

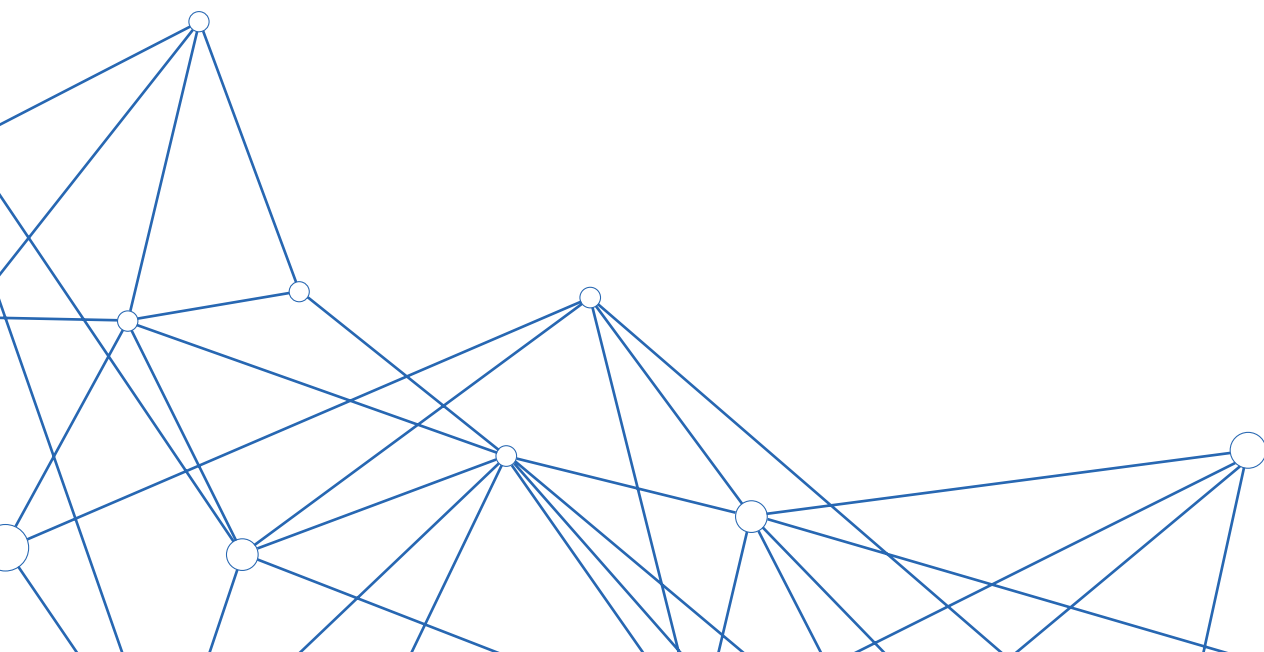
sentor



**Svenskarnas syn på IT-säkerhet
2017**

Innehållsförteckning

Definition av känslig data.....	1
Förtroende för företag och myndigheter	2
IT-säkerhet och e-handel.....	3
Inställning till IT-säkerhet	6
Säkerhet på arbetsplatsen.....	7
Nätfiske.....	11
Säkra lösenord	13
Ransomware och lagring.....	15
Dataskyddslagen (GDPR).....	18
Cyberattacker och spioneri.....	21



Definition av känslig data

Vilken typ av information anser du är känslig data?

Vad som anses vara känslig data varierar. De flesta svenskar är dock överens om att kreditkortsnummer (96 procent) och personnummer (82 procent) är känslig data. 68 procent menar även att IP-adress kategoriseras som känslig data.



96%
anser att kreditkortsnummer
är känslig data



82%
anser att personnummer
är känslig data



68%
anser att IP-adress är
känslig data



35%
anser att politiska åsikter
är känslig data



28%
anser att sexuell läggning
är känslig data



26%
anser att telefonnummer
är känslig data



26%
anser att adress är känslig data



23%
anser att e-postadress
är känslig data

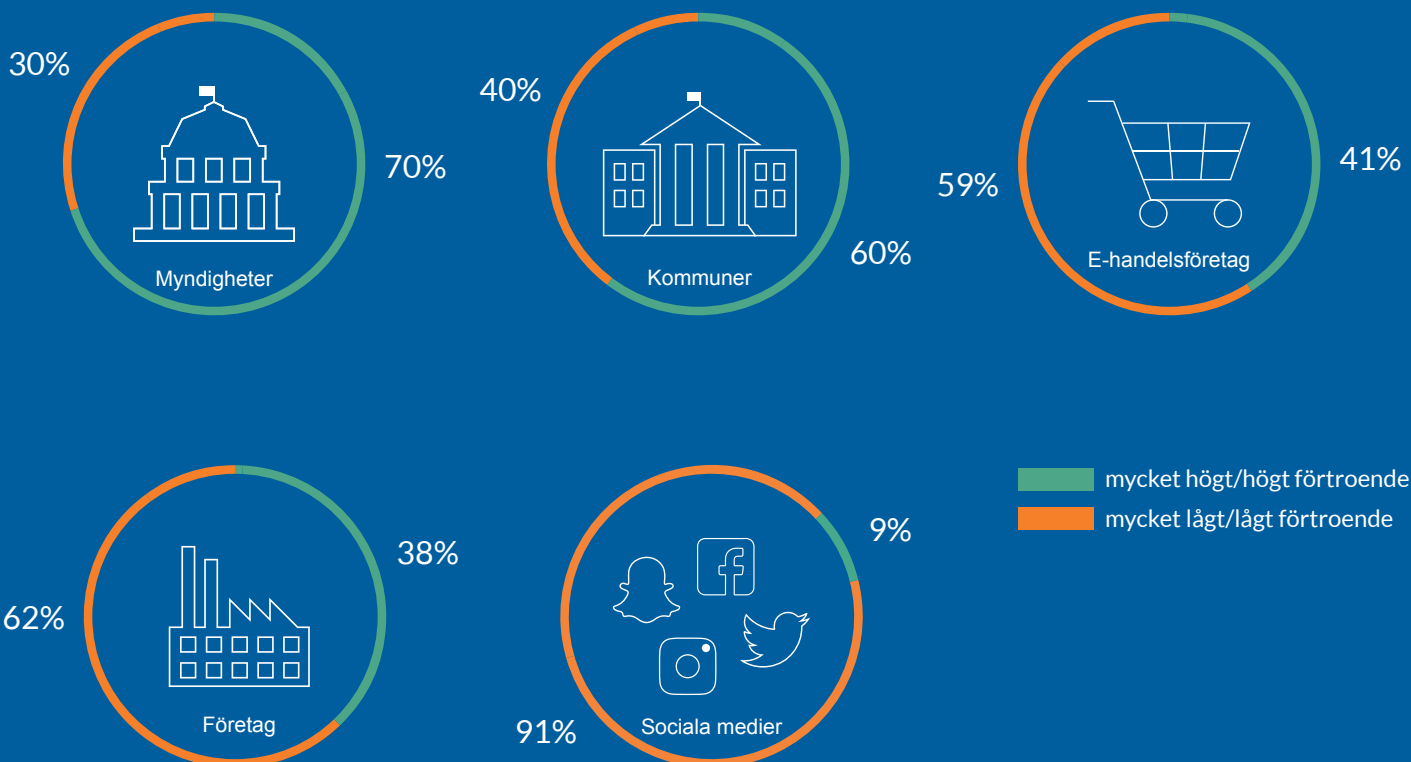


10%
anser att namn är känslig data

Förtroende för företag och myndigheter

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

Många företag och myndigheter har tillgång till känslig data. Precis som föregående år har den svenska befolkningen högre förtroende för offentlig sektor, jämfört med privat sektor. Högt förtroende har svenskarna för myndigheter (70 procent), även om siffran är lägre jämfört med 2016 (79 procent). Endast 38 procent har förtroende för företag, till skillnad från 50 procent föregående år. Lägst förtroende har svenskarna för sociala medier.



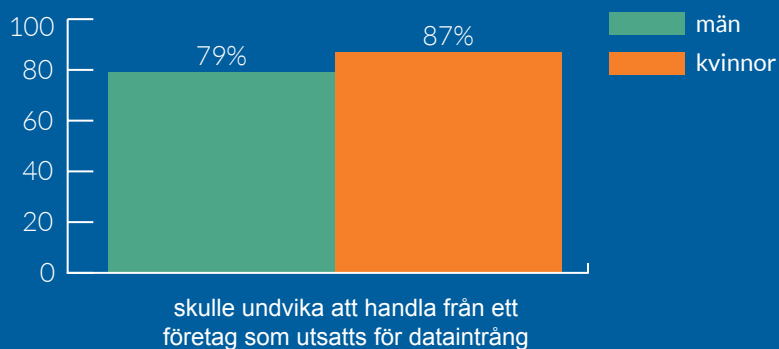
Skulle du undvika att handla från ett företag om du kände till att företaget utsatts för dataintrång?

4 av 5 svenskar uppger att de skulle undvika att handla från ett företag som utsatts för dataintrång. Kvinnor skulle i högre utsträckning undvika att handla från ett företag som drabbats av intrång (87 procent), jämfört med männen (79 procent).



83%

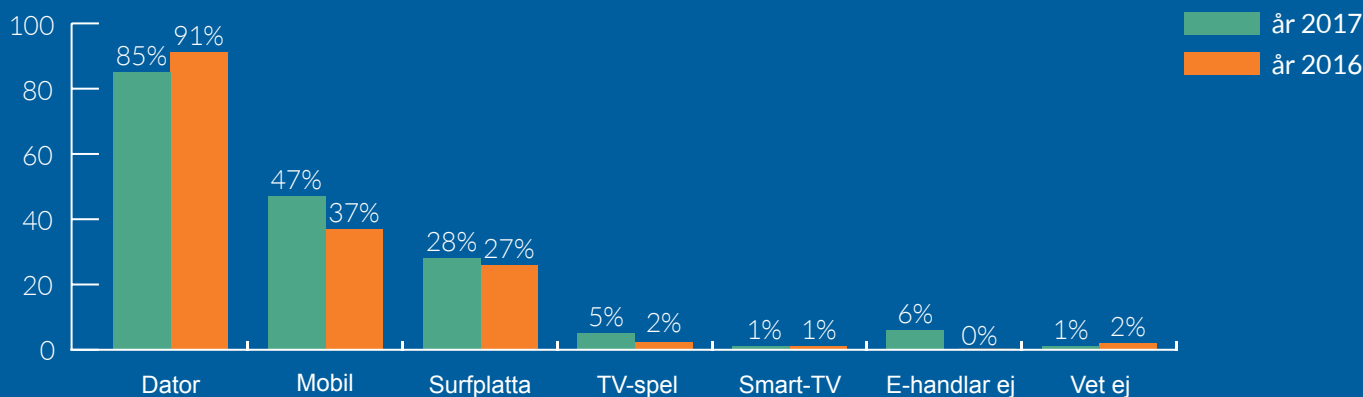
skulle undvika att handla från ett företag som utsatts för dataintrång



IT-säkerhet och e-handel

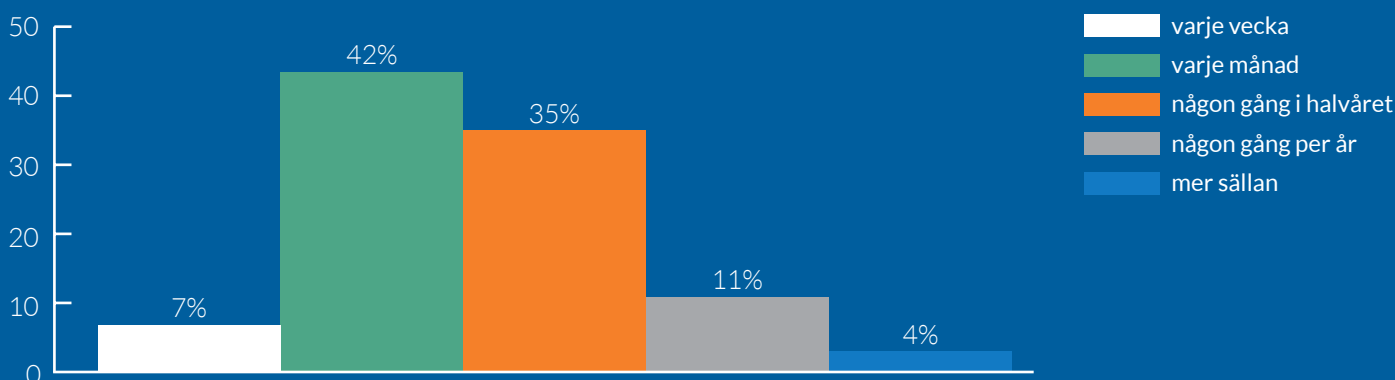
Vilken/vilka enheter använder du för att genomföra dina e-handelsköp?

Datorn är den enhet som flest använder när de genomför e-handelsköp (85 procent). Allt fler har även börjat använda mobilen för detta ändamål. Närmare hälften e-handlar via mobilen 2017, jämfört med 37 procent 2016.



Hur ofta e-handlar du?

5 av 10 e-handlar varje månad eller oftare. Det är lika vanligt bland män att e-handla som bland kvinnor. Även utspritt över åldersgrupper är det relativt vanligt att handla över Internet.



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

2 av 10 som e-handlar har någon gång e-handlat via ett offentligt nätverk. Vidare uppger var tionde svensk att de inte känner till om de varit uppkopplade mot ett offentligt nätverk under tiden som de har shoppat.



10%

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

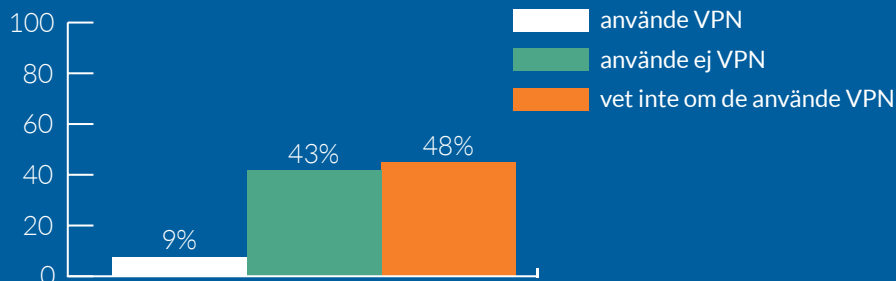
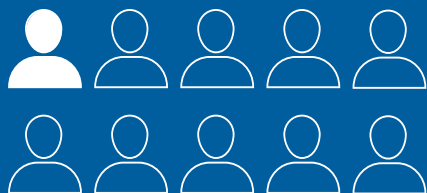


23%

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. Närmare 50 procent vet inte vad VPN innebär och endast 1 av 10 använder VPN.



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

Nästan alla svenskar anser att en hemsida med språkliga fel bidrar till att man väljer att avbryta ett planerat köp. Om man får en varning i webbläsaren, eller om hemsidan fått tveksamma omdömen i sociala medier, är anledningar som också får köparen att tänka efter innan man genomför köpet.

86%

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

83%

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

80%

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

56%

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

56%

uppges att de avbryter ett köp om de använder ett publikt/offentligt nätverk

51%

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

43%

avbryter ett planerat köp om de måste uppge sitt personnummer för köp

42%

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

Många svenskar oförsiktiga vid e-handelsköp

17 procent av svenskarna skulle inte avbryta ett e-handelsköp trots att de fick upp en varning i webbläsaren om att företagets säkerhetscertifikat ej var tillförlitligt. Vad anser du om det och hur illa är det att få upp en sådan varning?

- Det är oroande. Får man upp en varning om att det är problem med webbplatsens säkerhetscertifikat så bör man vara försiktig. Det kan vara en indikation på att någon manipulerar trafiken i syfte att avlyssna din information.

Hälften av svenskarna bryr sig inte om ifall företag de e-handlar ifrån använder sig av HTTPS. Vilka risker finns det med att genomföra ett köp från en sida som ej använder sig av HTTPS?

- Om inte HTTPS används skickas allt mellan webbplats och besökaren i klartext över internet, vilket innebär att någon med onda avsikter kan avlyssna trafiken och exempelvis få fram vilka inloggningsuppgifter du använder eller ditt kreditkortsnummer. Google Chrome har nu börjat uppmärksamma sina användare på när en webbplats använder HTTPS och inte, genom att etikettera med "secure" eller "!" bredvid webbadressfältet.

Om du får ge några råd för att e-handla på ett säkert sätt när man är på resande fot, vilka råd skulle du ge?

- Det bästa rådet jag kan ge är att använda din mobiltelefon som hotspot om du behöver handla online och är på resande fot. Att koppla upp sig mot 4G-nätet är säkrare än att surfa över ett publikt trådlöst nätverk. Sedan bör man naturligtvis inte bli alltför impulsiv och verifiera att den man har för avsikt att handla av är en seriös aktör.

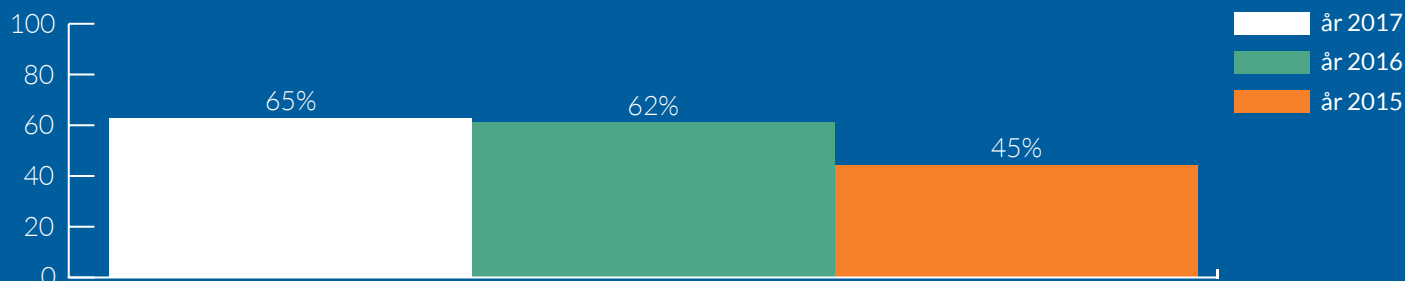


*Christian Angerbjörn,
Head of Technical Security på Sentor*

Inställning till IT-säkerhet

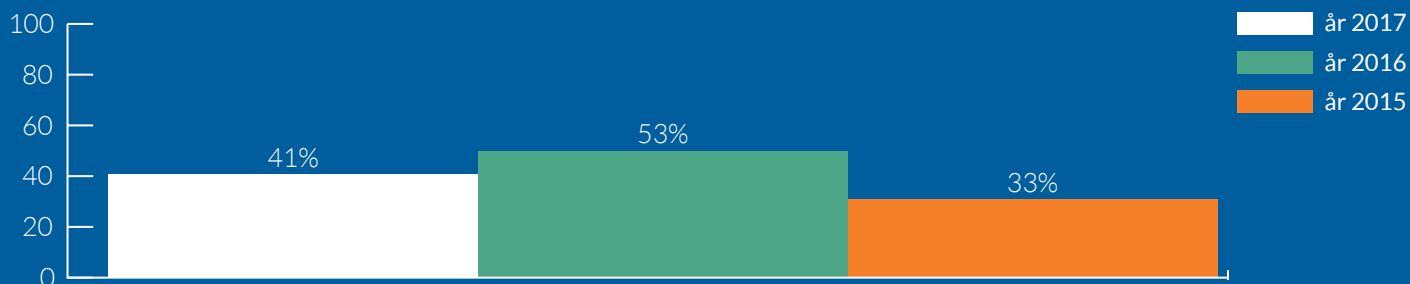
Är du orolig för att någon form av dataintrång eller IT-säkerhetsattack ska drabba dig? (virus, bedrägeriförsök eller liknande)

Rädslan för att drabbas av ett dataintrång eller en IT-säkerhetsattack är stor. Undersökningen för 2017 visar att svenskarnas rädsla för IT-säkerhetsattacker fortsätter att öka. 2015 var 45 procent av svenskarna oroliga, 2016 var siffran 62 procent och 2017 uppgav 65 procent en oro.



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

2017 uppgav 41 procent av svenskarna att de drabbats av ett dataintrång eller IT-säkerhetsattack, en minskning gentemot 2016 då 53 procent uppgav samma sak.



Säkerhet på arbetsplatsen

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

8 av 10 svenskar svarar att de har förtroende för IT-säkerheten på den egna arbetsplatsen.



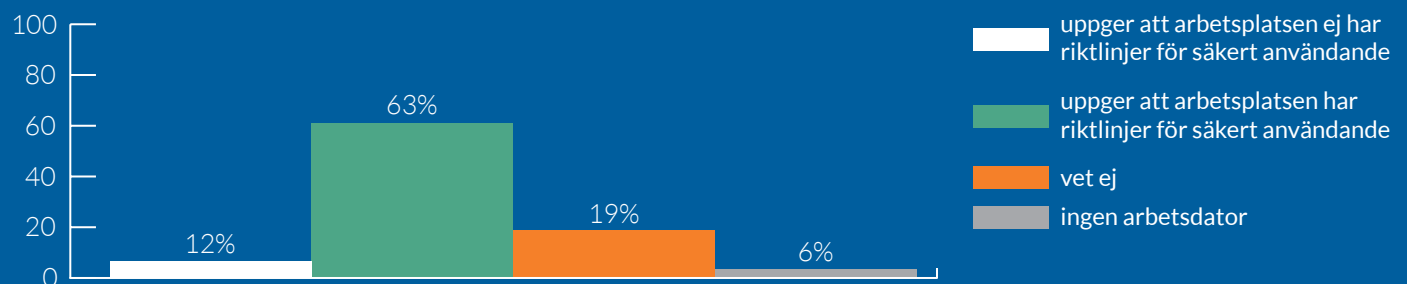
19%
känner lågt/
mycket lågt förtroende



81%
känner högt/
mycket högt förtroende

Har din arbetsplats riktlinjer för säkert användande av din arbetsdator?

1 av 5 svenskar (19 procent) vet inte om deras arbetsplats har riktlinjer för säkert användande av arbetsdatorn. 12 procent uppger att arbetsplatsen inte har riktlinjer för säkert användande.



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.



59%
hanterar känslig eller
hemlig information på
sin arbetsdator



41%
hanterar ej känslig eller
hemlig information på sin
arbetsdator

Har din arbetsdator använts av någon annan än dig själv?

Över 50 procent av svenskarna uppger att de lånat ut sin arbetsdator till någon annan, trots att det innebär en stor risk.



44%
uppger att en kollega använt deras arbetsdator



6%
uppger att en familjemedlem använt deras arbetsdator



3%
uppger att de lånat ut sin arbetsdator till någon annan än kollega och familjemedlem



49%
uppger att de inte lånat ut sin arbetsdator

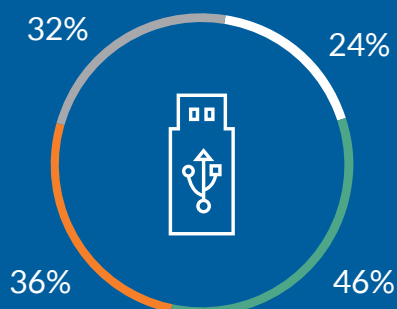
Har du kopplat in en privat USB-sticka eller extern hårddisk i din arbetsdator?

Att koppla in en privat USB-sticka eller extern hårddisk kan innebära stora risker. 4 av 10 svenskar uppger att de har gjort just detta. Uppdelat i åldersgrupper är det färre i åldersgruppen 18-39 år (24 procent) som kopplat in ett privat USB i sin arbetsdator, jämfört med åldersgruppen 30-45 år (46 procent).



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



ålder 18-29

ålder 30-45

ålder 46-59

ålder 60-75

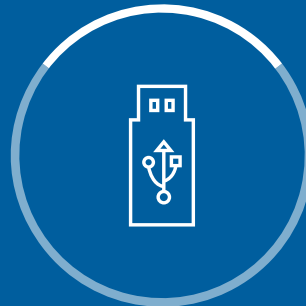
har kopplat in en USB-sticka eller extern hårddisk i sin arbetsdator

Använda USB-stickor och externa hårddiskar kan vara bärare av virus. Är det något som du har i åtanke när du kopplar in privata USB-stickor eller externa hårddiskar i din arbetsdator?

3 av 10 svenskar har inte tidigare haft i åtanke att USB-stickor och externa hårddiskar kan vara bärare av virus. Samtidigt hävdar 71 procent att de aldrig skulle låna ett USB eller en extern hårddisk från någon de ej litat på.



71%
skulle aldrig låna USB-stickor eller externa hårddiskar från någon de ej litat på



29%
har ej tänkt på detta

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

Knappt 4 av 10 svenskar har kopplat in en privat telefon eller dator på arbetsplatsens nätverk.



36%
har kopplat in en privat telefon eller dator på arbetsplatsens nätverk



64%
har ej kopplat in en privat telefon eller dator på arbetsplatsens nätverk

Har du laddat ned (via exempelvis The Pirate Bay) eller tittat på/lyssnat på upphovsrättsskyddat material (från exempel på Swefilmer/Dreamfilm) via din arbetsdator någon gång under de senaste 12 månaderna?

Att ladda ner eller titta på upphovsrättsskyddat material på sin arbetsdator är något som varken är lagligt eller säkert. 6 procent av svenskarna uppger att de använt sin arbetsdator till att titta på upphovsrättsskyddat material.



6%
har laddat ned eller tittat/lyssnat på upphovsrättsskyddat material via sin arbetsdator någon gång under de senaste 12 månaderna



94%
har ej laddat ned eller tittat/lyssnat på upphovsrättsskyddat material via sin arbetsdator någon gång under de senaste 12 månaderna

Stora risker med att koppla in privata enheter i företagets nät

36 procent av svenskarna uppger att de har kopplat in en privat telefon eller dator i företagets nät. Vilka är de stora farorna med att anställda gör så?

- Den uppenbara risken är att de privata utrustningar som kopplas in inte har de skyddsfunktioner som finns på den utrustning som är standard hos företaget och därmed kan vara smittade av virus och trojaner. Det finns även en risk att företagsinformation avsiktligt eller oavsiktligt förs över till dessa enheter och därmed kommer på vift.

- Normalt sett så omfattas inte heller privata utrustningar av företagets policy, till exempel kring hur de får användas och användaren kan därmed ha använt sin egen utrustning oaksamt.

3 av 10 uppger även att de inte tänkt på att använda USB-stickor och externa hårddiskar kan vara bärare av virus. Hur ser du på att man är öppna för att stoppa in externa enheter i arbetsdatorn och att det finns en omedvetenhet kring riskerna med detta?

- På samma sätt som en privat telefon eller dator kan vara infekterad så kan USB-stickor och externa hårddiskar vara det. Men om det dessutom är okända enheter som kopplas in ökar risken, eftersom du inte ens själv har koll på vad som finns lagrat på enheten. För att ta ett exempel spreds USB-stickor på marken i Göteborg och dessa innehöll skadlig kod, förmodligen med mål att infektera datorer hos företag som satt i närheten.

64 procent uppger att deras företag har riktlinjer för säkert användande av arbetsdatorn. Finns det fog för att tro att många av de anställda bryter mot dessa riktlinjer?

- Ja, det finns det, men här måste företagen se till att ta ett större ansvar. Man kan inte förvänta sig att användare följer riktlinjer som de inte känner till, så det här behöver kommuniceras bättre, till exempel med en kort beskrivning gällande hur utrustningen får användas, något som användaren skulle kunna få tillsammans med arbetsutrustningen.

6 procent uppger även att de har laddat ned upphovsrättsskyddat material eller tittat på upphovsrättsskyddat material via ex Swefilmer eller Dreamfilm. Att det är brottsligt att ladda ned filmer och dylikt känner många till. Men finns det några andra risker?

- Vi ser att den här formen av aktivitet förekommer hos våra kunder och här kan företagets policy variera kring hur man hanterar det. Riskerna när man laddar ner den här typen av material är bland annat att man kan få med en hel del oönskad skadlig kod, till exempel virus, trojaner eller ransomware. Risken för detta är ännu större om användaren även laddar ner piratkopierad mjukvara eller licensgeneratorer, något som normalt finns att hämta på samma siter som har filmer.



Mikael Witt,
Head of Managed Security Services på Sentor

Nätfiske

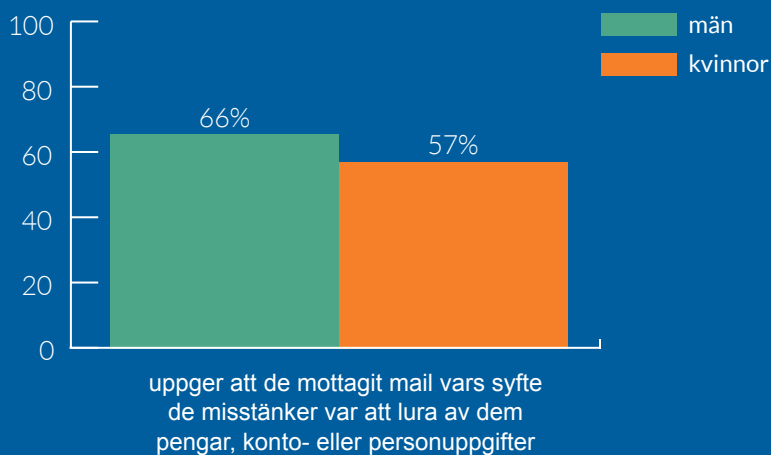
Har du (under de senaste 12 månaderna) mottagit mail vars syfte du misstänker var att lura av dig pengar, konto- eller personuppgifter?

Flertalet svenskar misstänker att de mottagit mail från en it-bedragare, 62 procent uppger att de blivit utsatta. 66 procent av männen har blivit utsatta, motsvarande siffra för kvinnorna är 57 procent.



62%

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



Lämnade du ifrån dig någon känslig information?

Av de som mottagit ett mail som de misstänker haft syftet att lura av dem känslig information uppger 2 procent att de lämnade ifrån sig känslig information.

2%

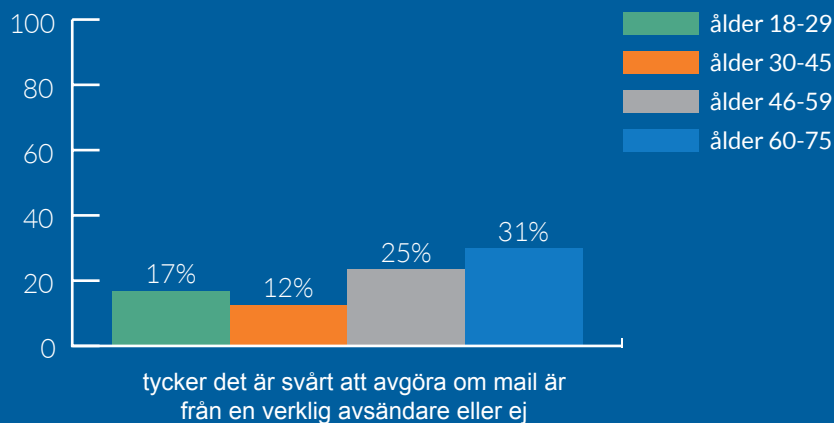
uppger att de lämnade ifrån sig känslig information

98%

uppger att de inte lämnade ifrån sig känslig information

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

2 av 10 svenskar har svårt att avgöra om mail kommer från en verklig avsändare. I åldersgruppen 18–29 år uppger 17 procent att det är svårt att avgöra om deras mail kommer från en verklig avsändare, till skillnad från åldersgruppen 60-75 år där 31 procent uppger att det är svårt att se skillnad.



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

I takt med de sociala mediernas framväxt har tillvägagångssätten för att komma åt människors känsliga information ändrats. 3 av 10 svenskar hävdar att de har blivit kontaktade av en person via sociala medier vars intention var att komma över känslig information.



31%
har blivit kontaktade av en person via sociala medier som de misstänkt var ute efter känslig information



69%
har inte blivit kontaktade av en person via sociala medier som de misstänkt var ute efter känslig information

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

Att låna ut pengar över internet kan vara riskabelt. Majoriteten av svenskarna hävdar att de inte skulle låna ut pengar. 23 procent uppger dock att de skulle låna ut pengar till en familjemedlem, även om vederbörande kontaktade dem över internet.



23%
skulle låna ut pengar till en familjemedlem



14%
skulle låna ut pengar till en nära vän



2%
skulle låna ut pengar till en bekant



75%
skulle inte låna ut pengar

Säkra lösenord

Anser du att ditt lösenord till din mail är säkert?

74 procent av svenskarna anser att deras lösenord till mailen är säkert, en minskning från förra årets kartläggning där 83 procent uppgav att de hade ett säkert lösenord till sin mail.



74%
anser att lösenordet till
deras mail är säkert



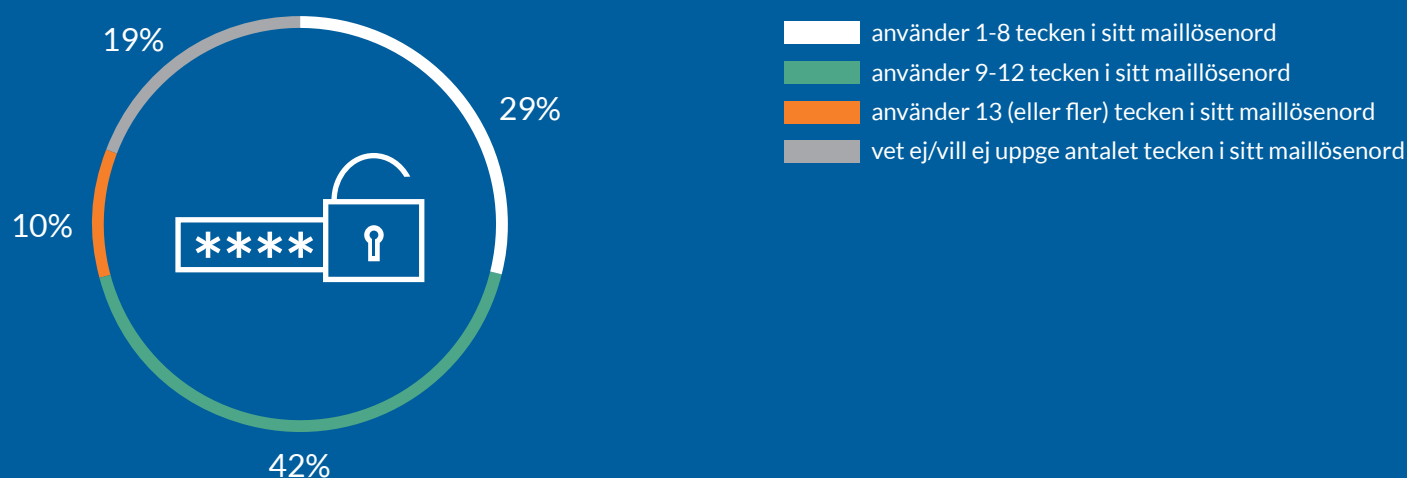
25%
anser inte att lösenordet
till deras mail är säkert



1%
har ingen mail

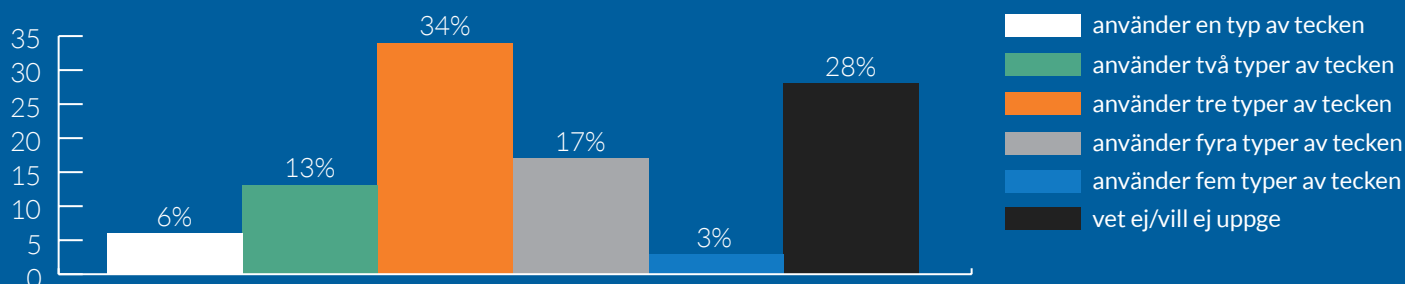
Hur många tecken består ditt maillösenord av?

Samtidigt som 74 procent anser sig använda ett säkert lösenord uppger 29 procent att de använder 1–8 tecken i sitt lösenord. 42 procent säger sig använda 9–12 tecken och 10 procent använder 13 tecken eller fler.



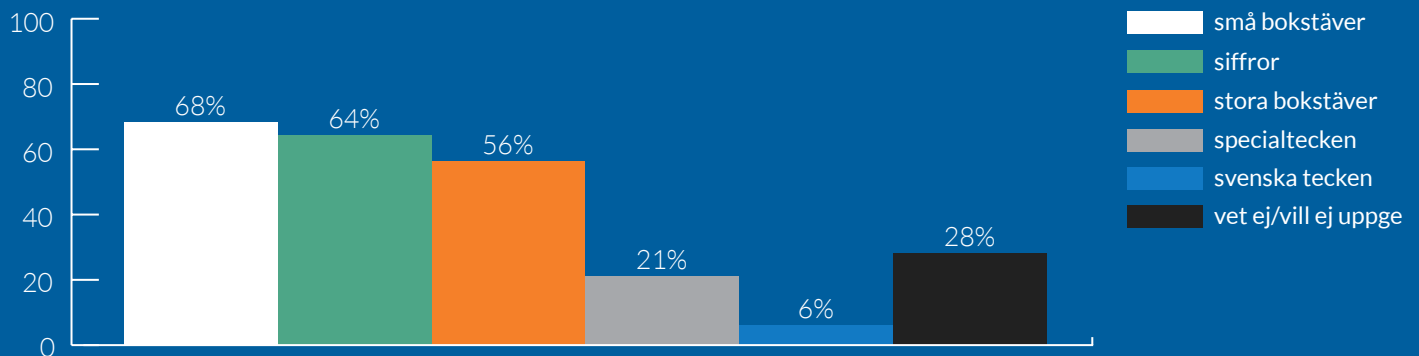
Inom IT talar man om olika sorter av tecken. Vilka av dessa teckentyper använder du dig av i ditt lösenord till din mail? (flera svar är möjliga)

34 procent av svenskar använder tre typer av tecken. Endast 3 procent använder fem typer av tecken.



Vilka av dessa teckentyper använder du dig av i ditt lösenord till din mail

Många svenskar använder små bokstäver i sina lösenord, däremot är det endast 6 procent som inkluderar svenska tecken.



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

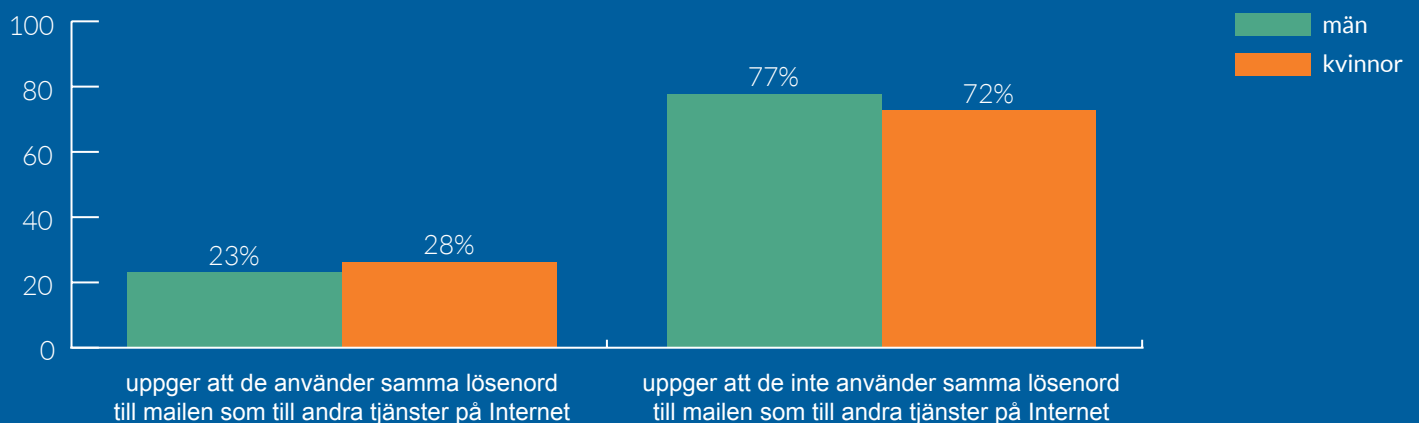
1 av 4 uppger att de använder sitt maillösenord på andra tjänster på Internet. Kvinnor är i högre utsträckning benägna att återanvända lösenord, till skillnad från män.



26 %
uppger att de använder samma lösenord till mailen som till andra tjänster på Internet



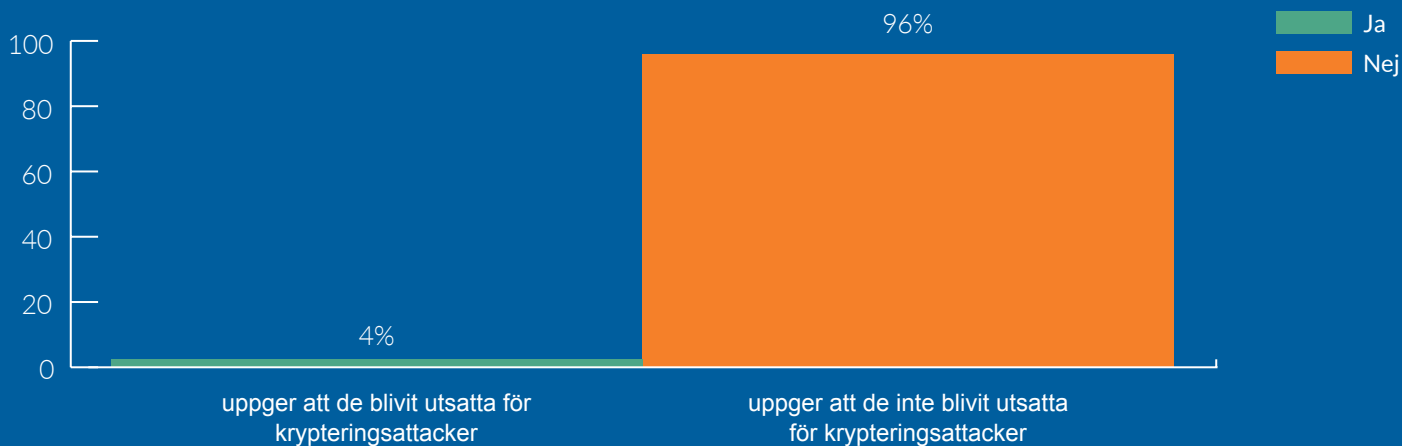
74 %
uppger att de inte använder samma lösenord till mailen som till andra tjänster på Internet



Ransomware och lagring

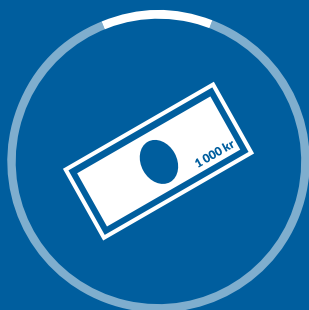
Har någon krypterat dina filer (så att du inte kan använda datorn) och använt sig av utpressning där de krävt pengar i utbyte mot att låsa upp de krypterade filerna?

Fyra procent av svenskarna uppger att de utsatts för ransomware (även kallat utpressningsvirus). Översatt till den svenska befolkningen motsvarar det drygt 300 000 svenskar.

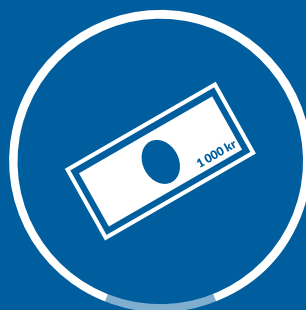


Om du skulle få dina filer låsta/krypterade så att din dator inte gick att använda. Skulle du då vara beredd att betala 1000 kronor i lösensumma för att få tillgång till dessa igen?

1 av 10 personer är beredda att betala 1000 kronor för att få tillgång till sina filer, om de skulle utsättas för en krypteringsattack.



12%
skulle betala 1000 kronor i lösensumma för att få tillgång till sina filer



88%
skulle inte betala 1000 kronor i lösensumma 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.



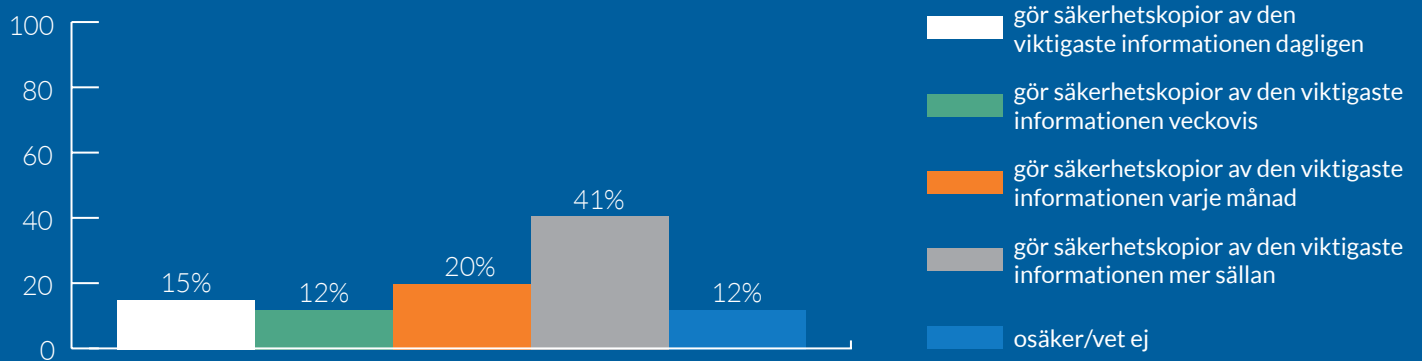
69%
gör säkerhetskopior av den viktigaste informationen på sin dator



31%
gör inte säkerhetskopior av den viktigaste informationen på sin dator

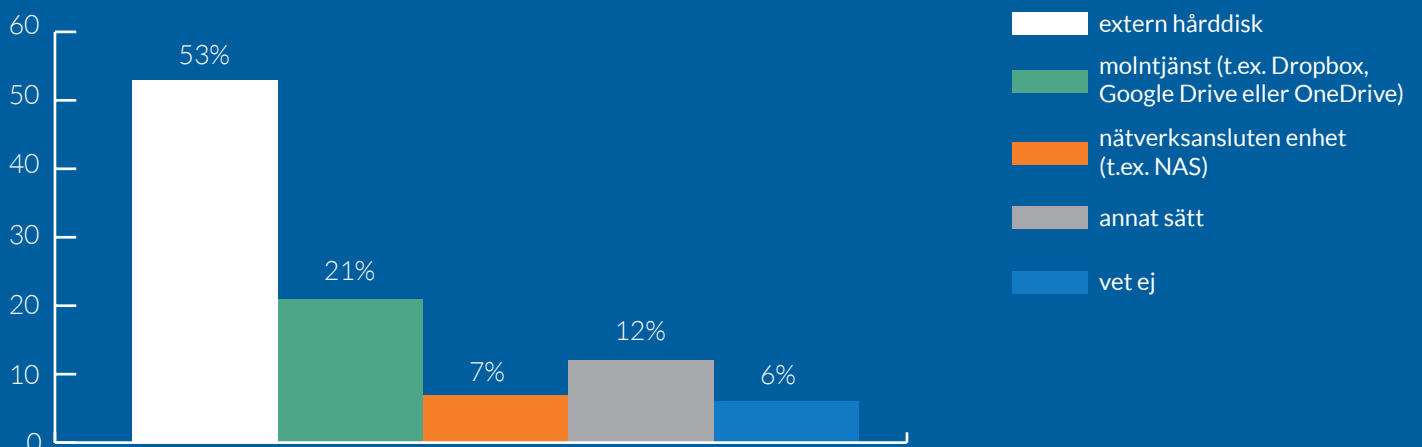
Hur ofta gör du backup/säkerhetskopior av din viktigaste information?

Närmare 7 av 10 tar säkerhetskopior av den viktigaste information på sin dator. Få tar dock säkerhetskopior regelbundet, 61 procent uppger att de säkerhetskopierar sin information varje månad eller mer sällan.



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

Det är mest vanligt att säkerhetskopiera till en extern hårddisk (53 procent), därefter kommer molntjänst (21 procent).



Ransomware allt vanligare

I Sentors rapport uppger 4 procent av svenskarna att de har drabbats av ransomware, där utpressare krävt dem på pengar i utbyte mot att låsa upp de krypterade filerna. Vad anser du om det?

- Ransomware är den formen av attacker som sprids i störst utsträckning just nu, så det är inte förvånande att många drabbas. Privatpersoner har ofta sämre kunskap och skydd vilket gör att de lättare blir offer.

Det är ändå förhållandevis många som har drabbats och har fått sin dator krypterad. Varför växer antalet attacker så kraftigt?

- Den enkla förklaringen är att det finns enorma pengar att tjäna för skurkarna, de som är duktiga kan tjäna miljonbelopp. Det är dessutom enkelt att sprida den skadliga koden via exempelvis mail samtidigt som det är låg risk att åka dit eftersom angriparna kan kräva in betalningen i form av kryptovaluta såsom Bitcoin.

Vilka är de enklaste åtgärderna som du som privatperson kan vidta för att undvika att drabbas av ransomware?

- Framför allt bör man vara försiktig med att klicka på länkar och öppna bilagor i mejl. Håller man även webbläsaren och insticksprogram uppdaterade till den senaste versionen kan man också undvika många attacker. Sedan bör man vara försiktig med att stoppa in okända enheter i sin dator och hålla sig borta från obskyra hemsidor.

dor.

1 av 10 uppger att de skulle vara beredda att betala 1000 kronor för att få tillgång till sina filer igen ifall de drabbats av ransomware. Polisen och andra auktoriteter säger att man inte ska betala, hur ska man resonera om man har drabbats?

- Det är upp till varje person att avgöra om det är värt att betala för att få tillbaka sina filer. Om det är det enda alternativet som återstår är det förståeligt att många väljer att betala trots att det göder kriminell verksamhet. Dock bör man känna till att det inte finns några garantier för att man får tillbaka sina filer eller att ens dator är fri från skadlig kod, bara för att man betalar lösensumman.

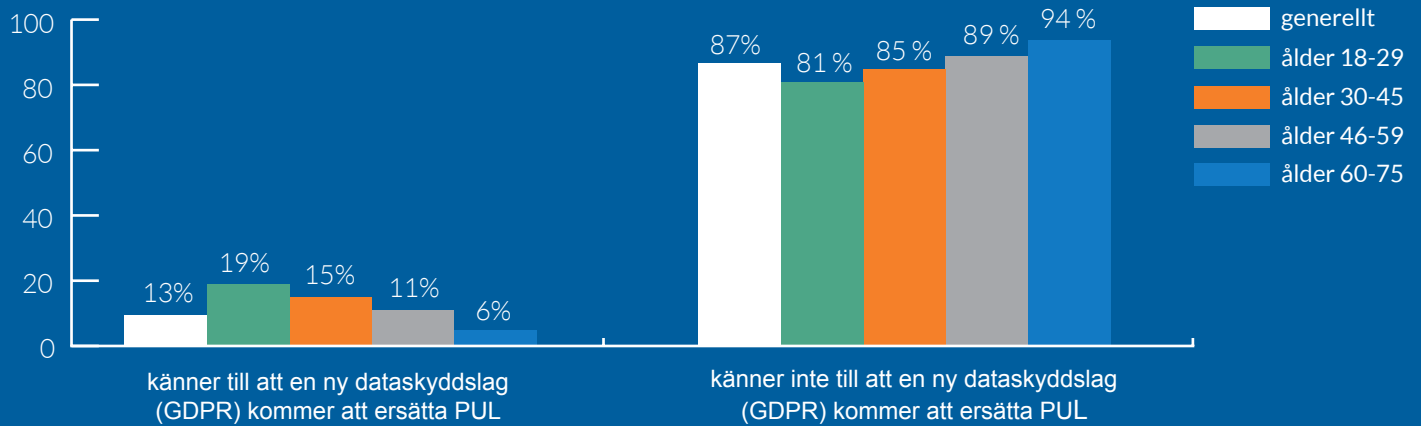


*Kalle Zetterlund,
Senior Technical Security Consultant*

Dataskyddslagen (GDPR)

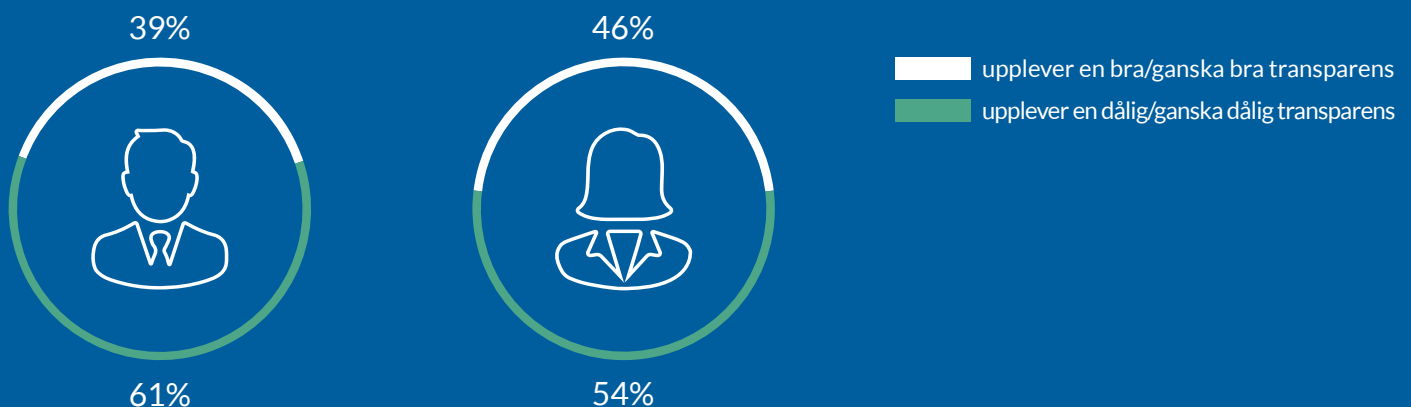
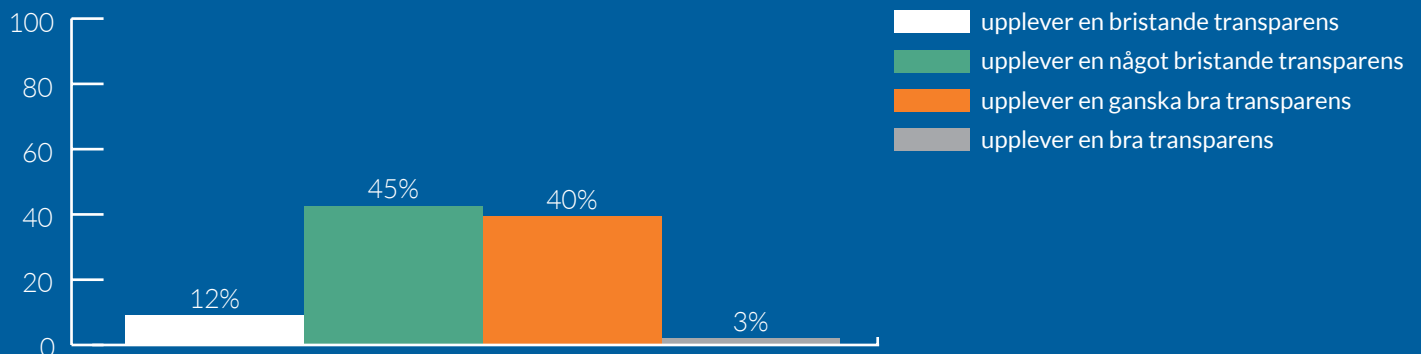
Känner du till att en ny dataskyddslag, General Data Protection Regulation (GDPR), kommer att ersätta Personuppgiftslagen (PUL) från och med maj 2018?

87 procent känner inte till att PUL kommer ersättas av en ny dataskyddslag (GDPR). 19 procent i åldrarna 18-29 år menar att de känner till detta, motsvarande siffra för åldersgruppen 60-75 år är 6 procent.



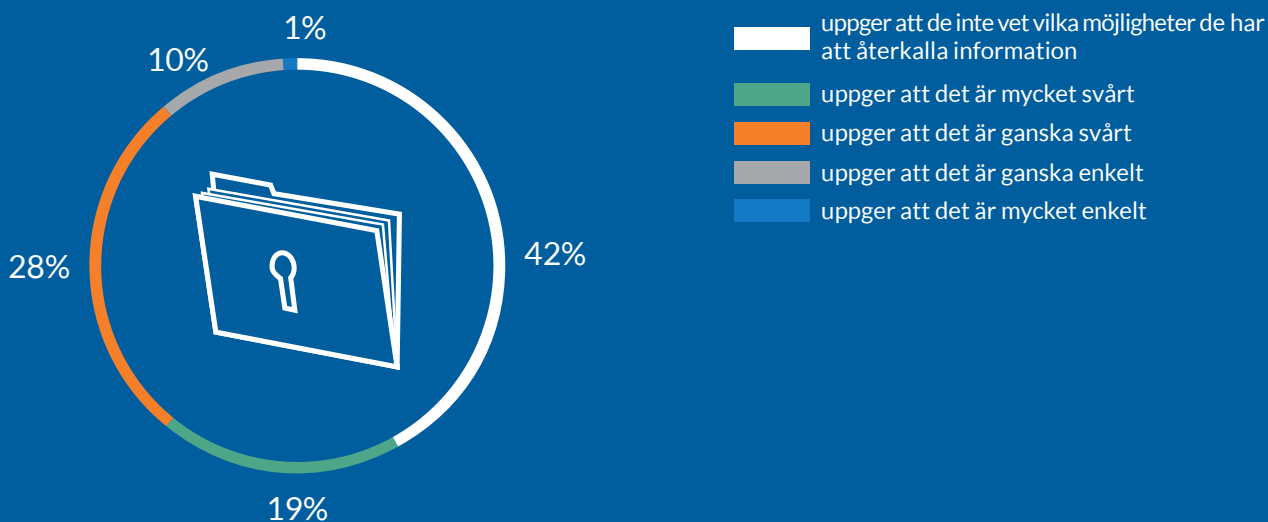
Hur transparenta tycker du svenska organisationer är på sina webbsidor gällande datainsamling och hur data används (exempelvis när du fyller i ett formulär på en webbplats)?

Närmare 6 av 10 anser att svenska organisationer brister i transparens gällande hur data används. Fler män (61%) än kvinnor (54%) 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. 42 procent vet inte vilka möjligheter de har att återkalla information och 47 procent menar att det är ganska, eller mycket svårt.



Nästan alla svenskar skulle avstå från att samarbeta med en organisation som missbrukat personlig data.

Majoriteten (96 procent) av svenskarna skulle avstå från att samarbeta med en organisation som missbrukat personlig data.



Ny dataskyddslag ersätter PUL

87 procent av svenskarna känner inte till att den nya dataskyddsförordningen GDPR kommer att ersätta PUL i Sverige, vilket innebär förändringar både för företag och privatpersoner. Hur ser du på siffran?

- Den stämmer säkert. Jag upplever att många organisationer haft frågan på agendan ett tag men nu på ett mer strukturerat sätt börjar ta tag i GDPR-problematiken. Bland privatpersoner är dock inte kännedomen lika stor.

6 av 10 svenska organisationer brister i transparens gällande hur data används, exempelvis när du fyller i ett formulär på en webbplats. Vilken bild har du av det?

- Tror den faktiska siffran är ännu högre då det är en enorm utmaning att ha koll på all data som samlas in och behandlas. Ju större organisation (antal system och integrationer), desto större utmaning.

Endast 1 av 10 uppger att det är enkelt att återkalla samtycke hos organisationer som fått möjlighet att lagra information om sig. GDPR skärper nu regelverket kring detta, hur tror du att det kommer påverka?

- Syftet med GDPR är att förstärka individers rättigheter avseende personlig data och dess användning. Visst kommer detta att leda till ytterligare krav på förändringar och anpassningar i organisationers processer och arbetssätt, men jag ser detta som en positiv utveckling.



Jörgen Elovsson,
Senior Information Security Consultant på Sentor

Vilka ser du som de största utmaningarna för organisationer att lösa i anslutning till den nya lagen?

- Den sannolikt största utmaningen är tolkningen av vad lagtexten innebär i praktiken och hur man vet när man är klar, dvs uppnår GDPR compliance. I dagsläget finns ingen certifiering för GDPR och flera områden behöver förtydligas. Artikel 29-gruppen förväntas ta fram förtydliganden under maj och det kommer säkerligen mer information innan lagen träder i kraft i slutet av maj 2018.

Och vilka är de största vinsterna för den enskilda individen?

- Svårt att säga men jag hoppas slippa scrolla igenom 50 sidor avtalstext och klicka accept. Skämt åsido, de höga böterna gör att företag och organisationer måste ta detta på större allvar, vilket kommer leda till ett bättre aktivt och passivt skydd för den enskilda individen. Med passivt skydd menas att integritetskontroller måste införas utan ansträngning på individen. Det aktiva skyddet innebär bl.a att individens rättigheter att begära ut 'sin' information och bli 'glömd' måste tillgodoses.

Endast 4 procent skulle kunna tänka sig att fortsätta ett samarbete med en organisation som läckt personlig data. Har vi underskattat affärsrisken av detta tidigare? Borde organisationer redan ha gjort mer för att skydda personlig data?

- Man kan alltid göra mer, men det är också en kostnadsfråga. Även om man har en väldigt säker miljö kan man tyvärr inte till hundra procent skydda sig mot dataläckor. Däremot kan man, om en läcka inträffar, ha kontroller på plats som gör den mest känsliga datan mer eller mindre oanvändbar genom t.ex. anonymisering, kryptering och pseudonymisering.

Cyberattacker och spioneri

Cyberattacker är ett ämne som debatterats flitigt i media den senaste tiden efter att anklagelser riktats mot Ryssland för att ha försökt påverka det amerikanska presidentvalet. Är cyberattacker något som du känner oro över?

Svenskar har en splittrad syn på cyberattacker. 4 av 10 känner sig oroliga, medan 3 av 10 inte vet hur de känner inför ämnet.



41%
av männen känner
sig oroliga



35%
av kvinnorna
känner sig oroliga

Anser du att det svenska försvaret borde få större resurser för att skydda Sverige mot cyberattacker?

Hela 7 av 10 svenskar anser att det svenska försvaret borde få större resurser för att skydda Sverige mot cyberattacker, 9 procent är negativt inställda till frågan.



67%
tycker att det svenska försvaret
borde få större resurser för att
skydda Sverige mot cyberattacker



9%
tycker inte att det svenska
försvaret borde få större resurser
för att skydda Sverige mot
cyberattacker



24%
vet inte om det svenska försvaret
borde få större resurser för att
skydda Sverige mot cyberattacker

Känner du oro för att någon ska hacka din dators webcam eller mikrofon i syfte att spionera på dig?

1 av 5 känner oro för att bli spionerade på via sin egen dator. 36 procent i åldersgruppen 18-29 år känner sig oroliga, motsvarande siffra är 22 procent i åldersgruppen 30-45 år. 18 procent i åldersgruppen 46-59 år känner oro och 15 procent i åldersgruppen 60-75 år.



22%
känner oro för att någon ska spionera på dem via deras dator



78%
känner ingen oro för att någon ska spionera på dem via deras dator

Har du någon gång misstänkt att någon spionerar på dig, antingen via webcam och mikrofon eller via ett avlyssningsprogram på din dator?

Det finns flera sätt att hacka sig in i någons dator och därmed få möjlighet att spionera på användaren, exempelvis via webcam eller mikrofon. 6 procent av svenskarna misstänker att de någon gång har blivit utsatta för spionage.



6%
har någon gång misstänkt att någon spionerat på dem via datorn



94%
har aldrig misstänkt att någon spionerat på dem via datorn

För mer information, vänligen kontakta:
Tomas Wahlstedt, Mob: +46 707 573 009 Mail: tomas.wahlstedt@sentor.se



sentor