KnowBe4

Var uppmärksam på cybersäkerhetsklyftan: Utvärdering av säkerhets-utbildning och uppfattning om hotbild i Sverige och Danmark

VAR UPPMÄRKSAM PÅ CYBERSÄKERHETSKLYFTAN: UTVÄRDERING AV SÄKERHETSUTBILDNING OCH UPPFATTNING OM HOTBILD I SVERIGE OCH DANMARK

Denna rapport analyserar läget för cybersäkerhetsmedvetenhet och attityder till cyberbrottslighet i Sverige och Danmark. Den är baserad på undersökningsdata som samlats in av YouGov och utforskar frekvensen av utbildning i säkerhetsmedvetenhet, erfarenheter av cyberhot och uppfattningar om risker för cyberbrott bland anställda vuxna. Studien har beställts av KnowBe4 och innehåller svar från 1 000 deltagare i åldern 18 år och äldre i varje land, vilket ger värdefulla insikter om det nuvarande cybersäkerhetslandskapet i dessa länder.

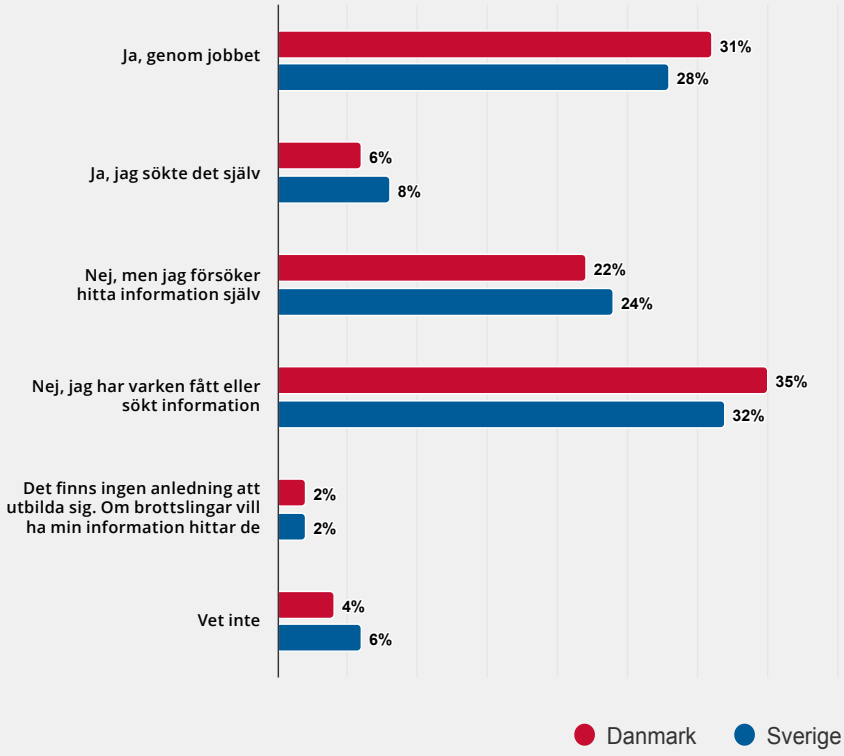
Utbildning i säkerhetsmedvetenhet

För att bättre förstå hur medvetna de tillfrågade är om cybersäkerhet frågade KnowBe4 om de får cybersäkerhetsutbildning i sina organisationer.

Hela 72 % av de tillfrågade i Sverige och 69 % i Danmark får ingen cybersäkerhetsutbildning på jobbet.

24 % av svenskarna och 22 % av danskarna som inte får utbildning på jobbet söker dock själva efter information för att utbilda sig om cybersäkerhet och hur man skyddar sig nätet. Det är dock oroande att över 30 % av de tillfrågade i båda länderna inte utbildar sig själva eller får utbildning av sina arbetsgivare.

Har du någonsin fått utbildning för att bättre rusta dig mot cyberbrottslighet?



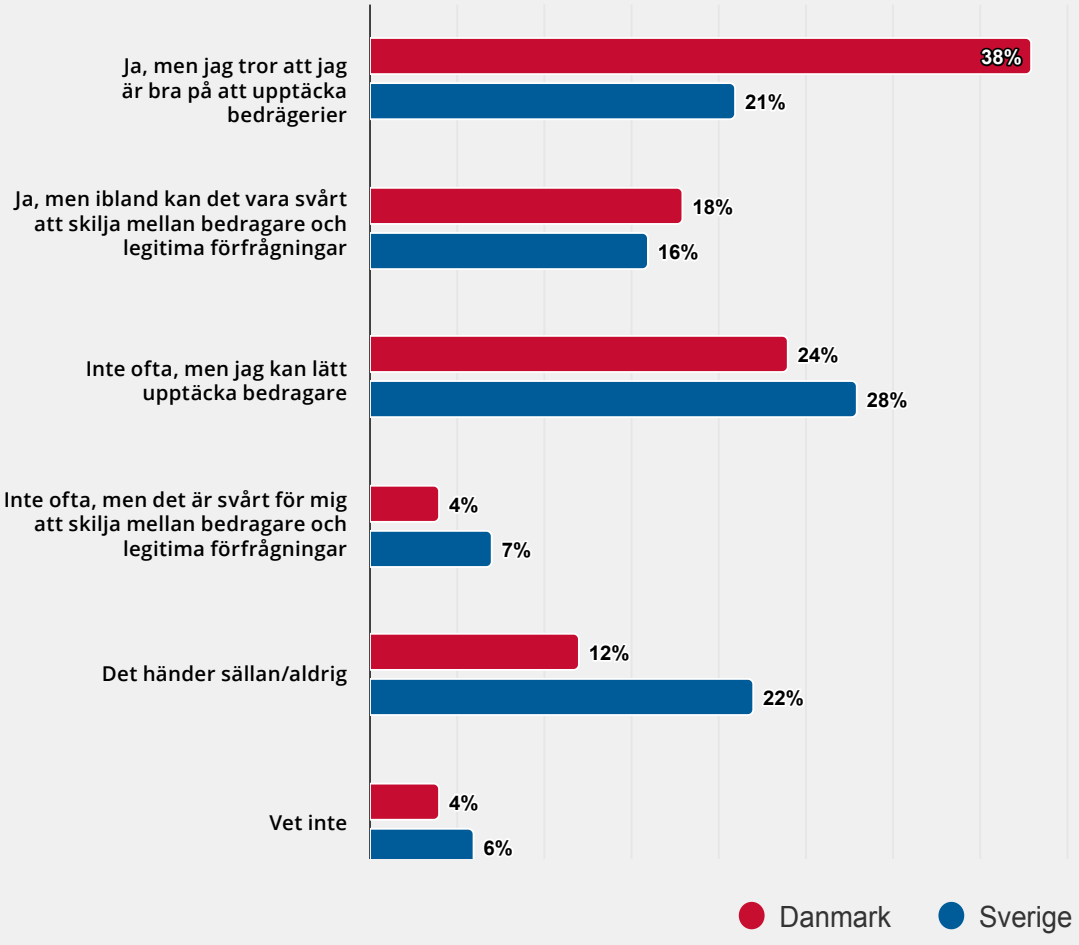
Den höga andelen anställda som inte får utbildning i cybersäkerhet är oroande med tanke på att cyberattackerna blir alltmer sofistikerade och frekventa. Bristen på formell utbildning kan potentiellt leda till att en betydande del av arbetsstyrkan och därmed organisationen blir sårbar för olika cyberhot.

Erfarenhet av cyberhot

På frågan om de svarande upplevt cyberhot som nätfiske-e-post, nätfiske-SMS, oönskade meddelanden och falska följare eller vänförfrågningar på sociala medier, var det en betydande skillnad mellan länderna. Nästan 21 % av svenskarna och 40 % av danskarna svarade att de ofta utsätts för försök till cyberbrottslighet, men att de också känner att de kan upptäcka bedragarna ganska lätt. Ytterligare 16 % respektive och 28 % av de tillfrågade i Sverige och Danmark uppgav att de upplever detta ofta och att det är svårt för dem att skilja mellan bedragare och legitima förfrågningar, vilket gör dem mer sårbara för att falla offer för cyberbrottslighet.

Skillnaden i erfarenheter av cyberhot mellan Danmark och Sverige är anmärkningsvärd och bör undersökas ytterligare. Det kan bero på skillnader i hur cyberbrottslingar riktar in sig, variationer i internetanvändningsmönster eller en skillnad i medvetenhetsnivå mellan de två länderna.

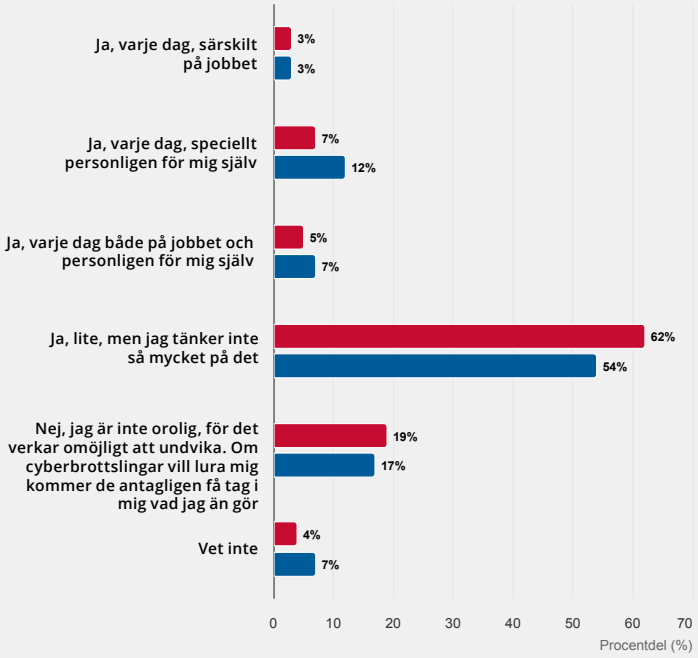
Upplever du ofta försök till cyberbrottslighet såsom nätfiskemejl, nätfiske-SMS, följare/vänförfrågningar eller meddelanden från falska profiler på sociala medier eller liknande?



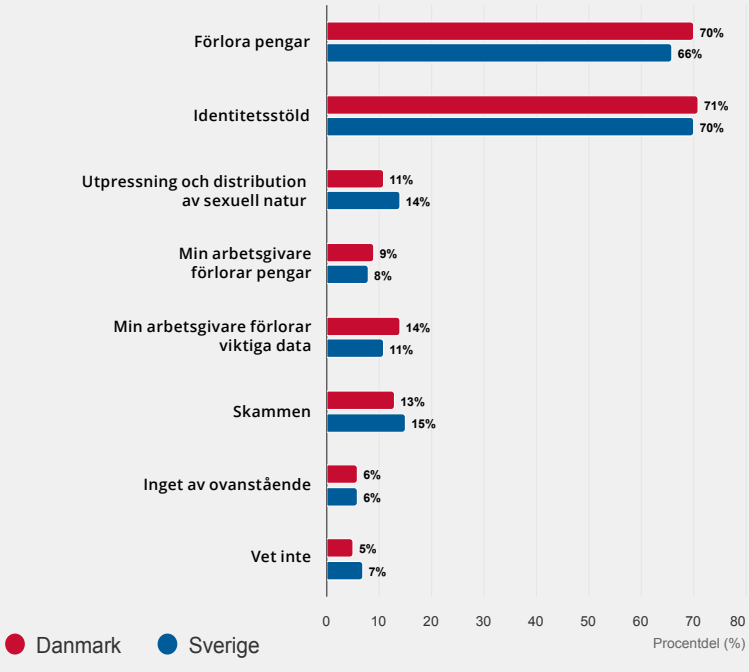
Attityd till cyberbrottslighet

Bristen på utbildning blir mer uppenbar när man frågar om de svarande oroar sig för att bli utsatta för cyberbrott. En stor del av de tillfrågade (54 % i Sverige och 62 % i Danmark) svarade att de inte är så oroliga eftersom de inte riktigt tänker på det. Detta förhållningssätt är oroande eftersom det gör dem mer mottagliga för cyberhot.

Är du rädd för att bli offer för cyberbrottslighet?



Vad är du rädd för om du blir offer för cyberbrottslighet?



Bara 15 % och 10 % av de tillfrågade i respektive länder uppger att det är ett dagligt bekymmer för dem, medan 17 % av svenskarna och 19 % av danskarna inte är oroliga alls eftersom de tror att om cyberbrottslingar vill lura dem, kommer de ändå att hitta på ett sätt. De främsta farhågorna i båda länderna är identitetsstöld och att förlora pengar.

Den relativt låga nivån av oro för cyberbrottslighet bland de tillfrågade i båda länderna är oroväckande. Denna likgiltighet kan leda till sämre vaksamhet och ökad sårbarhet för cyberattacker. Att en betydande del av de tillfrågade anser att de inte kan förhindra beslutsamma cyberbrottslingar tyder på ett behov av utbildning om effektiviteten av korrekta cybersäkerhetsåtgärder.

SLUTSATS OCH NÄSTA STEG

Undersökningsresultaten visar att det finns betydande brister i medvetenheten om och utbildningen i cybersäkerhet i både Sverige och Danmark. För att ta itu med dessa problem och förbättra den övergripande cybersäkerheten i dessa länder rekommenderar KnowBe4 följande:

1. **Utbildning i säkerhetsmedvetenhet:** Organisationer måste börja implementera obligatoriska utbildningsprogram för säkerhetsmedvetenhet i båda länderna för att ta itu med den betydande bristen på formell utbildning.

2. **Riktade kampanjer:** Utveckla riktade informationskampanjer för att belysa vikten av cybersäkerhet och de potentiella riskerna med likgiltighet personligen och för arbetsgivare, särskilt med tanke på den höga andelen respondenter som inte oroar sig för cyberbrottslighet.

3. **Flexibla utbildningsalternativ:** Erbjud olika utbildningsformat för att tillgodose olika inlärningspreferenser.

4. **Skräddarsydd utbildning:** Skräddarsy cybersäkerhetsutbildning för att ta itu med specifika rädslor som ekonomisk förlust och identitetsstöld, och ge konkreta åtgärder för att minska dessa risker.

5. **Förenkla säkerhetsprocedurerna:** Se till att säkerhetsprotokoll är användarvänliga för att minska bristande efterlevnad på grund av komplexitet.

6. **Nätfiskesimuleringar:** Genom att utföra frekventa nätfiskesimuleringar och andra praktiska övningar kommer anställda att bättre kunna identifiera och reagera på cyberhot.

7. **Regelbundna repetitionskurser:** Erbjud mer frekvent, småskalig träning och simulerat nätfiske för att förstärka bästa praxis och hålla säkerheten i fokus

8. **Främja positiv säkerhetskultur:** Motverka uppfattningen att utbildningen bara är en övning där man sätter kryss i rutor genom att göra den engagerande och relevant.

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