitiken används ju däremot redan elektroniska omröstningar på vissa håll för frågor av mindre känslig natur.

Det är inte bara valmyndigheten och enskilda individer som kan bli utsatta för cyberattacker. Även de politiska partierna kan vara föremål för attacker. Vilka uppgifter sitter de på som kan vara intressanta för en angripare?

Politiker i riksdagen får ta del av sekretessklassad information som naturligtvis kan vara av intresse för aktörer både inom och utanför rikets gränser.

När det gäller information inom ett parti så är det kanske framförallt information om kampanjarbete som kan vara av intresse för andra partier eller angripare som vill påverka valresultatet, men som inom alla organisationer kommuniceras förstås en del information av privat natur eller personliga förhållanden som man önskar minimera spridningen på.

68 procent av svenskarna uppger att de har lågt eller mycket lågt förtroende för politiska partiers förmåga att skydda känslig data. Vilken skulle du säga är den största utmaningen för de politiska partierna kopplat till IT-säkerhet?

Användare med begränsad datorvana som ändå måste hantera känslig information är en utmaning för alla sorters organisationer. Man kan införa en rad system och processer som minskar riskerna, men låter sig en användare ändå luras av en bedragare via mail eller telefonsamtal blir det trots allt ofta möjligt för en angripare att få ett fotfäste.

Allt fler tycker att politiska åsikter är att beteckna som känslig data. Om jag som privatperson vill vara anonym med min politiska hemvist, men ändå vill surfa på sociala nätverk och på webbsidor, vad ska jag då tänka på för att undvika att detta läcker ut?

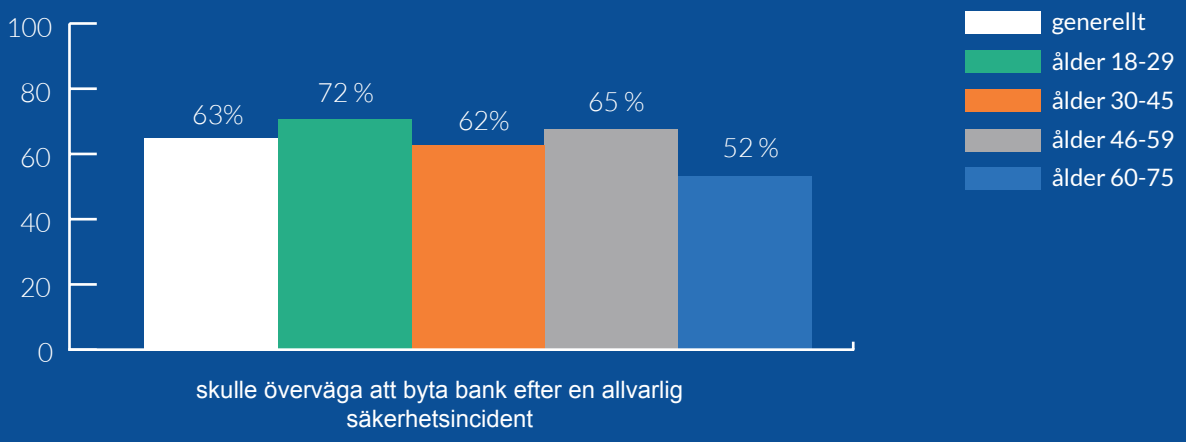
Olika test som delas via sociala nätverk är inte sällan designade för att kartlägga just ens åsikter eller köpvanor, även om kopplingen kanske inte är uppenbar. Man kan i viss mån begränsa att den här informationen läcker genom att använda sig av privat surf-läge; funktionen för att öppna ett nytt privat fönster, som hittas i webbläsarens meny. Detta är dock inte ett komplett skydd; vill man vara säker på att inte spåras behöver man använda någon form av anonymiseringstjänst som TOR eller VPN med tillhörande mjukvara.

Kalle Zetterlund
CTO på Sentor

Banklojalitet

Skulle du överväga att byta bank om det framkom att din bank har drabbats av en allvarlig säkerhetsincident, ex. ett dataintrång?

Svenskar i åldersgruppen 60-75 skulle i lägre grad (48 procent) överväga att byta bank efter en allvarlig säkerhetsincident, jämfört med snittet (37 procent).



Skulle du överväga att byta bank om det framkom att din bank hade missbrukat dina personuppgifter?

Nästa samtliga, oavsett åldersgrupp, skulle överväga att byta bank om denna hade missbrukat ens personuppgifter.

98%

skulle överväga att byta bank om denna hade missbrukat ens personuppgifter.

IT-säkerhet inom bankväsendet

Bank- och finanssektorn har under de senaste åren genomgått stora förändringar. Idag är i princip all traditionell bankverksamhet ersatt med digitala tjänster och infrastruktur som stödjer dessa. Den digitala transformationen har inneburit stora möjligheter för de företag och organisationer som har lyckats anpassa sig efter utvecklingen genom att erbjuda sina kunder användarvänliga och tillgängliga onlinetjänster. Samtidigt exponerar den digitala närvaron den redan utsatta och samhällskritiska bank- och finansbranschen för helt nya risker och hot i form av cyberkriminalitet.

Svenskarna har generellt höga tankar om sina bankers säkerhetsarbete – Bland annat uppger 87 % att de har högt eller mycket högt förtroende för bankernas hantering av känslig information. Anser du att det höga anseendet är befogat?

Ja, de stora bankerna har ett gediget säkerhetsarbete och landet ligger generellt bra till. Samarbetet kring säkerhet, till exempel med BankID, visar att det fungerar bra. Det finns dock mindre banker som kämpar med resurser till säkerhetsarbetet.

Att hanteringen av personuppgifter är viktigt för svenskarna framkommer tydligt i svaren. Nästan samtliga, oavsett grupp, skulle överväga att byta bank om det framkom att denna hade missbrukat ens personuppgifter. Hur ser du på det?

Bankens agerande är ofta genomtänkt. Det som händer nu är att regelverket (PSD2) ändras så att andra företag kan få tillgång till dina konton – med ditt godkännande. Det finns en uppsjö med appar som sammanställer prenumerationer, kontouppgifter etc. Dessa företag kan vara nystartade, med de bästa av avsikter, men som kämpar med mognad och säkerhet i sin produkt. Där finns anledning att vara försiktig.

David Borin
Senior Informationssäkerhetskonsult på Sentor

Finns det något man som privatperson kan göra för att utröna hur väl ens bank hanterar känslig information eller andra säkerhetsaspekter?

De flesta fall där privatpersoner råkar illa ut är när bedragare stjäl din inloggning eller kortinformation. Var försiktig när du laddar ned appar till din Android-telefon eller när okända ringer dig för att lura till sig inloggningar via BankID. Ingen på en riktig bank ringer dig för att be dig logga in – och händer det – be att få ringa tillbaka via växeln.

Om Sentor

Sentor är ett svenskt cybersäkerhetsföretag som arbetar med att skydda samhällsviktiga digitala funktioner och organisationers affärsverksamhet, mot nutida och framtida cyberhot.

Med spetskompetens inom områdena; teknisk IT-säkerhet, informationssäkerhet och managerad säkerhet, kan Sentor täcka stora delar av en organisation digitala säkerhetsbehov.