KnowBe4

Adgangskodepraksis og cybersårbarhed: Adgangskodevaner i Danmark og Sverige

ADGANGSKODEPRAKSIS OG CYBERSÅRBARHED: ADGANGSKODEVANER I DANMARK OG SVERIGE

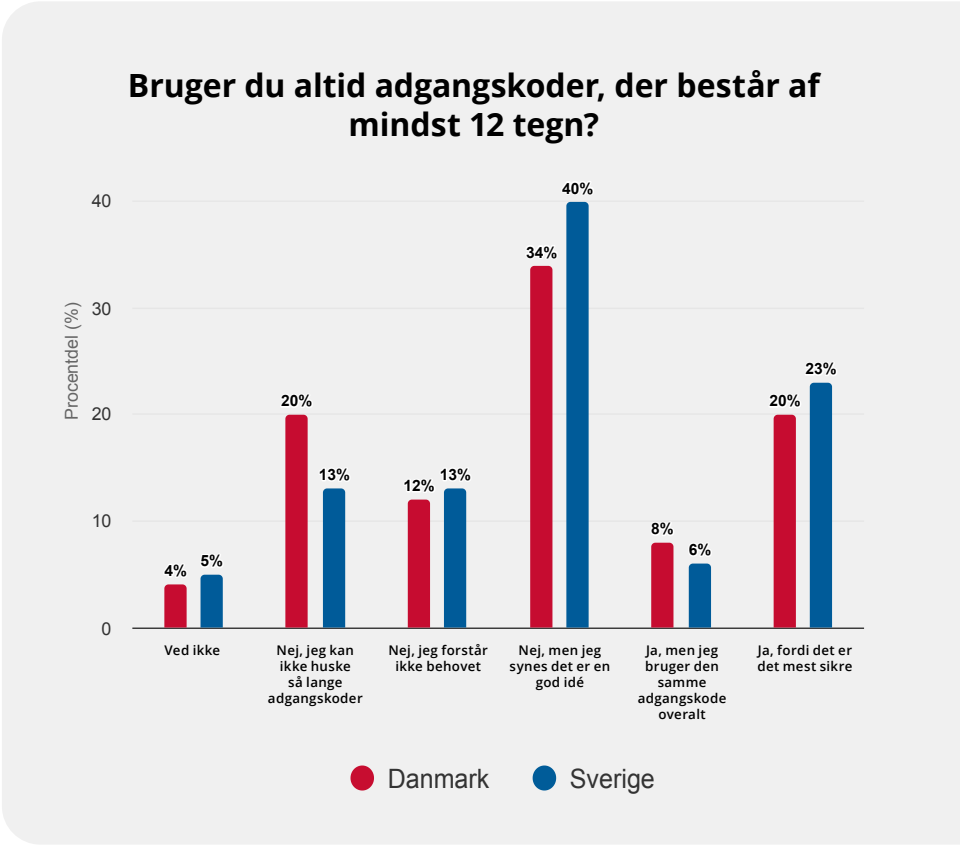
Denne rapport analyserer undersøgelsesdata om adgangskodevaner i Danmark og Sverige, indsamlet af YouGov fra 1.000 voksne i beskæftigelse på 18 år og ældre i hvert land. Undersøgelsen, der er bestilt af KnowBe4, kaster lys over forskellige aspekter og holdninger i forbindelse med adgangskodevaner og fremhæver potentielle cybersikkerhedsrisici for både enkeltpersoner og deres arbejdspladser.

Adgangskodens længde og kompleksitet

For bedre at forstå, om respondenterne er opmærksomme på styrken ved stærke adgangskoder, spurgte KnowBe4, om deres adgangskoder består af mindst 12 tegn. Næsten 20 % af respondenterne i Danmark og 13 % i Sverige svarer, at deres adgangskoder er kortere, fordi de ikke kan huske længere adgangskoder.

Mere bekymrende er de respondenter, der svarer, at de ikke forstår, hvorfor de har brug for adgangskoder på mindst 12 tegn (12 % i Danmark og 12 % i Sverige), og den lille gruppe, der svarer, at deres adgangskoder er på 12 tegn eller længere, men at de bruger den samme adgangskode overalt (8 % i Danmark og knap 6 % i Sverige). Det er dog opmuntrende, at over 20 % af de adspurgte i begge lande svarer, at deres adgangskoder altid består af mindst 12 tegn, fordi de er mest sikre.

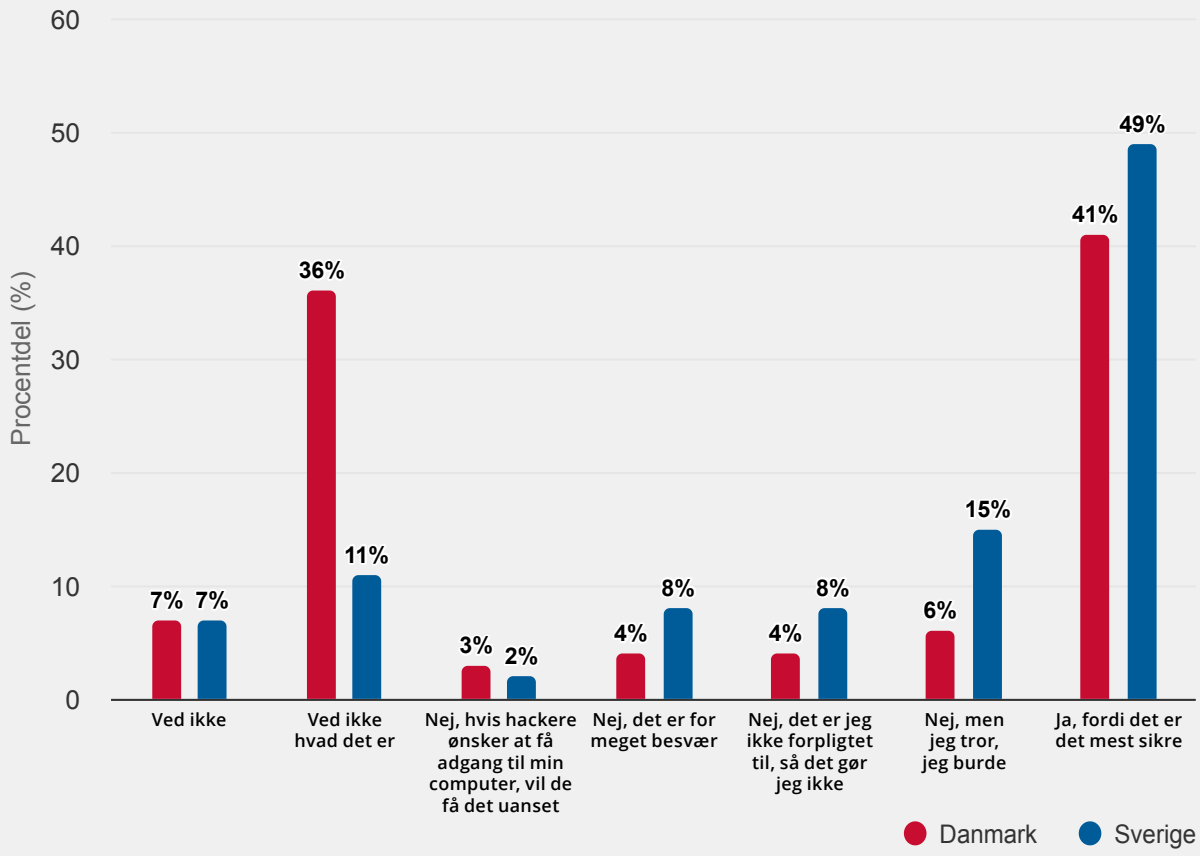
Korte eller simple adgangskoder er betydeligt nemmere for cyberkriminelle at knække, hvilket potentielt kan føre til uautoriseret adgang til både personlige- og arbejdskonti. Denne sårbarhed kan resultere i databrud, identitetstyveri og økonomiske tab for enkeltpersoner. For organisationer kan kompromitterede medarbejderkonti fungere som indgangspunkter for større angreb, hvilket potentielt kan føre til datatyveri, ransomware-angreb eller skade på omdømme.



Multifaktorgodkendelse

Multifaktorgodkendelse (MFA) er almindeligt kendt for at være en del af gode cybersikkerhedsvaner for at holde logindata og følsomme oplysninger sikre. Chokerende nok ved 36 % af de danske respondenter ikke, hvad multifaktorgodkendelse er. Til sammenligning svarer kun 11 % af de svenske respondenter det samme. Svenskerne bruger også multifaktorgodkendelse mere end danskerne, da 49 % svarer, at de bruger det, fordi det er det mest sikre, mens 41 % af danskerne svarer det samme.

Bruger du nogen form for multifaktorgodkendelse?



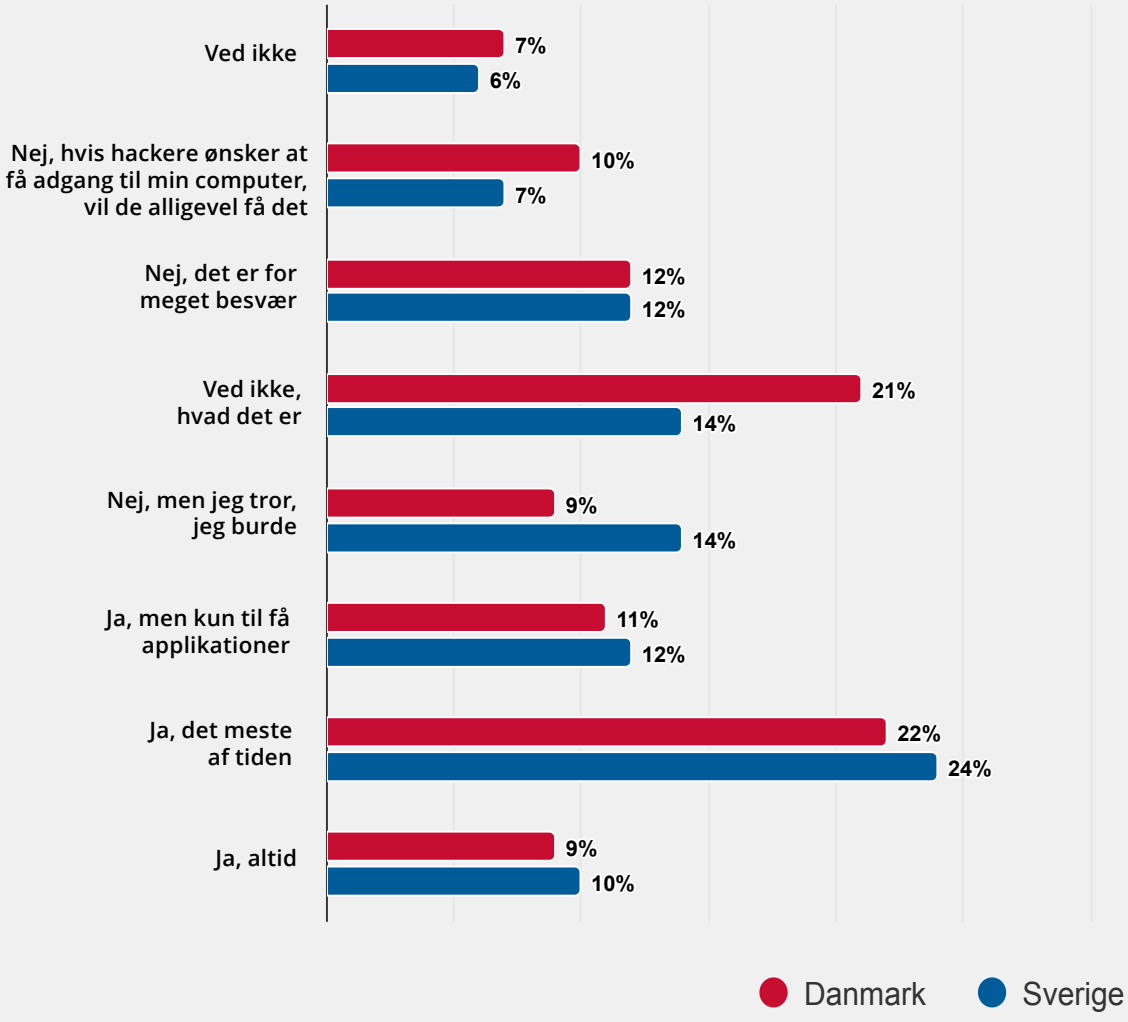
Især den manglende brug af multifaktorgodkendelse blandt danske respondenter er bekymrende. Uden denne ekstra sikkerhedsforanstaltning er konti mere sårbare over for uautoriseret adgang, når en ofte anvendt adgangskode bliver kompromitteret. For virksomheder kan dette betyde øget risiko for databrud, økonomisk svindel eller uautoriseret adgang til følsomme oplysninger.

Adgangskodeadministratorer

Adgangskodeadministratorer er ikke særligt populære i de to lande. 9 % af danskerne svarer, at de altid bruger en adgangskodeadministrator til at gemme deres adgangskoder, og 10 % af svenskerne gør det samme. Det er lovende, at adgangskodeadministratorer langsomt men sikkert bliver brugt af flere mennesker, idet 24 % af de svenske respondenter svarer, at de bruger en meste af tiden, og det samme gør 22 % af danskerne.

Begrænset anvendelse af adgangskodeadministratorer øger sandsynligheden for genbrug af adgangskoder på tværs af flere konti, da brugerne kæmper for at huske adskillige komplekse adgangskoder. Ved genbrug af den samme kode vil en enkelt kompromitteret adgangskode potentielt påvirke både personlige og arbejdsrelaterede konti. For organisationer kan dette føre til udbredte sikkerhedsbrud, hvis en medarbejders genbrugte adgangskode afsløres i en ikke-relateret datalækage.

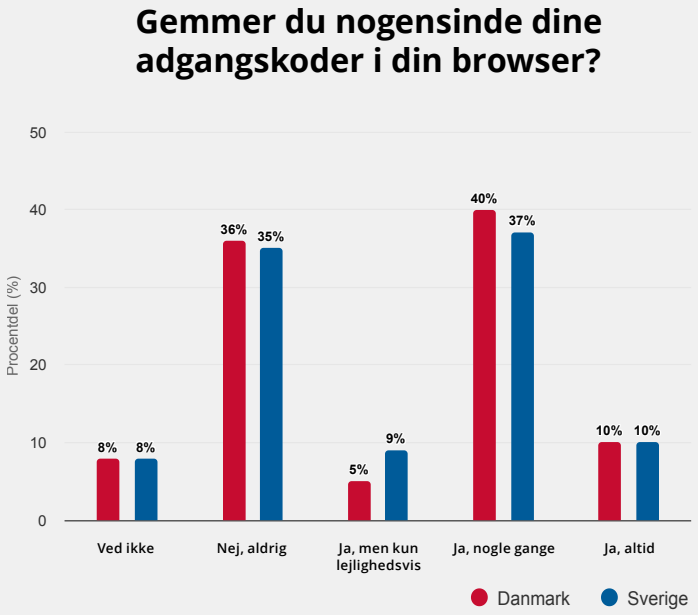
Bruger du en adgangskodeadministrator til at oprette og gemme dine adgangskoder?



Opbevaring af adgangskoder

I undersøgelsens sidste spørgsmål bliver respondenterne spurgt, om de gemmer deres adgangskoder i deres internetbrowsere. Over 35 % af både svenske og danske respondenter svarer, at de aldrig gør det, men bekymrende nok svarer over 37 %, at de gør det nogle gange.

Det kan være risikabelt at gemme adgangskoder i browsere uden yderligere sikkerhedsforanstaltninger. Hvis en enhed bliver stjålet eller kompromitteret, bliver alle gemte adgangskoder tilgængelige for angribere. Dette kan føre til tyveri af personoplysninger og



KONKLUSION OG NÆSTE SKRIDT

Undersøgelsen afslører adgangskodevaner blandt både danske og svenske respondenter og understreger, at der er plads til forbedringer på områder som adgangskodelængde, anvendelse af multifaktorgodkendelse og brugen af adgangskodeadministratorer. Uden disse sikkerhedsforanstaltninger risikerer både enkeltpersoner og deres organisationer at blive udsat for forskellige cybertrusler, herunder databrud, identitetstyveri og uautoriseret adgang til følsomme oplysninger.

For at løse disse problemer og forbedre cybersikkerhedsniveauet og reducere risikoen for adgangskoderelaterede sikkerhedshændelser i begge lande anbefaler KnowBe4 følgende:

1. **Træning i sikkerhedsbevidsthed:** Implementér omfattende træningsprogrammer om cybersikkerhed på arbejdspladser med fokus på vigtigheden af stærke adgangskodevaner.
2. **Adgangskodeadministratorer:** Tilskynd brugen af adgangskodeadministratorer for at lette oprettelsen og opbevaringen af komplekse og unikke adgangskoder til hver konto.
3. **Multifaktorgodkendelse:** Aktivér multifaktorgodkendelse ved alle arbejdsrelaterede konti og uddan medarbejderne om fordelene ved personlig brug.
4. **Adgangskodepolitikker:** Etablér klare adgangskodepolitikker på arbejdspladsen, der kræver minimumslængde og kompleksitetsstandarder.
5. **Adgangskoderevisioner:** Udfør regelmæssigt adgangskoderevisioner for at identificere svage eller genbrugte adgangskoder i arbejdspladsens systemer.
6. **Opbevaring af adgangskoder:** Sæt fokus på farerne og fraråd praksis med at gemme adgangskoder i browsere - især til arbejdsrelaterede konti.
7. **Løbende uddannelse:** Uddan løbende de ansatte om nye cybertrusler og vigtigheden af gode adgangskodevaner for at afbøde disse risici.
8. **Single Sign-On-løsninger:** Overvej at implementere Single Sign-On-løsninger i organisationer for at reducere antallet af adgangskoder, som medarbejderne skal huske, samtidig med at sikkerheden opretholdes.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E09K01