sentor

Svenskarnas syn på IT-säkerhet

2020

Innehåll

Introduktion och metod

Förord

Det är nu femte året i följd som Sentor tar fram rapporten *Svenskarnas syn på IT-säkerhet*. När vi inledde arbetet med den första rapporten visste vi inte att den skulle bli ett stående inslag. Men den respons vi har fått från er läsare har inte bara gjort oss stolta och glada, den har även förstärkt känslan av att rapporten bidrar till att skapa bättre insikter kring hur svenskar tänker och agerar i frågor kopplade till IT-säkerhet.

När vi ser en del av svaren i år får vi också en ögonöppnare. Det är tydligt att vi har en hel del utmaningar framför oss, både när det kommer till bedrägerier och riskfyllda beteenden. Vad som däremot blir tydligt är att det finns mycket vi tillsammans kan göra för att stärka landets IT-säkerhet, både för den enskilde individen och för våra statliga och privata verksamheter.

Metod

Svenskarnas syn på IT-säkerhet bygger på en undersökning som har tilldelats 1010 svenskar i åldersintervallet 18-75 år. Urvalet görs genom en webbrekryterad panel, med befolkningsrepresentativa kvoter avseende respondenternas kön, ålder, utbildning och geografisk fördelning. Det slutgiltiga resultatet är riksrepresentativt och statistiskt säkerställt, samt vägt utifrån den demografiska strukturen i Sverige för att spegla den vuxna befolkningen.

Sentors VD har ordet

Inledningen på 2020 har på många sätt varit speciell. Allt vi tidigare har sett som självklart har snabbt ställts på ända. Fokus ligger istället på att skydda människor i vårt samhälle och trygga vården för de som drabbas i pandemins spår. Förutom de rent hälsomässiga aspekterna har vi även kunnat följa vilka enorma ekonomiska konsekvenser pandemin har fört med sig, både globalt och här hemma i Sverige.

Utifrån min roll som VD på Sentor kan jag se ett förändrat landskap framför mig, när hälsoläget återgår till det normala. Jag tror att vi kommer att få uppleva hur den här krisen inte bara lett till ett annat synsätt vad gäller beredskap och risk, utan hur den även har drivit fram en digitaliseringsvåg för stark för att stoppa. Sektorer som tidigare legat långt efter i den digitala utvecklingen, sköter nu ledigt sina möten över videolänk och hanterar dokument i molntjänster.

Det är en fantastisk utveckling som för med sig en rad olika fördelar sett ur ett användarperspektiv. Men när transformationen går snabbt är det ofta på bekostnad av risk- och säkerhetsavväganden. Vet man vilka som har fått access till det där systemet? Vem har koll på den fysiska lokalen när ingen är på plats? Är det säkert att dela dokument i den där molntjänsten eller att ha videomöten i Zoom?

Min förhoppning är att de flesta organisationer ställer sig frågor som dessa för att försäkra sig om att de vet vad de gör. Om inte riskerar den omedelbara krisen vi befinner oss i nu, och det införande av ny teknik som den har medfört, att öppna spelplanen för illasinnade som står redo att utnyttja situationen. Vad sådana risker kan leda till, det kan ni läsa mer om i årets rapport tillsammans med mycket annat.

Stay safe!

Martin Zetterlund, vd

Förtroendebarometern

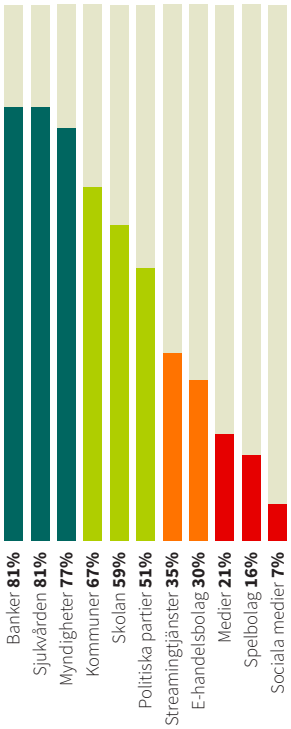
Idag hanterar flera aktörer din känsliga information (som exempelvis personuppgifter). Hur ser ditt förtroende ut för att följande aktörer skyddar den informationen från missbruk och intrång?

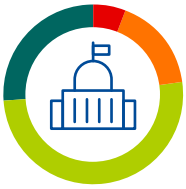
1

Precis som tidigare år placerar sig bank- och sjukvårdssektorn sig högt när svenskarna rankar vilka aktörer de har högst förtroende för när det kommer till att skydda känslig information. 81 procent uppger att de har ett högt förtroende för att aktörer inom dessa två sektorer skyddar känslig information på ett ändamålsenligt sätt. Strax därefter följer myndigheter på 77 procent. I botten finner vi, precis som tidigare år, sociala medier. (7 procent), spelbolag (16 procent) och traditionella medier (20 procent).

- Mycket lågt förtroende
- Ganska lågt förtroende
- Ganska högt förtroende
- Mycket högt förtroende

Mycket/ganska högt förtroende





Myndigheter:
- 6%
- 17%
- 51%
- 26%

Kommuner:
- 7%
- 26%
- 52%
- 15%

Banker:
- 5%
- 14%
- 49%
- 32%

Sjukvården:
- 4%
- 15%
- 47%
- 34%

Skolan:
- 8%
- 33%
- 46%
- 13%

Sociala medier:
- 57%
- 36%
- 6%
- 1%

Medier:
- 38%
- 41%
- 18%
- 3%

E-handelsbolag:
- 26%
- 44%
- 27%
- 3%

Politiska partier:
- 14%
- 35%
- 41%
- 10%

Spelbolag:
- 57%
- 27%
- 13%
- 3%

(Online gambling, live casino, etc)

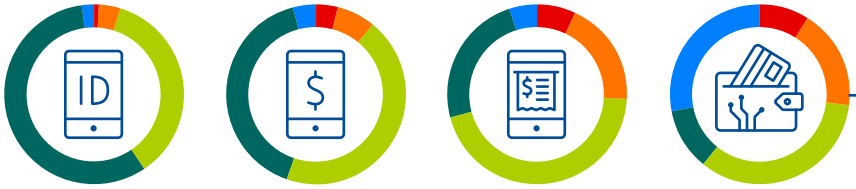
Streamingtjänster/ underhållningstjänster :
- 24%
- 41%
- 32%
- 3%

(Netflix/Spotify, etc)

Hur ser ditt förtroende ut för följande aktörers förmåga att tillhandahålla en säker tjänst?

2

Sedan en tid tillbaka genomför vi både köp och autentiserar oss via olika digitala tjänster. Några av de mest välanvända digitala tjänsterna för köp och autentisering är BankID, Swish, Klarna och Paypal. Bland dessa aktörer hamnar BankID i topp – hela 94 procent uppger att de har ett högt förtroende för deras förmåga att tillhandahålla en säker tjänst. Därefter följer Swish på 86 procent och Klarna på 69 procent. Paypal hamnar sist på 45 procent, sannolikt för att färre svenskar använder deras tjänster.



BankID:	Swish:	Klarna:	Paypal:
1%	4%	7%	9%
3%	7%	19%	18%
36%	45%	45%	34%
58%	41%	24%	11%
2%	3%	5%	28%

- Mycket lågt förtroende
- Ganska lågt förtroende
- Ganska högt förtroende
- Mycket högt förtroende
- Vet ej / Ej svar

Skulle du byta befintlig leverantör/tjänst (* av ovanstående alternativ) om det framkom att de har missbrukat dina personuppgifter?

3

I årets rapport uppger 3 av 4 svenskar att de skulle byta bank ifall det framkom att den hade missbrukat vederbörandes personuppgifter. Än mindre lojala är vi mot e-handelsbolag, där 79 procent uppger att de skulle byta leverantör vid samma överträdelse.

Det finns dock ytterligare aspekter att ta hänsyn till, bland annat att det är betydligt enklare att byta från en e-handlare till en annan, jämfört med hur komplicerat det kan vara att byta bank. Vidare skulle 6 av 10 svenskar vara beredda att byta streamingleverantör vid samma scenario – kanske har vi svårare att tänka oss ett liv utan våra spellistor på Spotify eller favoritserier på Netflix, som för många av oss har blivit en naturlig del av vardagen?

Hur väl dessa tjänster är integrerade i våra liv kan också vara en förklaring till varför yngre personer, som generellt sett använder sig av digitala tjänster i större utsträckning än vad äldre gör, också tenderar att har mer överseende med eventuella övertramp från sina leverantörer.

Bank	E-handelsföretag	Spelbolag	Streamingtjänster
75%	79%	47%	60%
8%	4%	2%	13%
17%	14%	4%	19%
0%	3%	47%	8%

- Ja, jag skulle byta
- Nej, jag skulle inte byta
- Vet ej
- Använder inte sådana tjänster

Hur väl stämmer följande påståenden in på dig?

Jag skulle avsluta samarbetet (till exempel sluta handla av, stödja, använda deras tjänst) med en organisation som missbrukat personlig data (till exempel sålt vidare personlig information och/eller bilder).

4

- Instämmer helt och hållet **54%**
- Instämmer **42%**
- Instämmer inte **4%**
- Instämmer inte alls **0%**

I en situation där en organisation grovt missbrukat personlig data är svenskarna oresonliga. Hela 96 procent uppger att de skulle avsluta samarbetet med en organisation om så vore fallet.

96%
instämmer/instämmer helt och hållet

Jag skulle undvika att handla av ett företag om jag kände till att företaget utsatts för ett dataintrång.

5

- Instämmer helt och hållet **33%**
- Instämmer **46%**
- Instämmer inte **20%**
- Instämmer inte alls **1%**

I de fall där ett företag istället angrips eller oavsiktligen läcker information så är svenskarna mindre benägna att säga upp affärsrelationen. Ändå uppger 79 procent att de skulle undvika att handla av ett företag som utsatts för ett dataintrång.

79%
instämmer/instämmer helt och hållet

Jag känner en oro för hur mina personuppgifter hanteras i allmänhet.

6

- Instämmer helt och hållet: **11%**
- Instämmer: **42%**
- Instämmer inte: **39%**
- Instämmer inte alls: **8%**

Det senaste året har flertalet personuppgiftsläckor uppmärksammats i både svensk och internationell media. Nationellt är 1177-läckan den mest omtalade, då miljontals inspelade vårdsamtal låg öppet exponerade på internet. Kanske kan den och andra incidenter vara bidragande till att 53 procent av svenskarna känner en oro för hur deras personuppgifter hanteras i allmänhet.

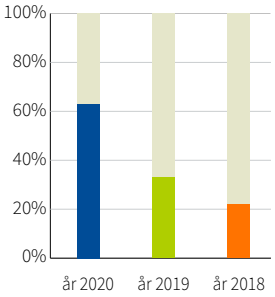
53%
instämmer/instämmer helt och hållet

Säkerhet i hemmet / Internet of Things

IoT-enheter är saker som är uppkopplade mot internet, såsom smart-TV, högtalare, övervakningskameror, lampor, lås och larm. Innehar du en eller flera sådana enheter i ditt hem?

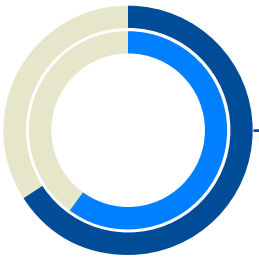
IoT-trenden håller i sig, och det med besked. Andelen som har IoT-enheter i hemmet uppgår till 63 procent, vilket motsvarar en ökning på hela 90 procent från föregående år. Vidare kan vi konstatera att användningen av IoT-enheter ökar stadigt i alla ålderskategorier, men störst procentuell ökning ser vi bland de äldre åldersgrupperna. Till exempel så har majoriteten av personer mellan 60-75 år uppkopplade prylar i hemmet, vilket är en ökning på över 100 procent från förra året, och över 300 procent sedan 2018.

7a



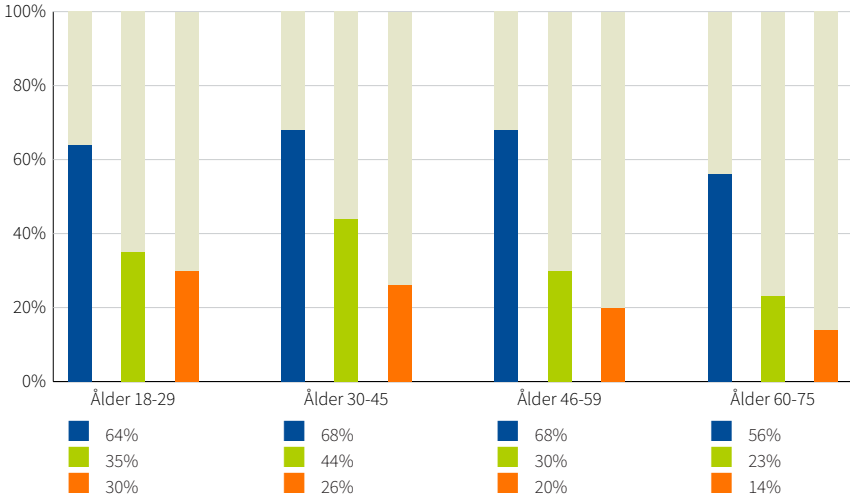
TOTALT

- Ja **63%**
- Ja **33%**
- Ja **22%**



FÖRDELAT ÖVER KÖN 2020

- Män Ja **66%**
- Kvinnor Ja **60%**

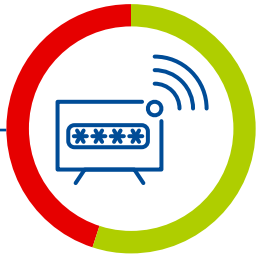


FÖRDELAT ÖVER ÅLDER

- 2020 Ja
- 2019 Ja
- 2018 Ja

7b

Om ja, har du vidtagit några säkerhetsåtgärder för dessa enheter, till exempel bytt ut standardlösenordet, uppdaterat integrerad mjukvara eller försett dem med ett separat nätverk?



Ja **55%**
Nej **45%**

IoT-prylar bör hanteras med samma försiktighetsåtgärder som datorer, telefoner och andra digitala enheter. Det innefattar bland annat att se till att de är uppdaterade med den senaste mjukvaran, utrustade med svårknäckta lösenord och de bör helst vara isolerade från andra enheter med hjälp av separata nätverk. Drygt hälften uppger att de har vidtagit en eller flera av dessa åtgärder.

8

Känner du till säkerhetsriskerna med att koppla upp IoT-enheter i hemmet?

Ja **55%**
Nej **45%**

Uppkopplade prylar i hemmet kan underlätta många praktiska aspekter i vardagen. Men de kan även medföra risker; både för den enskilda individen, då det kan läcka känslig information eller vara en väg in för angripare till användarens nätverk, men också för resten av Internet, eftersom hackade prylar ofta används i attacker mot andra offer genom så kallade botnät. Drygt hälften anser sig känna till riskerna med att koppla upp IoT-enheter i sina hem.

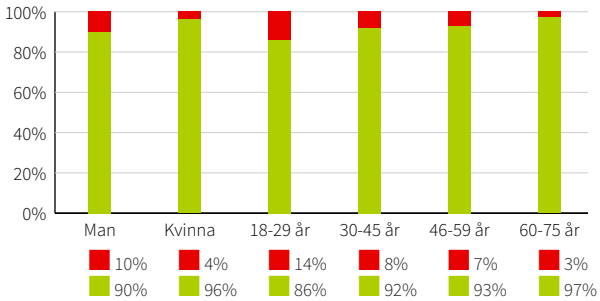
9

Skulle du köpa IoT-produkter från en leverantör som har drabbats av en uppmärksammad säkerhetsincident?

Säkerhet anses vara en viktig aspekt när konsumenter väljer sina IoT-produkter. Fler än 9 av 10 uppger att de skulle undvika att köpa IoT-produkter från en leverantör som de vet har drabbats av en säkerhetsincident. Yngre personer verkar dock besitta en högre tolerans för leverantörer med kända säkerhetsbrister än vad äldre personer har.

TOTALT

Ja **7%**
Nej **93%**



IoT-prylarna invaderar våra hem

IoT-trenden är onekligen här för att stanna - åtminstone om man ser till den lavinartade ökningen av användandet de senaste åren. Idag har majoriteten – gammal som ung – uppkopplade prylar i sina hem. Men vilka baksidor kan vi förvänta oss att se när internet fylls av potentiellt osäkra produkter? Det berättar, Joel Rangsmo på Sentor, mer om nedan.

Andelen folk som har uppkopplade prylar i sina hem har nästan fördubblats sedan förra året. Hur ser du på den utvecklingen ur ett säkerhetsperspektiv?

Precis som de allra flesta andra kommersiella produkterna på marknaden har IoT-enheter traditionellt sett inte utvecklats med säkerheten i centrum. Det har medfört att vi numera använder ett internet som är fullt av sårbara prylar som potentiellt kan utnyttjas av angripare som vill komma åt känslig information om en enskild användare eller andra enheter på samma nätverk. När jag och mina kollegor har anlitats för att utföra säkerhetsgranskningar av dessa produkter har vi i flera fall lyckats ta över produkter som övervakningskameror och andra känsliga föremål. I dessa fall har ju leverantören möjlighet att åtgärda sårbarheterna innan de når slutanvändarna, men alla aktörer är tyvärr inte lika noggranna med att testa sina produkter innan de släpps på marknaden.

Sårbara prylar utnyttjas även i så kallade botnets – nätverk av flera enheter som har kopplats samman med skadlig kod. Historiskt har vi sett flera virus som har utnyttjat dessa botnets för att utföra massiva överbelastningsattacker mot webbtjänster. Mest känt är Mirai som infekterade tusentals prylar och använde dessa för att stänga ner stora sajter som Amazon, Spotify och Twitter.

Vad ska man tänka på när man köper IoT-prylar? Och är det säkert att köpa produkter från till exempel Alibaba eller andra alternativa marknadsplatser?

Det är alltid bra att köpa IoT-produkter från erkända, stora aktörer, eftersom dessa med större sannolikhet har låtit en tredje part granska säkerheten. Mindre företag, så som startups, har många gånger inte samma resurser för att ta säkerheten i beaktning när de utvecklar sina produkter.

Vidare är det bra att undersöka om leverantören har släppt säkerhetsfixar på tidigare buggar för att se att den tar säkerheten på allvar. Här är det också viktigt att säkerställa att leverantören även tillhandahåller uppdateringar för äldre produktmodeller, vilket inte alla gör.

Angående frågan om att köpa uppkopplade prylar på Alibaba och liknande sajter så tycker jag tycker jag att man bör hålla sig borta, förutsatt att man inte är insatt. Det är svårt att veta vilka som ligger bakom produkterna som säljs där samt vilken säkerhetsnivå de håller. Tittar man till exempel på hemautomationsenheter som många köper nu, så använder dessa ofta tillhörande molntjänster som de kommunicerar med. Allt som laddas upp i dessa tjänster hamnar ju någonstans på internet, inte osannolikt på stora servrar i Kina eller liknande.

Vilken eller vilka säkerhetsåtgärder skulle du säga är viktigast att prioritera när man väl har införskaffat sina IoT-prylar?

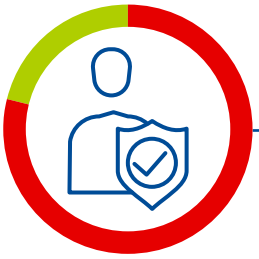
Innan du släpper dina uppkopplade prylar fria mot internet finns det ett par säkerhetsåtgärder du bör vidta. En är att byta ut standardlösenordet som ofta kommer med dessa produkter – att inte byta ut det är som att lämna kvar nyckeln i ytterlåset. En annan åtgärd du bör överväga är att skapa ett separat nätverk för dina IoT-enheter. Fördelen med det är att IoT-enheterna då ligger på ett isolerat nätverk, vilket innebär att de inte kan användas för att skada eller attackera någon dator eller annan enhet som är ansluten till ditt primära hemnätverk.

Precis som med andra digitala enheter, såsom din telefon och dator, är en av de viktigaste åtgärderna du kan vidta för att se till att dina IoT-prylar är säkra att hålla dem uppdaterade. När leverantörer, förutsatt att de är seriösa, hittar sårbarheter i sina produkter släpper de uppdateringar med säkerhetsfixar. Vissa leverantörer meddelar sina användare om dessa uppdateringar via mail eller andra direktkanaler, medan andra enbart informerar via sina webbsidor. Det kan därför vara en god idé att hålla lite koll på leverantörens webb, så man inte riskerar att missa viktig information.

Övervakning och integritet

Känner du en oro för att stora företag (som exempelvis Google och Facebook) inkräktar på din personliga integritet på internet?

10



Instämmer **79%**
Instämmer inte **21%**

Känner du en oro för att myndigheter inkräktar på din personliga integritet på internet?

11

Instämmer **39%**
Instämmer inte **61%**

En stor del av våra liv spenderas på internet, både privat och professionellt. Vi delar mycket information i tron – eller kanske förhoppningen – om att de aktörer som hanterar den gör det konfidentiellt och ändamålsenligt. Undersökningen visar dock att så många som 8 av 10 upplever en oro över att stora företag inte värnar om den personliga integriteten online. Generellt sett verkar förtroendet för myndigheter vara större i det hänseendet: hälften så många oroar sig över att myndigheter inkräktar på den personliga integriteten på internet.

Hur väl stämmer följande påståenden in på dig?

Jag tycker att polisen ska ha möjlighet att gå in i brottsmisstänktas datorer och mobiler för att läsa krypterad information.

12

- Instämmer helt och hållet **60%**
- Instämmer **30%**
- Instämmer inte **6%**
- Instämmer inte alls **4%**

Sedan den 1 mars 2020 får polisen, SÄPO, tullen och Ekobrottsmyndigheten i hemlighet installera programvara eller med andra hjälpmedel samla på sig information (exempelvis lagrade bilder eller filer) från brottsmisstänktas datorer, surfplattor och telefoner. Metoden ska få användas vid misstanke om brott med minimistraff två års fängelse. Hela 9 av 10 anser att polisen bör ha möjlighet att läsa krypterad information i brottsmisstänktas mobiler och datorer. Störst stöd hittar vi bland de äldre, där nästan samtliga står bakom beslutet.

Jag tycker att polisen ska ha möjlighet att använda ansiktsigenkänning på offentliga platser i brottsförebyggande syfte.

13

- Instämmer helt och hållet **52%**
- Instämmer **29%**
- Instämmer inte **12%**
- Instämmer inte alls **7%**

Sedan hösten 2019 har polisen Datainspektionens godkännande att använda ansiktsigenkänning för att utreda brott. Beslutet får stöd i undersökningen, där 8 av 10 uppger att de anser att polisen ska få använda ansiktsigenkänning på offentliga platser i brottsförebyggande syfte. Yngre tenderar dock att vara mer skeptiskt inställda till metoden än äldre.

Jag tycker att företag ska ha möjlighet att använda ansiktsigenkänning för kommersiella syften, såsom kartläggning av kundbeteenden och för att skapa anpassade budskap och erbjudanden.

14

- Instämmer helt och hållet **3%**
- Instämmer **5%**
- Instämmer inte **30%**
- Instämmer inte alls **61%**

När det kommer till ansiktsigenkänning för kommersiella syften ser opinionen dock annorlunda ut. Nästan samtliga (92 procent) uppger att de inte tycker att företag ska ha möjlighet att använda tekniken för att kartlägga kundbeteenden och skapa anpassade budskap och erbjudanden.

Var går gränsen för integritetskränkning?

Myndigheter och företag använder sig i allt större utsträckning av tekniska hjälpmedel för att utföra sina uppdrag och kartlägga våra beteenden. Samtidigt är den personliga integriteten något vi svenskar värderar högt, vilket ställer höga krav på aktörernas förmåga att hanterar den information vi lämnar ifrån oss ändamålsenligt och i linje med våra gemensamma principer. Hrafn Steiner, informationssäkerhetsexpert med juridisk bakgrund, tittar närmare på vad det innebär i praktiken.

Generellt sett känner svenskarna en betydligt större oro för att privata företag inkräktar på deras integritet på internet än vad myndigheter gör. Är du förvånad över det resultatet?

Jag är inte särskilt förvånad över undersökningens resultat; i Sverige har vi, till skillnad från många andra länder, ett arv av hög tilltro till myndigheter. Att kunna använda det förtroendet till sin fördel är viktigt, framför allt i tider som dessa när vi är beroende av att folk följer myndigheternas rekommendationer och riktlinjer.

En viktig del i att upprätthålla det höga förtroendet är att värna om den personliga integriteten. Tittar man till exempel på situationen vi befinner oss i nu i samband med Covid19, så har man gjort ett avvägande att inte smittspåra via mobiler som många andra länder gör, då det anses vara integritetskränkande i förhållande till den nytta som en sådan mobilapp skulle ge. Istället förlitar man sig på ett ömsesidigt förtroende som bygger på att folk självmant delar med sig av information för att kunna utföra smittspårning. Så integritetsaspekten finns helt klart med i flera myndigheters resonemang kring om och hur man ska använda data.

Tittar man specifikt på brottsbekämpande myndigheter kan kvantitativ datainsamling fungera som ett viktigt verktyg om det hanteras på rätt sätt. Tack vare Ipred-lagen har polisen numera en enorm tillgång till data som underlättar deras arbete. Om det framkommer att denna data har missbrukats och slagits på, på ett icke ändamålsenligt sätt, skulle det förstås åsamka stor skada på polisväsendets anseende.

Det är med andra ord varje enskild myndighets skyldighet att ta integritetsfrågor seriöst och upprätthålla förtroendet de har anförtrotts.

När det kommer till privata aktörer använder de i regel långt mycket mer sofistikerad teknik och tillvägagångssätt för att kartlägga människors förehavanden än vad myndigheter gör.
Jag skulle, i likhet med de allra flesta, rikta min oro åt det hållet istället. Vi har bland annat sett Facebook sälja data till Cambridge Analytica som i förlängningen kan ha påverkat utgången i Brexit-valet, för att nämna ett exempel. Jag är mer oroad över den sortens utveckling; när företag och organisationer kan skapa välriktade reklamkampanjer utifrån maximal påverkan, både i politiska och kommersiella syften.

Sedan den 1 mars i år får polisen, SÄPO, tullen och Ekobrottsmyndigheten i hemlighet läsa krypterad information vid brottsmisstanke. Håller du med majoriteten av svenskarna om att det är berättigat?

Principiellt tycker jag inte att det är konstigt att polisen har rätt till hemlig dataavläsning, eftersom det inte skiljer sig särskilt mycket från andra hemliga tvångsmedel, såsom hemlig teleavlyssning och hemlig rumsavlyssning. Det är heller inte ett oväntat steg i brottsbekämpningens utveckling. Tittar man på det historiskt sett så började det med att polisen ville ha rätt att öppna brev, och därmed tumma på posthemligheten. När vi senare övergick till att använda telefoni i större utsträckning ville man även kunna lyssna av dem. Nu när IP-teknik i huvudsak används för kommunikation faller det sig naturligt att polisen vill ha samma möjligheter ta del av informationen som flödar där.

Problemet jag ser med just dataavläsning är hur det ska implementeras i praktiken. I propositionen står det att när verkställigheten, alltså rätten att använda tvångsmedlet, avslutas så ska de verktyg man använt tas bort eller göras obrukbara. Frågar man våra kollegor på vår tekniska säkerhetsavdelning så skulle de antagligen ha många frågor kring hur man skulle kunna göra det på ett säkert sätt.

En annan fråga jag ställer mig är hur man kan säkerställa att inga utomstående kan utnyttja sårbarheten som används under tiden som den hemliga dataavläsningen bedrivs. Och en tredje fundering är varifrån polisen kommer tillskansa sig kunskap och teknik. Ska de helt och hållet förlita sig på egenutvecklade saker, eller vänder man sig till marknaden för att införskaffa sig tekniker från mer ljusskygga aktörer?

Innan det går att dra några slutsatser anser jag att våra brottsförebyggande myndigheter behöver redogöra bättre för hur detta ska verkställas utan att varken integriteten eller säkerheten utmanas.

En stor majoritet anser att polisen ska få använda ansiktsigenkänning på offentliga platser i brottsförebyggande syfte. Ser du några potentiella risker med införandet av sådan teknik?

Ansiktsigenkänning i brottsförebyggande syften är inte helt oproblematiskt. Tittar man till exempel på hur tekniken har använts i USA så har den inte fungerat riktig som tänkt. Bland annat har det resulterat i många false positives bland minoriteter, eftersom AI:t är tränat på en viss typ av utseenden.

När det kommer till den svenska polisen handlar det mer om att använda tekniken för att automatisera arbete som tidigare har varit manuellt. Precis som vi varit inne på tidigare är det dock viktigt att datan används på ett ändamålsenligt sätt för att inte riskera att skada polisväsendets anseende.

Med det sagt tycker jag ansiktsigenkänning kan vara ett bra verktyg – så länge man inser begränsningarna och bevisvärdet det medför – samt att man alltid frågar sig hur datan ska användas och hur den potentiellt kan missbrukas.

Säkerhet på arbetsplatsen

Hur väl stämmer följande påståenden in på dig?

Jag har förtroende för att min arbetsgivare hanterar mina personuppgifter på ett säkert sätt?

15

Det finns anledning att tro att säkerheten bland olika arbetsgivare varierar kraftigt, då resurserna för att hantera dessa frågor är små bland många av de mindre aktörerna. En stor majoritet av svenskarna har dock förtroende för att deras arbetsgivare hanterar personuppgifter på ett säkert sätt – Hela 9 av 10 instämmer i det påståendet.

- Instämmer helt och hållet: **39%**
- Instämmer: **52%**
- Instämmer inte: **7%**
- Instämmer inte alls: **2%**

Instämmer/Instämmer helt: **91%**

Jag vet vad jag ska göra ifall jag mottar ett mail på min arbetsdator som jag misstänker är skickat av en bedragare.

16

Många av de säkerhetsincidenter som sker bland företag inleds med att en anställd klickar på en bilaga eller länk i ett mail. Syftet kan exempelvis vara att stjäla inloggningsuppgifter eller att installera skadlig programvara på offrets dator. Därför är det viktigt att veta hur man ska agera om man mottar ett bedrägligt mail på sin arbetsdator. Bland svenskarna uppger 86 procent att de har koll på läget och vet hur de ska agera vid en sådan situation, medan endast 5 procent svarar att de inte vet. 9 procent av de arbetsföra uppger att de inte har någon arbetsdator.

- Instämmer helt och hållet: **50%**
- Instämmer: **36%**
- Instämmer inte: **5%**
- Instämmer inte alls: **0%**
- Har ingen arbetsdator: **9%**

Instämmer/Instämmer helt: **86%**

17

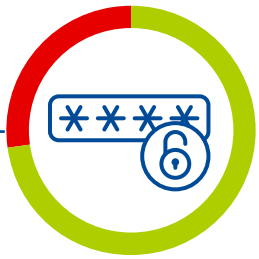
Genomför ni regelbundna utbildningsinsatser gällande IT-säkerhet på din arbetsplats?

Ja: **48%**
Nej: **52%**

En viktig del i att stärka organisationens säkerhet är att utbilda personalen regelbundet. Hälften av de svenskar som arbetar uppger att sådan utbildning är något som deras arbetsgivare erbjuder sina anställda att ta del av.

18

Om man har en arbetsdator, krävs det regelbundna lösenordsbyten för att logga in på din arbetsdator?



Ja: **73%**
Nej: **27%**

Lösenord har sedan lång tid tillbaka varit ett krav för att logga in på datorn och de konton som den anställde kontrollerar. I tidigare rekommendationer tryckte man på vikten av att lösenord på regelbunden basis byttes ut. Närmare 3 av 4 svenskar uppger att det är en regel som gäller inom deras organisationer.

19

Behöver du använda tvåfaktorsautentisering för att logga in på din arbetsmail?

Ja: **24%**
Nej: **76%**

Tvåfaktorsautentisering innebär att en ytterligare autentisering läggs till utöver lösenord för att bekräfta att du verkligen är du när du loggar in. Vanligtvis kombineras användarnamn och lösenord med en kod som du får via sms eller genereras i en app. Tvåfaktorsautentisering implementeras i allt högre omfattning, men än idag saknar många organisationer detta. Endast 1 av 4 svenskar uppger att deras organisationer använder tvåfaktorsautentisering vid inloggning på arbetsmailen.

Vilka säkerhetsrutiner gör skillnad?

Företag är ofta måltavla för angripare, eftersom dessa vanligtvis sitter på större tillgångar än privatpersoner. Ett företag med många anställda innebär också många potentiellt svaga länkar, då attacker mot företag ofta riktar sig till dess användare. Att ha väl avvägda och etablerade säkerhetsrutiner på plats är därför en av de effektivaste säkerhetsåtgärderna man som organisation kan vidta. Kalle Zetterlund, CTO på Sentor, berättar lite om hur dessa rutiner bör – och inte bör – se ut.

Bland de som använder en arbetsdator så uppger 73 procent att de tvingas till lösenordsbyten vid inloggning på regelbunden basis. Vad anser du om att så många företag fortfarande står fast vid den principen – stärker det säkerheten?

Det finns visserligen några mindre säkerhetsvinster i att tvinga användare att byta lösenord med vissa intervall. Processen är dock väldigt mödosam för användarna, och det finns många andra saker man kan lägga den energin på som ger betydligt större effekter för säkerheten. Framförallt handlar det om att tillse att användare inte återanvänder lösenord från andra tjänster, eller att lösenorden förekommer i listor över läckta lösenord. Det senare är relativt enkelt att kontrollera – till exempel i en så kallad lösenordsrevision – men att verifiera att användare inte återanvänder lösenordet från någon annan tjänst kan i praktiken bara göras genom utbildningsinsatser. Detta stöds också av det amerikanska standardorganet NIST, som inte längre rekommenderar tvingande regelbundna lösenordsbyten.

Endast 24 procent uppger att de behöver använda tvåfaktorsautentisering för att logga in på sin arbetsmail. Varför uppmanar säkerhetsexperter till att aktivera det och varför tror du att det fortfarande är så många företag som inte har den funktionen påslagen?

E-post är, trots alla sina brister, ofta en central punkt för autentisering. En angripare med kontroll över sitt offers e-postadress kan normalt använda denna för lösenordsåterställning på en uppsjö av andra tjänster. Av den anledningen bör extra fokus läggas på att skydda e-postkonton, och tvåfaktorsautentisering är det enklaste sättet att lägga på ett extra lager av skydd. Att detta fortfarande inte görs i organisationer har förmodligen att göra med resursbrister inom IT-avdelningar; har man har fullt upp med att få driften att överhuvudtaget fungera så har man kanske inte någon tid kvar att lägga på säkerhetsarbete. Just denna insats kräver ju inte speciellt mycket tid, men det kan man å andra sidan inte veta förrän man satt sig in i det.

86 procent uppger att de vet hur de ska agera ifall de mottar ett phishing-mail till deras arbetsdator. Vad säger du om den höga siffran? Och hur bör man egentligen agera ifall man har mottagit ett phishing-mail, och kanske därtill klickat på innehåll i ett sådant?

Om siffrorna stämmer så går utvecklingen helt klart åt rätt håll, eftersom en av de mest centrala delarna i en sådan plan är att just utbilda sina användare i hur de ska agera i en sådan situation. Många phishing-mail är generiska i sin natur, och dessa kan ju bara ignoreras. Men när det rör sig om riktade kampanjer mot ens organisation är det viktigt att detta meddelas till IT-avdelningen så att de kan vidta lämpliga åtgärder. Även om det är svårt att avgöra ifall det rör sig om en riktad attack eller inte så är det ändå lämpligt att vidarebefordra till IT-ansvariga.

Har man klickat på en länk i ett sådant mail och råkat ge bort sitt lösenord så är det förstås viktigt att man byter ut detta lösenord på alla ställen där det använts så fort som möjligt. Har man istället öppnat filer i ett sådant mail så bör datorn snarast möjligt försättas i viloläge/vänteläge eller stängas av, och därefter bör IT-ansvarig kontaktas. Detta rör dock det generella fallet, har ens IT-avdelning andra rekommendationer så är det förstås dessa man bör följa.

Ungefär hälften uppger att de genomför regelbundna utbildningsinsatser kopplade till IT-säkerhet. Vad skulle du säga är de viktigaste områdena att täcka i ett utbildningsprogram i syfte att stärka den grundläggande säkerhetsnivån hos ett företag?

Utbildningsinsatser bör vara kopplade till de specifika hoten man ser riktade mot sin organisation eller bransch. Därutöver finns det ett antal områden som är gemensamma för alla branscher. Till denna kategori hör phishing, social engineering, malware och säker informationshantering.

Internetbedrägerier

Bedrägeriförsök på internet kan ge sig i uttryck i många former; allt från massutskick av bedrägliga mail, till mer sofistikerade attacker mot utstuderade offer. 3 av 4 svenskar uppger att de har utsatts för någon form av bedrägeriförsök på internet. Störst andel ser vi i åldersgruppen 30-45, där andelen är 84 procent.

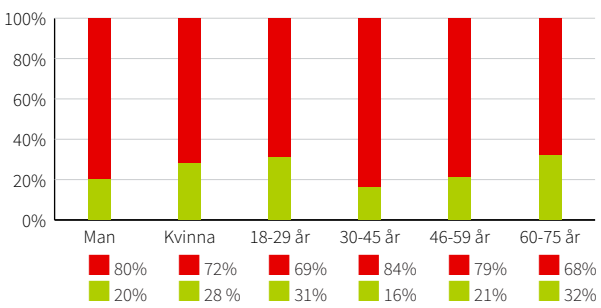
Andelen som har utsatts för fullbordade nätbedrägerier är däremot lägre – drygt 1 av 10 uppger att de har fallit offer för lyckade bedrägeriförsök. Yngre är generellt mer utsatta (19 procent), sannolikt för att de exponeras i högre utsträckning än äldre ålderskategorier.

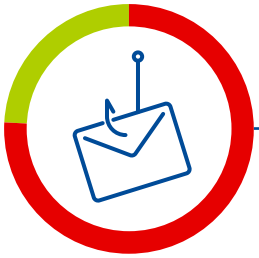
Vidare uppger varannan svensk att de känner någon som har fallit offer för bedragare på internet, vilket indikerar att fenomenet är utbrett och att många kan relatera till det.

Vad stämmer om nätbedrägeri?

20

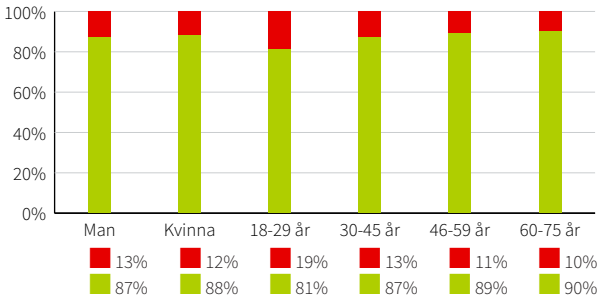
Jag har utsatts för bedrägeriförsök (via ex. falska mail, falska samtal etc.).





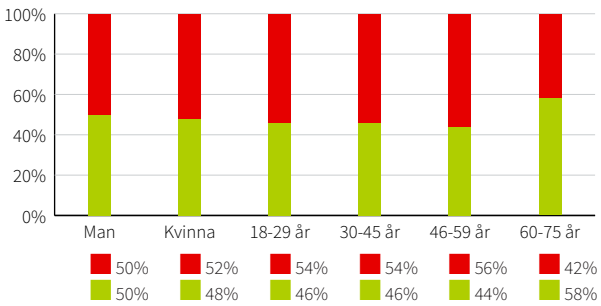
Stämmer **76%**
Stämmer inte **24%**

Jag har utsatts för nätbedrägeri (ex. identitetsstöld, fått uppgifter stulna etc.).



Stämmer **13%**
Stämmer inte **87%**

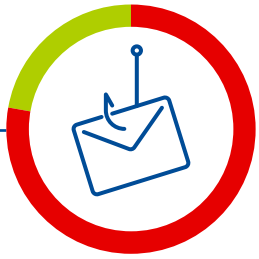
Jag känner någon som har utsatts för nätbedrägeri.



Stämmer **51%**
Stämmer inte **49%**

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

21



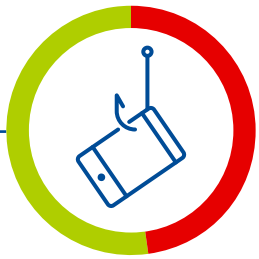
Ja **78%**
Nej **22%**

34%
ökning jämfört med föregående år.

Nätfiske, också kallat phishing, är en form av bedrägeri som går ut på att mailledes förmå mottagaren att lämna ifrån sig kritisk information eller ladda ner skadlig programvara. Fenomenet är utbrett, och de allra flesta har någon gång utsatts för brottet. 78 procent uppger att de under de senaste året har mottagit mail vars syfte du misstänker var att lura av dem pengar, konto- eller personuppgifter. Det motsvarar en ökning på 34 procent från föregående år.

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

22



Ja **48%**
Nej **52%**

26%
ökning jämfört med föregående år.

Sms-versionen av phishing kallas smishing och har blivit allt vanligare på senare år. Nästan hälften av svenskarna svarar att de har fallit offer för smishing de senaste 12 månaderna, vilket innebär en ökning på 26 procent jämfört med föregående år.

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

23

Ja **41%**
Nej **59%**

118%
ökning jämfört med föregående år.

Undersökningen visar att bedrägerier via sociala medier är ett växande problem – sedan förra året har antalet personer som uppger att de har utsatts för bedrägeriförsök via sociala medier ökat med hela 118 procent.

Nätbedrägerier – ett växande problem

Bedrägerier på nätet har blivit ett vanligt inslag i den svenska brottsstatistiken. Metoderna är många och ökar stadigt i takt med att bedragarna försöker hitta nya kreativa sätt att lura privatpersoner och företag på pengar eller känslig information. Vi har pratat med Jan Olsson, kriminalkommissarie på Noa (Nationella operativa avdelningen) och expert på bedrägerifrågor, om hur polisen ser på utvecklingen och arbetar med dessa frågor.

Enligt vår undersökning har internetbedrägerier ökat ganska markant det senaste året. Stämmer den bilden överens med vad ni på polisen ser för utveckling inom området?

På sätt och vis gör den det. Antalet anmälda bedrägerier har faktiskt minskat, vilket jag delvis tror beror på att folk helt enkelt är mer medvetna idag än för bara några år sedan. Däremot upplever vi att försöken ökar och att problemet är mer utbrett nu än tidigare.

Vanligtvis bemödar sig dock inte de som har utsatts för bedrägeriförsök att anmäla det, vilket gör att statistiken inte helt återspeglar verkligheten. Så trots färre anmälningar är min uppfattning att bedrägerier på nätet inte har avtagit, utan snarare tvärtom.

Andelen som uppger att de har kontaktats av potentiella bedragare via sociala medier har ökat med över 100 procent sedan föregående år. Vilka trender ser ni inom det området?

På sociala medier ser vi bland annat en ökningen av så kallade ponzibedrägerier, företag som hävdar att man kan tjäna stora pengar över natten på deras tjänster. Inte sällan frontas kampanjen dessutom av någon kändis som förstås inte har givit sitt medgivande till detta. Ett aktuellt exempel med svensk anknytning är företaget Onecoin som tjänade miljardtals kronor på sin falska kryptovaluta, och som nu står åtalade för en av världens största bedrägerihärvor.

Utöver det ser vi bland annat allt fler bedrägerier via köp- och säljkanaler där man inte använder seriösa betalningslösningar som till exempel Blocket och andra liknande sajter har.

Hur ska man agera om man misstänker att man har utsatts för ett bedrägeriförsök på internet?

Även om det "bara" rör sig om ett bedrägeriförsök tycker jag att man ska göra en anmälan. Ju fler som anmäler, desto högre upp på vår agenda hamnar ärendet. Kan vi påvisa att det är ett utbrett problem så kan det förstås resultera i att vi får större medel och fler resurser till att utreda och förebygga dessa brott.

Hur tycker du att de stora aktörerna hanterar de här frågorna? Får ni inom polisen den hjälp ni behöver för att utreda fall?

Vi inom polisen har på nationell nivå inlett ett samarbete med flera av de stora aktörerna, såsom Google, Facebook och Microsoft där Nationellt IT-Brottscentrum är Singel Point Of Contact, förkortat SPOC. Syftet är att likforma förfrågningarna efter de krav som dessa aktörer ställer för att kunna besvara de frågor som kommer från oss på svensk polismyndighet.

Av de förfrågningar vi skickar till dessa aktörer skulle jag säga att vi får hjälp med mer än hälften. Det ligger förstås delvis även i deras eget intresse, eftersom deras varumärken skulle påverkas negativt om det framkom att de att agerar plattformar för kriminalitet. Sedan finns det förstås även aktörer som är lite mer ljusskygga och som helst inte vill vara behjälplig med att svara på frågor om de verkligen inte måste.

Hur går angriparen tillväga för att få tag i sina pengar efter ett framgångsrikt bedrägeri?

Det finns oerhört många mer eller mindre kreativa sätt att tvätta pengar efter ett lyckat bedrägeri. Där man tidigare använde sig av money mules som med en väska fylld med sedlar for mellan länderna, har man idag digitaliserat förfarandet avsevärt. Transaktioner mellan bankerna är fortfarande vanliga, men då tillhör oftast mottagarkontot en utländsk bank och kontoinnehavaren är en fiktiv person.

Inte sällan använder man sig av växling till kryptovaluta för att försvåra polisens möjlighet att kunna identifiera vem mottagaren är. Eller så sätts pengarna in på ett spelkonto där de medvetet förloras mot en "kompis" vid pokerbordet på nätet.

Ett stort bekymmer just nu är de ekonomiska transaktioner som sker till länder som samarbetar dåligt med omvärlden, det vill säga inte lämnar ut uppgifter om vem mottagaren av transaktionen är eller återbördar beloppet. Det sker tusentals transaktioner till dessa banker varje år som europeisk polis aldrig har möjlighet att utreda. Där kan pengarna sedan tvättas lokalt genom att exempelvis investeras i produktion, som sedan säljs tillbaka till västvärlden i form av varor.

Vilka skulle du säga står bakom majoriteten av dessa bedrägerier; är det enskilda privatpersoner eller är det organiserade grupperingar?

När det kommer till mer omfattande verksamheter, såsom stora investeringsbedrägerier, rör det sig definitivt om organiserad brottslighet. De som hackar ditt Facebook-konto och ber anhöriga logga in på sin bank eller föra över pengar tillhör ofta mindre grupper som inte alltid är definierbara som organiserad brottslighet. Enskilda individer står dock bakom flertalet av de bedrägerier som sker på nätet, exempelvis kortbedrägerier som är det största enskilda brottet i Sverige idag.

Vilka är de vanligaste bedrägerierna idag?

Mest utbrett mot företag just nu är ransomware, även om få anmäler de brotten. Det näst största problemet är anställda som klickar på länkar i phishingmail och blir av med uppgifterna till sina Office 365-konton. Jag skulle säga att det i princip inte finns något företag med fler än 50 anställda som inte har drabbats av detta. Phishing överlag är ett stort problem som ligger till grund för de allra flesta komplexa bedrägerierna online – allt från breda ransomware-attacker till mer utstuderade VD-bedrägerier.

Vilka typer av bedrägerier kan vi förvänta oss att se mer av i framtiden?

Tittar man på brott riktade mot företag så kommer ransomware förbli det största problemet. En inte obetydlig del kommer att utgöras av mellanstatliga attacker i form av dataintrång i syfte att försöka tillskansa sig information av olika slag. Jag ser ingen anledning till att den utvecklingen kommer avta, eftersom det har visat sig vara väldigt gynnsamt.

Även på den privata sidan kommer phishing hålla i sig, främst på grund av stordriftsfördelarna; det kostar ingenting att genomföra, så även om det bara genererar en mindre summa per offer blir det mycket i slutändan. Parallellt tror jag även att investeringsbedrägerier kommer fortsätta öka på alla möjliga sätt, både i form av pyramidspel och andra typer av scams.

Men, kommer de fullbordade brotten öka över tid? Jag sticker nog ut hakan och säger att jag inte är så säker på det. Tidigare har vi som människor inte hängt med i den tekniska utvecklingen. Nu börjar vi närma oss en punkt där fler och fler av oss besitter kunskap och förståelse om hur den digitala världen fungerar. Och det visar ju sig i statistiken; många utsätts för bedrägeriförsök, men färre faller för det.

Med det sagt tror jag inte att internetbedrägerier någonsin kommer försvinna. Men vi kommer bättre på att skydda oss emot det; dels genom ökad medvetenhet, men även tack vare att företag tar större ansvar genom att se till att deras tjänster är säkra.

sentor

Om Sentor

Sentor är ett svenskt cybersäkerhetsföretag som möjliggör för organisationer att existera i en digitalt uppkopplad värld. Vi kombinerar spetskompetens, innovativ säkerhetsteknik och threat intelligence i syfte att hjälpa organisationer att bekämpa cyberkriminalitet, skydda data och minimera säkerhetsrisker.

Vi strävar även efter att höja den allmänna medvetenheten om säkerhet, bland annat genom att förse både privatpersoner och företag med information som bidrar till förbättrad kännedom och fördjupade insikter inom en rad olika ämnen kopplade till digital säkerhet.

Sedan 2018 driver vi även projektet Digital kvinnofrid tillsammans med Uppsala kvinnojour i syfte att stärka den digitala säkerheten hos kvinnojourer samt de kvinnor och barn de möter i sina verksamheter. Tack vara Digital kvinnofrids kompetenshöjande insatser får kvinnojourer och andra organisationer möjlighet att förbättra verksamhetens interna säkerhet, och ger dem kunskap och verktyg som kan förmedlas till stödsökande kvinnor.

För mer information, besök www.sentor.se