sentor

Svenskarnas syn på IT-säkerhet

2019

Innehåll

Förord

För fjärde året i rad genomför Sentor undersökningen “Svenskarnas syn på IT-säkerhet”. Målet med undersökningen är att både du som läsare och vi som kunskapsförmedlare ska få bättre insikt i hur svenskar tänker och agerar i frågor kopplade till IT-säkerhet. På så sätt hoppas vi även kunna identifiera och adressera verkliga behov och utmaningar, som i förlängningen kan ligga till grund för vårt gemensamma arbete med att höja landets IT-säkerhet på både individ- och verksamhetsnivå.

År 2019 har redan bjudit på flera uppmärksammade IT-säkerhetsincidenter. Den som fått överlägset störst medialt utrymme nationellt är “1177-läckan”, då ljudfiler med 2,7 miljoner inspelade samtal till 1177 Vårdguiden låg oskyddade på en öppen webbserver. Händelsen har sedermera beskrivits som en av de största personuppgiftsläckorna i svensk historia.

Incidenter av det här slaget, tillsammans med en rad andra faktorer, avspeglar sig förstås i den allmänna opinionen. En stor del av årets undersökning fokuserar därför på förtroende och lojalitet mot olika branscher, vilket vi kan konstatera varierar kraftigt. Till exempel skulle drygt hälften byta bank ifall det framkom att den har missbrukat vederbörandes personuppgifter, medan bara 1 av 10 skulle fortsätta använda ett spelbolags tjänster om det framkom att bolaget begått samma överträdelse.

Vi kan även konstatera att e-handelsföretag också har mycket att leva upp till när det gäller IT-säkerhet. 7 av 10 uppger att de hade bytt e-handelsleverantör om det framkom att de hade missbrukat personlig data, och 3 av 4 skulle undvika att handla av ett företag om de kände till att företaget utsatts för dataintrång. Den stora konkurrensen i spel- och e-handelsindustrin bidrar förstås till de höga siffrorna, och gör det kanske än viktigare för dessa aktörer att skapa förtroende och lojalitet bland sina kunder.

En annan intressant observation är att svenskarna generellt sett har ett lågt förtroende för våra politiska partier och deras företrädares förmåga att hantera känslig information. Mer än hälften uppger att de har lågt eller mycket lågt förtroende för våra politiska partiers förmåga att hantera känslig information, samtidigt som man ställer högre kunskapskrav på folkvalda och beslutsfattare än gemene man. 3 av 4 anser att förtroendevalda ska ha högre kännedom om IT-säkerhet än allmänheten, men bara 1 av 10 tror att samma personer införlivar de förväntningarna. Det tycks alltså finnas ett stort gap mellan förväntan och förtroende som förstås får betraktas som en utmaning svensk politik står inför.

Detta och mycket mer finns att ta del av i rapporten i sin helhet.

Vid frågor om rapporten, maila oss på info@sentorsecurity.com.

Trevlig läsning!
Martin Zetterlund, vd

Förtroende för statliga och privata organisationer

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

1

Under de senaste åren har flera säkerhetsincidenter uppmärksammats och kanske är det just därför – post Facebook och Cambridge Analytica – som sociala medier har lägst förtroende hos svenskarna. Hela 80 procent har lågt eller mycket lågt förtroende för sociala mediers förmåga att hantera känslig data. I toppen hittar vi bankerna, trots att förtroendet för sektorn sjunkit med 19 procent sedan 2018.

*Med känslig information menas exempelvis kreditkortsuppgifter

MYNDIGHETER:
28 % har lågt eller mycket lågt förtroende
67 % har högt eller mycket högt förtroende
5 % har ingen åsikt

KOMMUNER:
36 % har lågt eller mycket lågt förtroende
56 % har högt eller mycket högt förtroende
8 % har ingen åsikt

BANK:
23 % har lågt eller mycket lågt förtroende
73 % har högt eller mycket högt förtroende
4 % har ingen åsikt

SJUKVÅRD:
25 % har lågt eller mycket lågt förtroende
71 % har högt eller mycket högt förtroende
4 % har ingen åsikt

FÖRETAG:
40 % har lågt eller mycket lågt förtroende
46 % har högt eller mycket högt förtroende
14 % har ingen åsikt

SOCIALA MEDIER:
81 % har lågt eller mycket lågt förtroende
12 % har högt eller mycket högt förtroende
7 % har ingen åsikt

MEDIER:
64 % har lågt eller mycket lågt förtroende
25 % har högt eller mycket högt förtroende
11 % har ingen åsikt

E-HANDEL:
46 % har lågt eller mycket lågt förtroende
41 % har högt eller mycket högt förtroende
13 % har ingen åsikt

POLITISKA PARTIER:
56 % har lågt eller mycket lågt förtroende
28 % har högt eller mycket högt förtroende
16 % har ingen åsikt

SPELBOLAG:
(Online gambling, live casino):
65 % har lågt eller mycket lågt förtroende
12 % har högt eller mycket högt förtroende
23 % har ingen åsikt

STREAMING-TJÄNSTER/ UNDERHÅLLNINGS-TJÄNSTER:
(Netflix/Spotify):
41 % har lågt eller mycket lågt förtroende
40 % har högt eller mycket högt förtroende
19 % har ingen åsikt

- Lågt eller mycket lågt förtroende
- Högt eller mycket högt förtroende
- Ingen åsikt

Högst förtroende bland svenskarna har banker och sjukvård. Lägst förtroende har spelbolag och sociala medier. Förtroendet för företag och e-handelsbolag har ökat jämfört med föregående år (21 procent respektive 17 procent ökning från föregående år). Trots att bank toppar listan har svenskarnas förtroende för sektorn sjunkit med 19 procent sedan 2018. Mer än hälften har lågt eller mycket lågt förtroende för politiska partier. Många kan inte ta ställning till spelbolagen, förmodligen för att många inte har någon erfarenhet av deras tjänster.

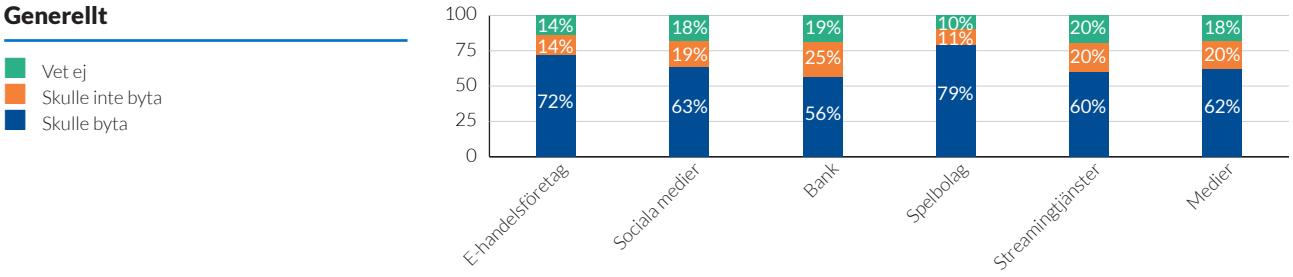
2

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

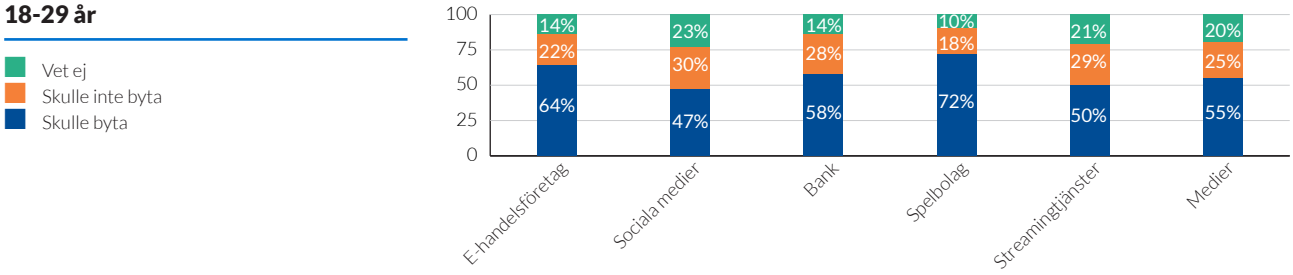
Generellt sett är vi mest förlåtande mot banker och minst lojala mot spelbolag. Drygt hälften skulle byta bank om det framkom att de har missbrukat vederbörandes personuppgifter, medan bara 1 av 10 skulle fortsätta använda ett spelbolags tjänster om det framkom att de missbrukat personuppgifter. Här bör man dock väga in att det är betydligt lättare att byta spelleverantör än bank. Samma sak gäller e-handelsföretag, som 7 av 10 uppger att de hade bytt ut om de framkom att de hade missbrukat personlig data.

Åldersmässigt tenderar yngre att ha mer överseende med leverantörer som brister i sin datahantering än de äldre ålderskategorierna. Exempelvis svarar bara 47 procent i åldergruppen 18-29 att de skulle sluta använda sociala medier, medan motsvarande siffra bland 60- till 75-åringar är 77 procent.

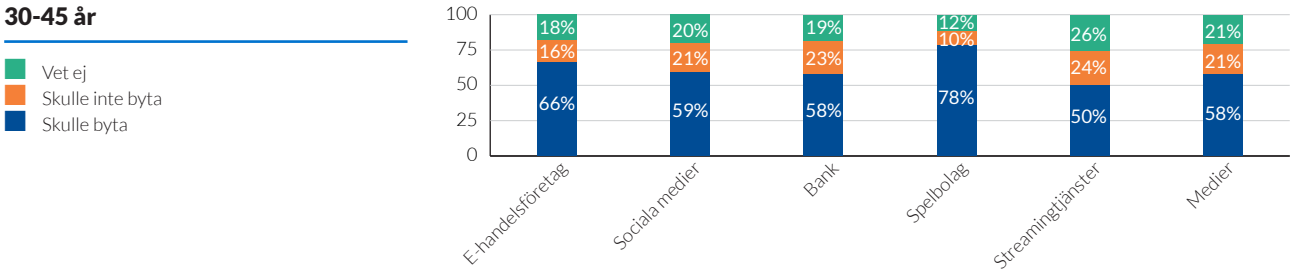
Generellt



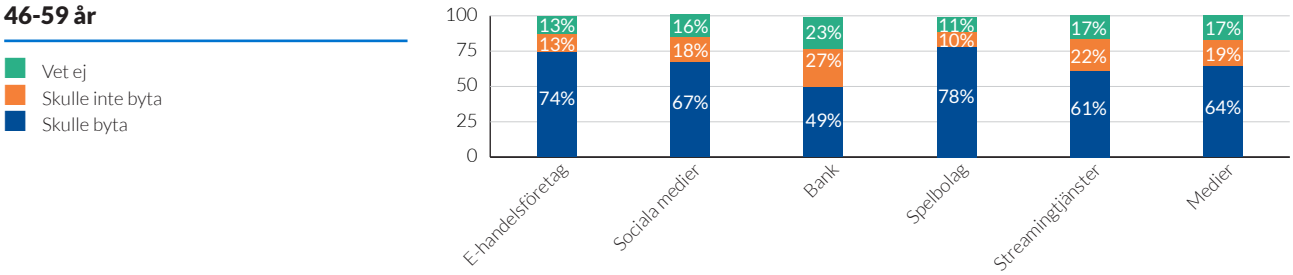
18-29 år



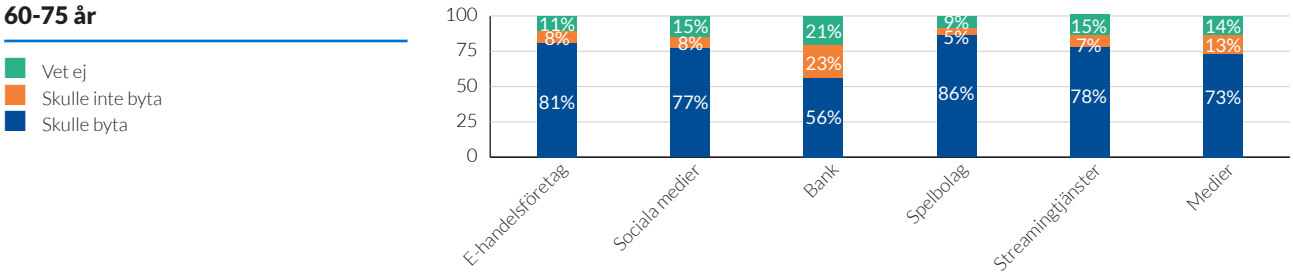
30-45 år



46-59 år



60-75 år



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

3

Undersökningen visar att 3 av 4 skulle undvika att handla av ett företag om de kände till att företaget utsatts för dataintrång. En nedåtgående trend, om vi jämför med föregående år. 2018 svarade 78 procent och 2017 svarade 83 procent att de skulle undvika att handla från ett sådant företag. Kanske bidrar den ökade mediala uppmärksamheten kring IT-säkerhetsattacker till att de normaliseras.

Ja: **74 %**
Nej: **26 %**

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)?

4

Uppsåtet är viktigt – en slutsats vi kan dra om vi jämför denna frågan med föregående fråga. Närmare 9 av 10 (88 procent) skulle inte handla av ett företag som missbrukat personlig data, medan 74 procent uppgav att de skulle undvika att handla från ett företag som istället utsatts för en attack.

Ja: **12 %**
Nej: **88 %**

Dataintrång – vad innebär det?

!

Dataintrång innebär att man utan tillstånd väljer att ge sig själv tillgång till information som lagras digitalt. Att manipulera eller radera information utan tillstånd räknas också som brottsligt.

Att utföra ett dataintrång kan även inkludera att hindra andra från att använda ett system. Det kan till exempel ske i form av överbelastningsattacker som syftar till att generera så mycket webbtrafik mot exempelvis ett webbformulär att det inte går att använda.

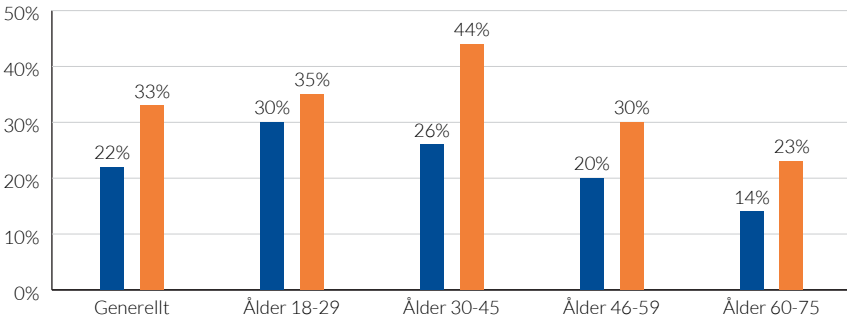
Inställning till säkerhet i hemmet / Internet of Things

1

Innehar du enheter i ditt hem som är uppkopplade till internet (IoT), som exempelvis högtalare, övervakningskameror, termostater, lås eller hushållsapparater?

Var tredje svensk har uppkopplade prylar, så kallade IoT-enheter, i sitt hem. Det är en ökning med 50 procent från i fjol. Vanligast förekommande är de i åldersgruppen 30-45 år, där nästan hälften (44 procent) uppger att de har uppkopplade prylar i hemmet. Det i sig är en ökning på 69 procent sedan föregående år.

2018
2019



Nedan presenteras svar från dem som svarat ja på fråga 1.

1a

Har du ett separat nätverk uppsatt för dina uppkopplade IoT-enheter?

Ja: **20 %**
Nej: **80 %**

Om du behöver ansluta en IoT-enhet bör du överväga att skapa ett separat trådlöst nätverk enbart för dessa 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. Bara 1 av 5 som har uppkopplade prylar i hemmet uppger att de använder ett separat nätverk för dessa.

1b

Har du någon gång uppdaterat programvara/operativsystem i dina IoT-enheter?

Ja: **56 %**
Nej: **44 %**

Många leverantörer av IoT-prylar prioriterar att få ut sina produkter snabbt på marknaden och slarvar med att tillhandahålla säkerhetsuppdateringar. Följden blir att många svenskar har sårbara IoT-enheter i sina hem. På frågan hur många som uppdaterar sina enheter är det endast drygt hälften som svarar ja.

Har du någon gång bytt standardlösenord på dina IoT-enheter?

1c

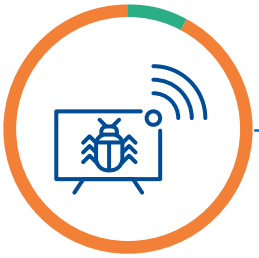
Att byta ut standardlösenordet på sina IoT-enheter är ett enkelt sätt att höja säkerheten, eftersom det ofta är simpelt och kan ha läckt ut på nätet. Välj en stark lösenordsfras som bara du känner till och se till att du inte återanvänder lösenordet någon annanstans. Drygt hälften uppger att de har bytt ut standardlösenorden på sina IoT-enheter.

Ja: **57 %**
Nej: **43 %**

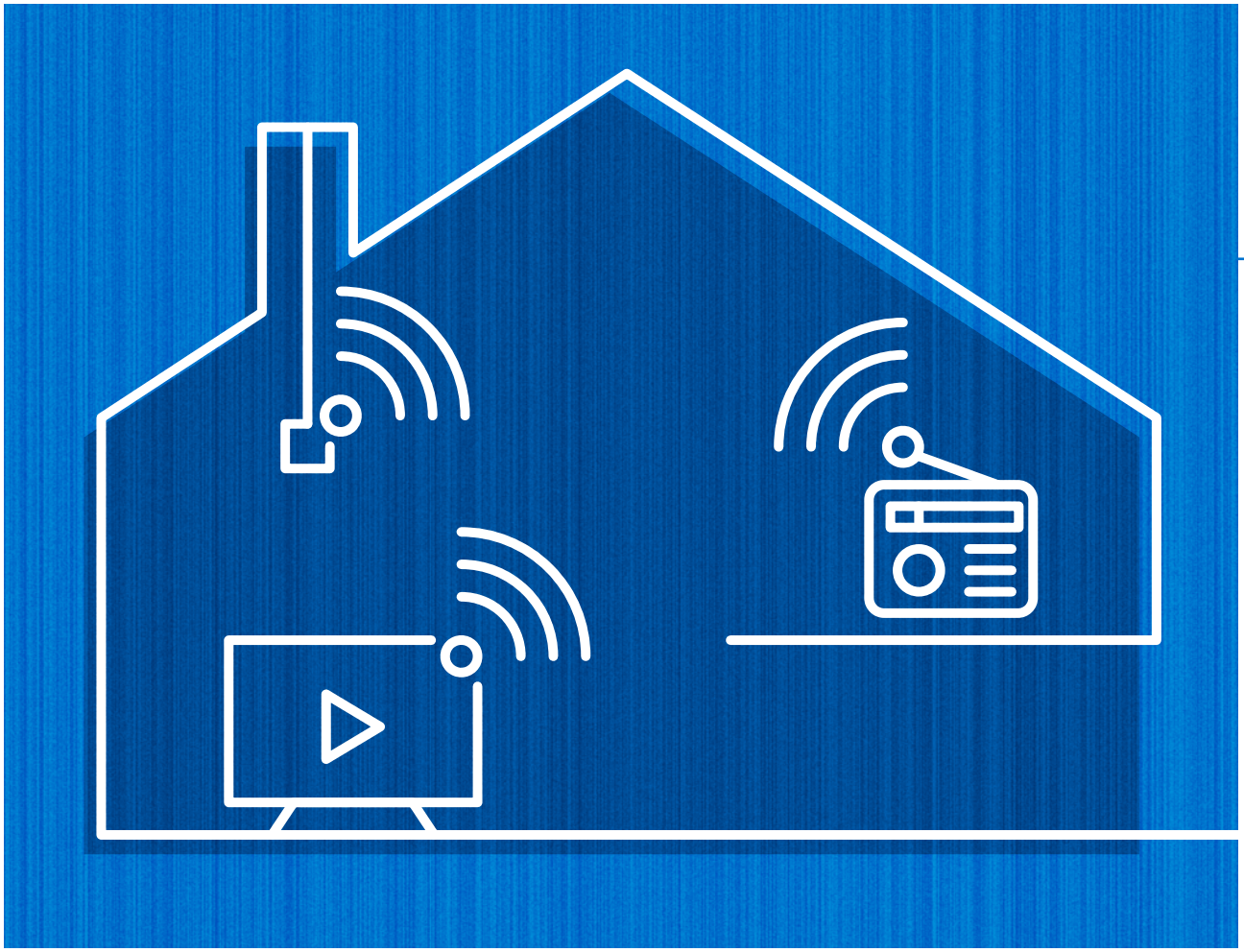
Skulle du köpa en IoT-enhet från en leverantör som har drabbats av en uppmärksammad säkerhetsincident?

1d

Undersökningen visar att konsumenterna ställer höga krav på säkerhet när de väljer sina leverantörer. Drygt 9 av 10 skulle inte köpa IoT-enheter från en leverantör som de vet har drabbats av en säkerhetsincident.



Ja: **8 %**
Nej: **92 %**



Riskerna med 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 man på olika sätt dra nytta av nya funktioner och underlätta vardagen. Det kan till exempel vara din garageport som känner av när du närmar dig dörren, eller dina glödlampor som tänds på beställning för att avskräcka tjuvar när du är på semester. Men precis som med andra enheter som är anslutna till internet så tillkommer också säkerhetsaspekter att ta i beaktning.

Vi användare uppskattar när det är enkelt att komma igång och ansluta våra enheter till internet. Genom att bara koppla in din enhet kan den automatiskt be om att få ansluta till ditt trådlösa nätverk, sedan är du igång.

Det finns dock skäl att vara restriktiv med vilka IoT-enheter du ansluter till internet, då de i många fall innehåller säkerhetsbrister. Ofta beror det på att många av de tillverkande företagen har lite erfarenhet av att producera produkter som ansluts till internet.

Organisationerna som står bakom många av IoT-produkterna lägger ofta resurser på design och användarvänlighet, samt att generera vinst. Säkerhet är dessvärre fortfarande inte ett prioriterat område hos många leverantörer.

Nackdelen för dig som användare är att du ofta har få alternativ eller ingen möjlighet alls att konfigurera enheterna för att stärka säkerheten. Du är beroende av den produkten som du har köpt eller fått levererat. Dessutom kan produkterna vara svåra att uppdatera, om de ens har den möjligheten. Det innebär att många av de IoT-enheter du inhandlat redan kan ha allvarliga säkerhetsbrister som andra redan har utnyttjat. Det kan få till följd att enheten ansluts till ett botnet så fort den ansluts till internet. Din enhet kan på så vis bli en delkomponent i en angripares överbelastningsattack

”När ett område växer så pass fort som IoT är det svårt att undvika att marknaden fylls på med aktörer som inte tar säkerheten på allvar. Det har resulterat i att Internet allt snabbare fylls med sårbara prylar. Detta utgör dels en risk för konsumenten, då uppkopplade prylar i hemmet kan läcka känslig information eller vara en väg in för angripare till användarens nätverk. Men det utgör också en fara för resten av Internet, eftersom hackade prylar ofta används i attacker mot andra offer, genom så kallade botnät.”

säger Joel Rangsmo, säkerhetsexpert på Sentor.

Säker mobilanvändning

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

1

Att hålla mobilens applikationer uppdaterade är viktigt för att undvika säkerhetshål. När leverantörerna släpper nya uppdateringar är det inte ovanligt att de innehåller säkerhetsfixar på kända sårbarheter. De kan även göra så att telefonen får ny funktionalitet och bättre prestanda.

- **34 %** har automatiska uppdateringar/uppdaterar inom en dag
- **24 %** uppdaterar inom en vecka från att det har meddelats att nya uppdateringar finns tillgängliga
- **18 %** uppdaterar när applikationer eller annat säger att de måste för att de ska fungera som de ska
- **10 %** uppdaterar inom en månad efter att det har meddelats att nya uppdateringar finns tillgängliga
- **8 %** vet inte eller har ingen uppfattning
- **4 %** har inte en smartphone
- **2 %** uppdaterar inte operativsystemet

Hur hanterar du uppdateringar av appar till din smartphone (exempelvis Facebook, Instagram eller BankID)?

2

De flesta apputvecklare jobbar ständigt med förbättringsarbete för sina appar. Genom att löpande uppdatera appar undviks sårbarheter. Vår undersökning visar att allt fler har automatiska uppdateringar av sina appar på daglig basis: 47 procent i år, jämfört med 39 procent 2018. Det är idag det vanligaste sättet att sköta sina uppdateringar.

- **47 %** har automatiska uppdateringar/uppdaterar inom en dag
- **19 %** uppdaterar inom en vecka från att det har meddelats att uppdateringar finns tillgängliga
- **19 %** uppdaterar när applikationer eller annat säger att de måste telefonen ska fungera som den ska
- **7 %** uppdaterar inom en månad
- **6 %** vet inte eller har ingen uppfattning
- **2 %** uppdaterar inte appar

3

Använder du dig av en lösenkod eller motsvarande (exempelvis fingeravtryck eller Face ID) för att logga in i din smartphone?

- Ja: **20 %**
- Nej: **42 %**
- Vet ej/vill ej uppge: **38 %**

Bara 1 av 5 uppger att de har lösenkod eller motsvarande på sin smartphone. Dessa siffror är antagligen inte helt korrekta, eftersom någon typ av lås brukar tillhöra standardinställningarna. En förklaring kan vara att det finns en oförståelse för frågan.

4

Hur hanterar du användandet av platstjänster i din smartphone?

- **60 %** tillåter endast platstjänster för specifika applikationer
- **16 %** har aldrig platstjänster påslaget
- **16 %** har alltid platstjänster aktiverat
- **8 %** vet ej om de har platstjänster aktiverat

Endast 8 procent av respondenterna har inte koll på om de har platstjänster aktiverat. Resterande har gjort ett aktivt val där de flesta, 60 procernt, enbart tillåter tjänsten för specifika appar.

5

Hur ser du på att stora aktörer (som exempelvis Google, Apple och Facebook) samlar in din platsinformation/geo-data från din smartphone?

- **17 %** är mycket negativt inställd
- **34 %** är negativt inställd
- **37 %** är varken positivt eller negativt inställd
- **7 %** vet ej/ingen uppfattning
- **5 %** är positivt inställd
- **0 %** är mycket positivt inställd

Varannan ser negativt på insamling av platsinformation. Mycket få, bara 5 procent, uppger att de är positiva och ingen svarar att de är mycket positivt inställda.

!

Du vet väl om att dina appar kan avslöja vart du befinner dig?

Många tänker inte på att deras användning av appar och sociala medier och kan avslöja information kring vart de befinner sig. För att säkerställa att du inte delar med dig av information som du vill hålla hemlig, finns det en rad säkerhetsåtgärder du kan vidta;

1. Använd inte delade konton till tjänster som Netflix och Spotify: andra användare på kontot kan se din IP-adress och aktivitet
2. Använd unika lösenord och aktivera tvåfaktorsautentisering
3. Stäng av platstjänster
4. Ta reda på vilken information dina appar samlar in och delar
5. Radera onödiga appar

Surfa säkert

Har du anslutit till ett publikt öppet trådlöst nätverk (exempelvis på tåg, flygplatser och caféer) under de senaste 12 månaderna?

1

Att ansluta sig till öppna nätverk kan vara en säkerhetsrisk av flera skäl. En potentiell angripare kan till exempel välja att störa ut ett trådlöst nätverks signal med ett eget Wi-Fi. Genom att sätta upp ett trådlöst nätverk på centralstationen och exempelvis döpa det till Free Public Wifi går det att få många ovetande användare att ansluta sig. När väl det är gjort är det öppet mål för angriparen att börja samla in kritisk information eller utnyttja informationen för att iscensätta en attack. I undersökningen uppger 3 av 5 har anslutit sig till publika öppna nätverk under det senaste året.

62 % har anslutit sig
38 % har inte anslutit sig

Om ja, Använde du VPN vid detta tillfälle/dessa tillfällen?

2

Ett sätt att skydda sig vid uppkoppling mot ett publikt nätverk är att använda VPN. Med hjälp av en VPN-lösning krypteras informationen mellan din dator och VPN:ets termineringspunkt och gör det betydligt svårare för en potentiell angripare som är uppkopplad på samma Wi-Fi att komma åt din informationen. Enligt undersökningen använde endast 9 procent sig av VPN vid tillfället eller tillfällena de anslöt sig till publika nätverk.

Ja: **9 %**
Nej: **62 %**
Ibland: **29 %**

Är jag säker om jag använder VPN?

!

Det är utan tvivel så att du surfar säkrare med VPN är utan. Men en VPN-tjänst ger inget hundraprocentigt skydd mot alla faror på nätet. VPN är ett viktigt verktyg, men är fortfarande bara en del i en längre säkerhetskedja. Trots fördelarna och tryggheten VPN medför, bör man fortfarande vara noggrann med andra delar i säkerhetskedjan, som exempelvis att använda sig av säkra lösenord, kryptera enskild information, använda antivirus-program, och uppdatera operativsystem och programvaror till senaste versionen.

Säker mailanvändning

1

Anser du att ditt lösenord till ditt primära mailkonto är säkert?

- **82 %** anser att deras lösenord är säkert
- **18 %** anser att deras lösenord inte är säkert

Att ha ett säkert lösenord är A och O för att undvika att drabbas av ett dataintrång. Andelen som anser att deras lösenord till mailen är säkert fortsätter öka. År 2017 ansåg sig 74 procent ha ett säkert lösenord, år 2018 var motsvarande siffra 78 procent. I år har siffran stigit till 82 procent.

2

Hur många tecken har du i lösenordet till ditt primära mailkonto?

- **24 %** svarar att deras lösenord består av 1-8 tecken
- **45 %** svarar att deras lösenord består av 9-12 tecken
- **12 %** svarar att deras lösenord består av 13 eller fler tecken
- **19 %** svarar att de inte vet eller inte vill uppge hur många tecken deras lösenord består av

Det är generellt sett bättre att ha ett lösenord med många tecken än ett med få. En kombination av olika sorters tecken innebär också att man försvårar för någon med onda avsikter. Endast 12 procent svarar att de använder sig av 13 tecken eller fler.

3

Använder du samma lösenord på någon annan internettjänst som du använder för din primära mail?

- **27 %** använder samma lösenord till sin mail som till andra tjänster på internet
- **53 %** använder inte samma lösenord till sin mail som till andra tjänster på internet
- **20 %** vet ej eller vill inte uppge om de använder samma lösenord till sin mail som till andra tjänster på internet

Genom att ha unika lösenord säkerställer man att ett dataintrång eller slarv någonstans inte drabbar ens andra konton. Eftersom mailen ofta är navet i ens digitala liv är det viktigt att lägga extra energi på att skapa ett bra lösenord där. Drygt hälften uppger att de har unika lösenord till sin mail.

Använder du tvåfaktorsautentisering vid inloggning på ditt primära mailkonto?

4

Tvåfaktorsautentisering innebär ett extra krav utöver ditt lösenord som visar på att du verkligen är du, oftast i form av en verifikationskod som skickas till dig via SMS eller en genererad kod i en app. Många onlinetjänster erbjuder tvåfaktorsinloggning. Trots det använder bara 1 av 5 tvåfaktorsautentisering när de loggar in på sitt mailkonto.

- **20 %** använder tvåfaktorsautentisering
- **42 %** använder inte tvåfaktorsautentisering
- **38 %** vet ej eller vill inte uppge om de använder tvåfaktorsautentisering

Tips för att inte få ditt lösenord hackat

!

1. **Välj ett långt lösenord**
   Ett tips är att du använder dig av en mening.
2. **Använd olika sorters tecken**
   Å, ä och ö är riktigt bra bokstäver att ha med.
3. **Välj bort personliga referenser**
   Din adress, ditt personnummer eller ditt namn bör undvikas.
4. **Använd olika lösenord för olika konton**
   Och tänk på att ha ett extra bra lösenord till mejlen!
5. **Använd tvåfaktorsautentisering**
   Exempelvis en verifikationskod som skickas via sms efter att du skrivit in det korrekta lösenordet.

Nätfiske och övriga bedrägerier

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

1

58 % ja
42 % nej

Fler än hälften av svenskarna har mottagit phishingmail, även kallat nätfiske, som i grund och botten är en form av social engineering. Angreppsmetoden går ut på att en eller flera bedragare skickar mail där de utger sig för att vara till exempel en bank eller en myndighet i syfte att få mottagaren att klicka på länkar eller ladda ner filer. Den som låter sig luras av ett sådant mejl kan därmed lockas att lämna ifrån sig kritisk information eller få sin dator infekterad av skadlig kod.

!

Så slipper du drabbas av nätfiske

Agera inte impulsivt
Angriparna försöker spela på din impulsiva sida genom att sända meddelanden som antingen intresserar dig eller som vill varna dig om något. Ett typiskt exempel är ”PostNord”-mejlen där mottagaren fått reda på att ens fraktsedel finns att ladda ned. Ett annat exempel är när ”Apple” ber dig om att uppdatera din kontoinformation till AppStore till följd av ett dataintrång.

Läs igenom mailet
De som står bakom den här typen av bluffmejl skickar ofta tusentals mejl samtidigt, ibland talar de inte ens språket som sina mottagare talar. Därför kör de mejlen genom någon översättningstjänst vilket många gånger leder till att språket blir bristfälligt formulerat i dessa mejl. Genom att läsa igenom mejlet ordentligt går det ofta att avslöja att det inte är någon större aktör som står bakom mejlet som har hamnat i din mejlkorg.

Kolla avsändaradressen
Det går att avslöja många av attackförsöken genom att ta en ordentlig titt på avsändaradressen. Vissa bedragare gör ingen ansats till att ens bry sig om avsändaradressen ut låter den var exempelvis suw43242@tse34rs.ru. Då är det lätt att se skillnad. Lite knepigare blir det när de ändrar en bokstav till en annan liknande bokstav eller siffra, exempelvis no-reply@bl0cket.se.

Du hittar fler tips på www.sentor.se

Om ja på fråga 1, lämnade du då ifrån dig pengar eller känslig information?

2

Det är viktigt att aldrig någonsin lämna ut uppgifter såsom kreditkortsuppgifter, inloggningsinformation eller bankkoder i ett mail. Banker eller myndigheter ber aldrig om den här typen av uppgifter via mail. Endast 1 procent av de som har mottagit den här typen av mail uppger att de vid tillfället lämnade ifrån sig pengar eller känslig information.

- **1 %** ja
- **99 %** nej

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

3

Det finns en rad olika saker man kan leta efter för att avslöja bluffmail. Bland annat genom att titta på avsändaradressen och hur mailet är formulerat. Felstavningar, personliga hälsningsfraser och långa och krångliga länkadresser är exempel på varningssignaler som indikerar att mailet inte är legitimt.

- **15 %** anser att de har svårt att urskilja bluffmail från legitima
- **85 %** anser att de inte har svårt att urskilja bluffmail från legitima

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

4

Så kallad smishing, sms-versionen av phishing, blir allt vanligare. Det kan exempelvis handla om att ett en förfalskad företagsadress skickar ut ett väldigt fördelaktigt erbjudande, i syfte att få mottagaren att klicka på en infekterad länk. Nästan 4 av 10 uppger att de har utsatts för smishing under de senaste 12 månaderna.

- **38 %** ja
- **62 %** nej

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

5

En femtedel uppger att de blivit kontaktade av personer på sociala medier, med syfte att lura av dem känslig information. En nedåtgående trend jämfört med 2018 då 30 procent svarade att de utsatts för bedrägeriförsök via sociala medier.

- **22 %** uppger att de har blivit kontaktade av personer via sociala medier vars syfte har varit att lura av dem känslig information
- **78 %** uppger att de inte har blivit kontaktade av personer via sociala medier vars syfte har varit att lura av dem känslig information

Fem vanliga social engineering-tekniker att hålla koll på

Vi har blivit allt mer bekanta med den typ av angripare som utnyttjar sina tekniska färdigheter för att hacka sig in i system och äventyra känslig data. Det finns dock andra typer av angripare som kombinerar sin tekniska kunskap med ett stort mått av social manipulation, så kallad social engineering. Nedan följer information om de fem vanligaste typerna av attacker som sociala ingenjörer använder för att nå sina mål: phishing, pretexting, tailgating, baiting och quid pro quo.

1. Phishing

Phishing, eller nätfiske, är en attack där angriparen väljer ut en eller flera mottagare och skickar falska mail utformade för att imitera en verklig person eller ett utskick från en organisation. Målet kan exempelvis vara att samla in kritisk information, dirigera offret till en infekterad webbplats eller manipulera mottagaren att agera snabbt utan att tänka.

När vi tänker på phishing tänker vi ofta på sämre utformade mail som innehåller både stavfel och grammatiska fel. Men i de fall en social ingenjör har riktat in sig på ett specifikt företag eller en specifik person, brukar attackerna ske med stor finess. Sådana riktade phishing-attacker, brukar benämnas som spear phishing. I dessa fall gör angriparen ett ordentligt researcharbete där man exempelvis kartlägger anställdas intressen i sociala medier och organisationens hierarki för att kunna skicka träffsäkra mail.

2. Pretexting

Pretexting är den mänskliga motsvarigheten till phishing, där någon utger sig för att vara en auktoritet inom ett område eller någon att lita på. Detta kan göras för att stjäla inloggningsuppgifter eller för att installera skadlig kod på datorn.

Ett vanligt tillvägagångssätt är att en angripare utger sig för att vara från företagets IT-support. Genom att övertyga användaren om att exempelvis en ny version av specifik programvara behöver installeras kan angriparen få tillgång till datorn och installera skadlig kod på den. Eftersom som få i stora organisationer har koll på vilka som arbetar i IT-supporten är det sannolikt att offret inte anar oråd över huvud taget.

Pretexting handlar till mångt och mycket om att bygga upp en trovärdig historia som gör att offret känner sig trygg i situationen och är benägen att dela med sig av både information och sin dator.

3. Tailgaiting

Tailgating innebär att angriparen helt enkelt följer efter en anställd på företaget in i ett begränsat område. Traditionellt kan det vara någon som ber framförvarande ifall de kan hålla upp dörren eftersom angriparen påstår sig ha glömt sitt passerkort. Väl inne i lokalen kan angriparen sedan utnyttja samma välvilja eller smälta in i en stor grupp av människor och ta sig vidare längre in i lokalen.

Tailgating kan även ta formen av att någon ber om att få låna en telefon eller laptop för att utföra en enklare åtgärd. Vad som egentligen sker är att någon tar chansen att installera skadlig programvara eller på något annat sätt utnyttjar den utlånade enheten.

4. Baiting

Baiting är precis vad det låter som, att angriparen slänger ut ett lockbete i syfte att lura privatpersoner eller företagsanställda att göra något som äventyrar deras egen eller organisationens säkerhet.

Ett sätt att utnyttja tekniken är att lämna ett USB-minne på ett strategiskt lämpligt ställe, märkt med ett relevant budskap. När USB-minnet sedermera installeras i datorn infekteras personens dator och eventuellt även företagets nätverk. Den skadliga koden kan sedan användas för att göra det möjligt för angriparen att exempelvis spionera på organisationen eller komma åt kritisk data.

5. Quid Pro Quo

Quid Pro Quo (this for that) tar sig formen av en begäran om att få information i utbyte mot ersättning. Det kan röra sig om att få ett klädesplagg eller invites till populära tjänster i ersättning mot inloggningsuppgifter.

Det kan låta som ett ineffektivt sätt att komma åt kritisk data, men har i själva verket visat sig vara tvärtom. Verkliga exempel har visat att det inte krävs så mycket för att anställda ska ge bort sina inloggningsuppgifter. Det kan i själva verket räcka med en billig penna eller en chokladbit.

Inställning till IT-säkerhet

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

1

Ju mer komplicerade attacker, desto större ansvar avkrävs av alla som som använder internet och uppkopplade enheter. Men trots att kunskapsnivån behöver öka, är det allt färre som känner sig oroade över sin IT-säkerhet. Närmare hälften känner oro för att en IT-säkerhetsattack ska drabba dem, cirka 10 procent färre än 2018.

- Ja; **48 %**
- Nej; **52 %**

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

2

Hela 60 procent upplever att det har blivit svårare att ta hand om den egna IT-säkerheten och endast 3 procent tycker att det känns lättare än tidigare. Oron bör betraktas som befogad, då vi exponeras för allt fler säkerhetsrisker i och med det ökande antalet digitala tjänster och produkter.

- Mycket lättare; **1 %**
- Något lättare; **2 %**
- Varken eller; **27 %**
- Något svårare; **39 %**
- Mycket svårare; **21 %**
- Vet ej; **10 %**

"Många svenskar inser exempelvis inte att det där viruset de har fått på datorn inte bara "segar ner" datorn utan också spionerar på dig eller använder din dator i ett så kallat botnät för att attackera större mål"

Hanna Eldmar, SOC Manager

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

3

Hur du skyddar dina digitala enheter är en bred fråga och inte alltid så lätt att svara på. Trots det svarar hälften att de vet hur de ska skydda sina digitala enheter från intrång - en minskning med 7 procent från 2018 då hela 58 procent upplevde att de besatt den kunskapen.

- Ja; **51 %**
- Nej; **49 %**

Tre tips som ökar din IT-säkerhet

Uppdatera programvaran
Nätbedragare letar ständigt säkerhetshål i de program du använder. Samtidigt gör leverantörerna sitt bästa för att täppa till dessa hål. Ställ in dina program så att de uppdateras automatiskt för bästa skydd.

Klicka inte!
Klicka inte på länkar eller bifogade filer om du inte litar på avsändaren. Nätfiske, där bedragare skickar mejl som ser ut att komma från riktiga företag som du kanske har konto hos, är en av de vanligaste farorna på internet.

Lämna inte ut information
Lämna aldrig ut din personliga information – vare sig över telefon, via mail eller på nätet – om du inte är helt säker på att motparten är vem den utger sig för att vara.

4

Tycker du att folkvalda eller beslutsfattare (såsom riksdagsledamöter) ska ha en högre kännedom/kunskap inom IT-säkerhet än allmänheten?

Ja; **75 %**
Nej; **25 %**

3 av 4 ställer högre krav på folkvaldas kunskap om IT-säkerhet än resten av allmänheten. Kraven kan betraktas som befogade, då dessa personer tenderar att hantera känslig eller till och med hemlig information i större utsträckning än andra grupper. Att de är just förtroendevalda bidrar förmodligen också till de höga förväntningarna.

5

Tror du att folkvalda eller beslutsfattare (såsom riksdagsledamöter) har en högre kännedom/kunskap inom IT-säkerhet än allmänheten?

Ja; **11 %**
Nej; **89 %**

Trots att förväntningarna på kunskapsnivån är hög, är det bara 11 procent som tror att våra folkvalda har en större kunskap om IT-säkerhet än gemene man. Varför är en svår fråga att besvara, men statistiken visar tydligt att det finns en kommunikationsutmaning för partier och folkvalda att bemöta.

sentor

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.

sentor.se