KnowBe4

Vær opmærksom på cybersikkerhedshullerne: Vurdering af sikkerheds-træning og trusselsopfattelse i Danmark og Sverige

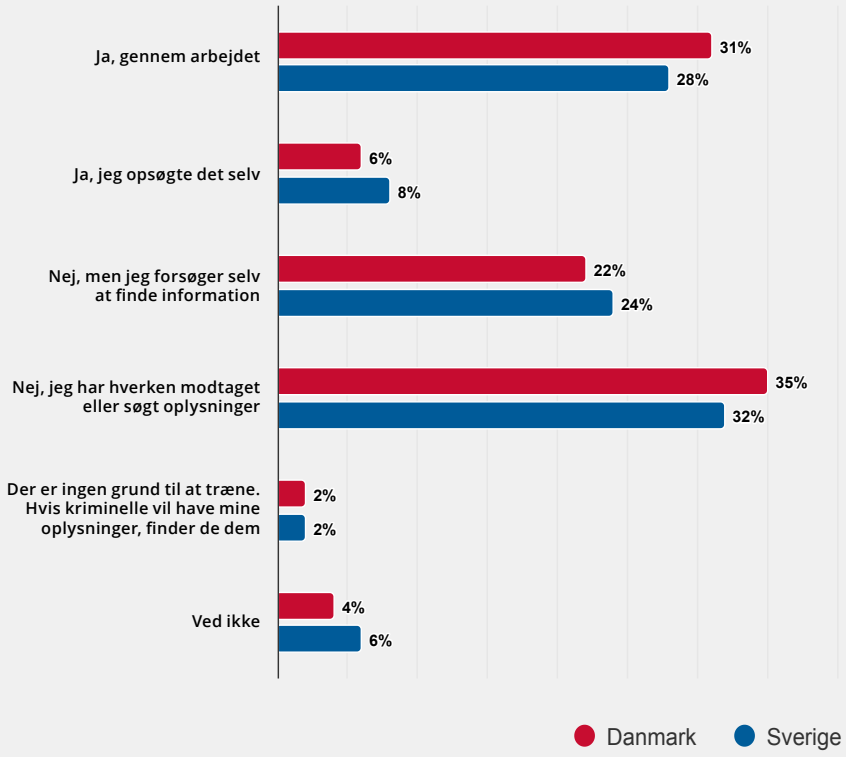
VÆR OPMÆRKSOM PÅ CYBERSIKKERHEDSHULLERNE: VURDERING AF SIKKERHEDSTRÆNING OG TRUSSELSOPFATTELSE I DANMARK OG SVERIGE

Denne rapport analyserer cybersikkerhedsbevidstheden og holdninger til cyberkriminalitet i Danmark og Sverige. En spørgeundersøgelse foretaget af YouGov sætter tal på hyppigheden af træning i sikkerhedsbevidsthed, erfaringer med cybertrusler og opfattelser af risikoen for cyberkriminalitet blandt voksne i beskæftigelse. Undersøgelsen, der er bestilt af KnowBe4, indeholder svar fra 1.000 deltagere på 18 år og ældre i hvert land, hvilket giver værdifuld indsigt i det nuværende cybersikkerhedslandskab i de to lande.

Træning i sikkerhedsbevidsthed

For bedre at forstå respondenternes bevidsthedsniveauer om cybersikkerhed spurgte KnowBe4, om de modtager cybersikkerhedstræning på deres arbejdsplads. Hele 69 % af respondenterne i Danmark og 72 % i Sverige modtager ingen cybersikkerhedstræning på arbejdspladsen. 22 procent af danskerne og 24 procent af svenskerne, der ikke modtager træning på arbejdspladsen, søger dog information online for at uddanne sig i cybersikkerhed og for at føle sig mere sikre. Det er imidlertid bekymrende, at over 30 % af respondenterne i begge lande ikke selvuddanner sig eller modtager uddannelse fra deres arbejdsgivere.

Har du nogensinde modtaget træning i sikkerhedsbevidsthed for at modvirke cyberkriminalitet?



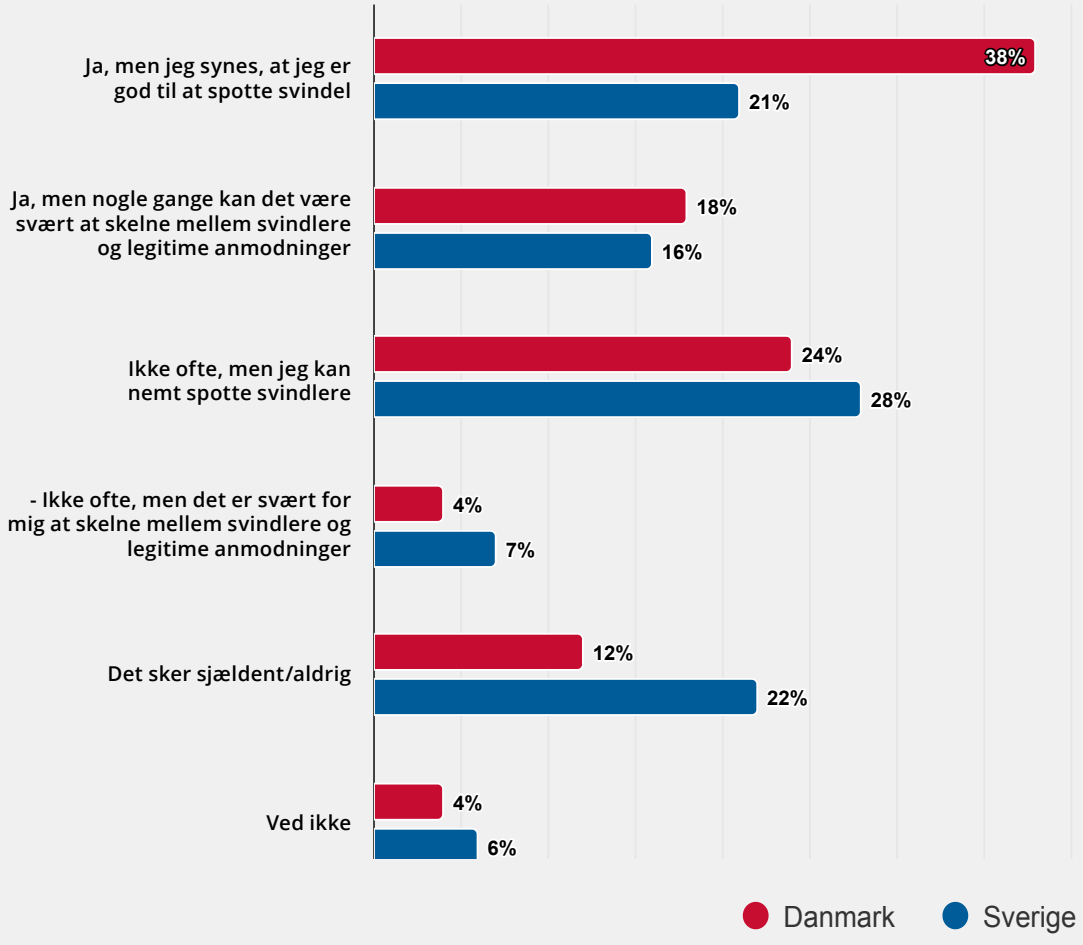
Den høje procentdel af ansatte, der ikke modtager cybersikkerhedstræning, er bekymrende set i lyset af de stigende antal og hyppigheden af mere og mere sofistikerede cyberangreb. Manglen på formel uddannelse kan potentielt gøre en betydelig del af arbejdsstyrken og dermed deres arbejdspladser sårbare over for forskellige cybertrusler.

Erfaring med cybertrusler

På spørgsmålet om, hvorvidt respondenterne oplever cybertrusler såsom phishing-e-mails, phishing-sms'er, uønskede beskeder og falske følgere eller venneanmodninger på sociale medier, er der en væsentlig forskel mellem landene. Næsten 40 % af danskerne og 21 % af svenskerne svarer, at de ofte oplever forsøg på cyberkriminalitet, men at de også føler, at de ret nemt kan spotte svindlerne. Yderligere 28 % og 16 % af respondenterne i henholdsvis Danmark og Sverige svarer, at de oplever dette ofte, og at det er svært for dem at skelne mellem svindlere og legitime anmodninger, hvilket gør dem mere sårbare over for at blive ofre for cyberkriminalitet.

Variationen i erfaringer med cybertrusler mellem Danmark og Sverige er bemærkelsesværdig og giver anledning til yderligere undersøgelse. Det kan tilskrives forskelle i de cyberkriminelles målretning, variationer i internetbrugsmønstre eller en forskel i bevidsthedsniveauer mellem de to lande.

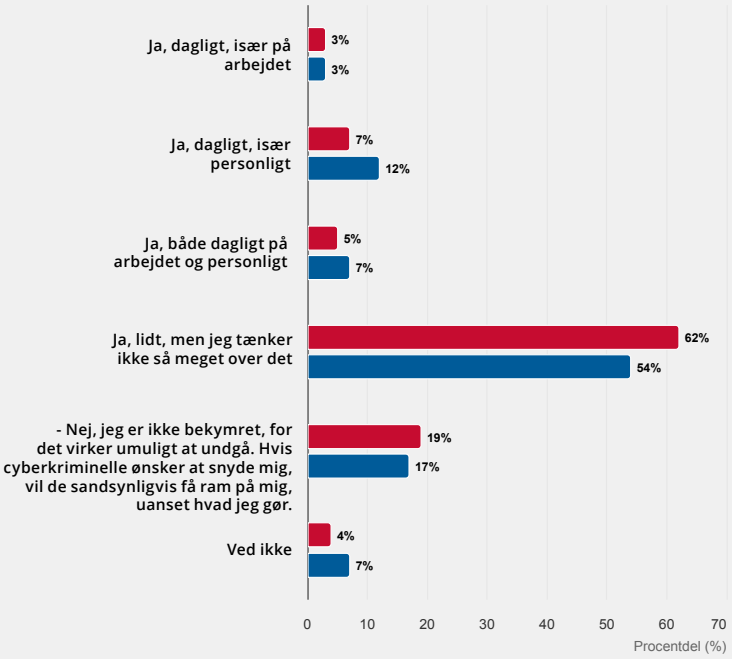
Oplever du ofte forsøg på cyberkriminalitet såsom phishing-e-mails, phishing-sms'er, følgere/venneanmodninger eller beskeder fra falske profiler på sociale medier eller lignende?



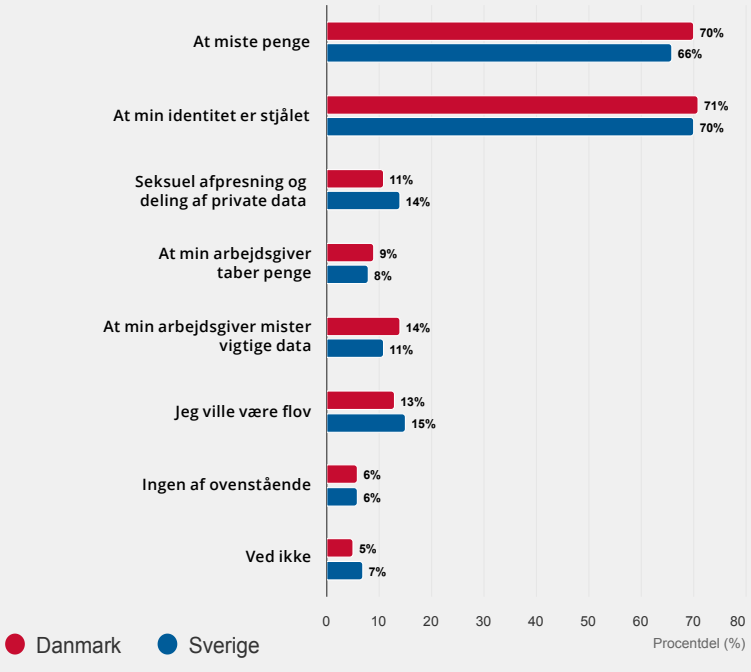
Holdninger til cyberkriminalitet

Manglen på træning bliver mere tydelig, når man spørger, om respondenterne er bange for at blive ofre for cyberkriminalitet. En stor del af respondenterne (62 % i Danmark og 54 % i Sverige) svarer, at de ikke er så bekymrede, da de ikke rigtig tænker over det. Denne tilgang er bekymrende, da den gør dem mere modtagelige for cybertrusler.

Er du bange for at blive offer for cyberkriminalitet?



Hvad frygter du ved at blive offer for cyberkriminalitet?



Kun 10 % og 15 % af de adspurgte i de to lande nævner, at det er en daglig bekymring for dem, mens 19 % af danskerne og 17 % af svenskerne slet ikke er bekymrede, fordi de tror, at hvis cyberkriminelle vil snyde dem, så finder de en måde at gøre det på. Når det kommer til at blive ramt af cyberkriminalitet, er den primære frygt i både Danmark og Sverige at miste penge og at blive offer for identitetstyveri.

Det relativt lave niveau af bekymring for cyberkriminalitet blandt respondenterne i begge lande er alarmerende. Denne selvtilfredshed kan føre til mindre årvågenhed og øget sårbarhed over for cyberangreb. Det faktum, at en betydelig del af respondenterne mener, at de ikke kan forhindre eller afværge ihærdige angreb fra cyberkriminelle, tyder på et behov for uddannelse i effektiviteten af korrekte cybersikkerhedsforanstaltninger.

KONKLUSION OG NÆSTE SKRIDT

Undersøgelsens resultater understreger betydelige huller i cybersikkerhedsbevidstheden og -træningen i både Danmark og Sverige. For at løse disse problemer og forbedre den overordnede cybersikkerhedsindstilling i disse lande anbefaler KnowBe4 følgende:

1. **Træning i sikkerhedsbevidsthed:** Arbejdspladser skal begynde at implementere obligatoriske træningsprogrammer for sikkerhedsbevidsthed i begge lande for at afhjælpe den betydelige mangel på formel uddannelse.

2. **Målrettede kampagner:** Udvikle målrettede oplysningskampagner for at fremhæve vigtigheden af cybersikkerhed og de potentielle risici ved selvtilfredshed hos både ansatte og arbejdsgivere – særligt set i lyset af den høje procentdel af respondenter, der ikke bekymrer sig om cyberkriminalitet.

3. **Fleksible træningsmuligheder:** Tilbyd forskellige træningsformater for at imødekomme individuelle læringspræferencer.

4. **Skræddersyet træning:** Skræddersy cybersikkerhedsuddannelse til at imødegå specifik frygt såsom økonomisk tab og identitetstyveri og skab fokus på konkrete og håndgribelige måder at afbøde disse risici.

5. **Forenkle sikkerhedsprocedurer:** Sikkerhedsprotokoller skal være brugervenlige for at reducere manglende overholdelse på grund af kompleksitet.

6. **Phishing-simuleringer:** Hyppige phishing-simuleringer og andre praktiske øvelser vil hjælpe medarbejderne med at blive bedre til at identificere og reagere på cybertrusler.

7. **Regelmæssige genopfriskningskurser:** Giv hyppigere, korte kurser og simuleret phishing for at styrke bedste praksis og opretholde sikkerhedsbevidstheden.

8. **Fremme positiv sikkerhedskultur:** Gør træningen til en engagerende og relevant oplevelse med afkrydsningsøvelser.

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