Årsrapport för 2020 gällande säkerhetsbeteenden för lösenord och autentisering

Har privatpersoner och IT-experter samma syn på säkerhetsfrågor?

En ny studie från Ponemon Institute visar att, trots ökande integritets- och säkerhetsproblem, både IT-experter och privatpersoner använder riskabla säkerhetsrutiner. Men förväntningar och verklighet möts sällan mellan de två grupperna när det handlar om implementeringen av användbara och önskvärda säkerhetslösningar.

Privatpersoner *vs.* IT-experter:

Attityder och beteenden kring säkerhet

Privatpersoner		IT-experter
25%	Har blivit **mycket mer oroade** för sin personliga integritet och datasäkerhet under de senaste två åren.	41%
76%	Av de tillfrågade som upplevt en **kontokapning** har vissa förändrat sitt sätt att hantera lösenord eller hur de skyddar sina konton.	69%
64%	**Använder inte** 2FA som en form av skydd för personliga konton.	60%
39%	**Återanvänder lösenord** på arbetet.	45%
51%	**Delar lösenord** med kollegor, ibland eller ofta.	42%

Säkerhet i organisationer

Av IT-experter anger **51%** att deras organisationer har upplevt en **nätfiskeattack**, medan **12%** av respondenterna har varit med om en **identitetsstöld** och **8%** har upplevt en **man-i-mitten-attack**.

31% av IT-experter hävdar att deras organisation använder en **lösenordshanterare** som ett effektivt verktyg för att skapa, hantera och lagra lösenord.

42% av IT-experter rapporterar att deras organisation är beroende av **lappar** för att hantera lösenord.

59% av IT-experter rapporterar att deras organisation är beroende av **det mänskliga minnet** för att hantera lösenord.

Lösenordshantering och förebyggande av kontokapning

46% av IT-experter **behöver använda 2FA för att få åtkomst** till företagskonton

37% av organisationerna som implementerar 2FA för att säkra kundkonton **använder mobila autentiseringsappar** och **28% använder SMS-koder.**

23% av privatpersonerna anser att 2FA-metoder som SMS eller mobila autentiseringsappar är **mycket opraktiska.**

54% anser att SMS eller mobila autentiseringsappar **stör deras arbetsflöde.**

47% anser att det är **irriterande** att kopiera och klistra in engångskoder.

Säkerhet för mobiltelefoner på arbetet

55% av organisationer **tillåter användning av privata mobiltelefoner.**

62% av organisationerna tror inte att de vidtar nödvändiga åtgärder för att **skydda information på mobiltelefoner.**

56% av de tillfrågade som använder en privat mobiltelefon för att få åtkomst till arbetsrelaterade artiklar **använder inte 2FA.**

Skydd av kundernas konton

Kundinformation och **personligt identifierbar information (PII)** är IT-experters högsta prioritet, dock rapporterar **61%** av svenskarna att kundkonton har varit föremål för ett kontokapning.

56% anser dock att användarnamn och lösenord erbjuder **tillräcklig säkerhet.**

23% av IT-experter **har inga planer** på att erbjuda 2FA till kunderna.

43% anser att det skulle bli **opraktiskt** för kunderna.

När det handlar om åtkomst till information på nätet anger privatpersoner att säkerhet (56%), prisvärdhet (57%) och användbarhet (35%) är mycket viktiga frågor.

En säkrare framtid

50% av svenskarna kommer endast att ta till sig nya tekniker som är enkla att använda och som förbättrar säkerheten.

51% av de tillfrågade svenskarna skulle föredra en metod för att skydda konton som inte innehåller lösenord.

56% av IT-experter anser att eliminering av lösenord skulle **förbättra säkerheten i deras organisation.**

54% av IT-experter anser att eliminering av lösenord skulle vara **betydligt mer praktiskt.**

59% av IT-experter anser att **användning av biometrisk alternativ** skulle öka säkerheten i deras organisation.

och **53%** av privatpersoner anser att användning av biometrisk alternativ skulle **förbättra säkerheten.**

54% av svenskarna anser att en **säkerhetsnyckel för hårdvaruautentisering** skulle ge ökad säkerhet.

60% av privatpersoner skulle vara **villiga att betala cirka 500 SEK** för att få högsta säkerhetsnivån för sina online-konton.

Hela Ponemon Institutes undersökning *Årsrapport för 2020 gällande säkerhetsbeteenden för lösenord och autentisering* finns på **https://www.yubico.com/authentication-report-2020/**

yubico

www.yubico.com

Yubico grundades 2007 med uppdraget att göra säker inloggning lätt och tillgänglig för alla. Yubico har i nära samarbete med ledande aktörer och internetföretag skapat de öppna autentiseringsstandarderna FIDO U2F och FIDO2/WebAuthn. Dessa standarder har antagits i stora online-plattformar och webbläsare, vilket möjliggör bland annat tvåfaktors-, multifaktors- och lösenordsfri inloggning och ett säkrare internet för miljarder människor.

© 2020 Yubico