



JÖNKÖPING UNIVERSITY
School of Engineering

Research Report

Identifiering av behov och uppfattningar kring cybersäkerhetsmedvetenhet hos olika användargrupper (ICANP)

Identifying Cybersecurity Awareness Needs
and Perceptions of user groups
(ICANP)

Joakim Kävrestad

Jönköping University
School of Engineering
Research Reports No. 11 • 2026



JÖNKÖPING UNIVERSITY
School of Engineering

Research Report

Identifiering av behov och uppfattningar kring cybersäkerhetsmedvetenhet hos olika användargrupper (ICANP)

Identifying Cybersecurity Awareness Needs
and Perceptions of user groups
(ICANP)

Joakim Kävrestad

Identifiering av behov och uppfattningar kring
cybersäkerhetsmedvetenhet hos olika användargrupper (ICANP)
Identifying Cybersecurity Awareness Needs and Perceptions of user
groups (ICANP)

Research Reports No. 11

© 2026 Joakim Kävrestad

Published by
School of Engineering, Jönköping University
P.O. Box 1026
SE-551 11 Jönköping
Tel. +46 36 10 10 00
www.ju.se

ISSN 1404-0018

Identifiering av behov och uppfattningar kring cybersäkerhetsmedvetenhet hos olika användargrupper (ICANP)

Identifying Cybersecurity Awareness Needs and Perceptions of user groups (ICANP)

Finansierat av Myndigheten för Samhällsskydd och Beredskap (MSB), projektnummer MSB-2024-03121.

Funded by the Swedish Civil Contingencies Agency, project number MSB-2024-03121.

Författare/Author:

Joakim Kävrestad: joakim.kavrestad@ju.se

Projektet har genomförts med stöd av:

The project has been supported by:

Erik Bergström, Jönköping School of Engineering

Nathan Clarke, University of Plymouth

Per Lagerström, Junglemap



JÖNKÖPING UNIVERSITY
School of Engineering

19 februari 2026

Sammanfattning

Denna rapport sammanfattar resultaten från projektet ICANP, som undersöker hur cybersäkerhetsmedvetenheten i Sverige kan stärkas genom att bättre anpassa information och utbildning till olika grupper i befolkningen. Den första delstudien visar att EU-länders nationella strategier lyfter medvetenhet som ett viktigt mål, men att de sällan erbjuder konkreta metoder för målgruppsanpassning. Den andra delstudien, en enkät med 2 049 personer, visar att faktorer som ålder, IT-kompetens och utbildningsnivå påverkar hur människor vill ta del av cybersäkerhetsinformation. Generella preferenser framträder också: kortfattad, enkel och situationsanpassad information föredras, och trovärdiga avsändare som särskilt myndigheter och tjänsteleverantörer värderas högt. Den tredje delstudien, baserad på intervjuer, bekräftar dessa mönster och visar att relevans, enkelhet och upplevd nytta är centrala för att människor ska ta till sig information om cybersäkerhet. Projektet drar slutsatsen att nationella program bör kombinera breda, generella insatser med riktade åtgärder mot grupper med särskilda behov och att livssituation, exempelvis familjeliv och livsfas, ofta är en viktigare utgångspunkt än traditionella demografiska kategorier att anpassa efter. Rapporten är skriven på svenska och innehåller en engelsk översättning skapad med Generativ AI.

Abstract

This report summarises the results of the ICANP project, which examines how cybersecurity awareness in Sweden can be strengthened by better tailoring information and training to different groups within the population. The first sub-study shows that the national strategies of EU countries highlight awareness as an important objective, but they rarely offer concrete methods for adapting initiatives to specific target groups. The second sub-study, a survey of 2,049 participants, shows that factors such as age, IT competence, and educational background influence how people prefer to receive cybersecurity information. General preferences also emerge: brief, simple, and context-based information is preferred, and credible senders such as public authorities and service providers are highly valued. The third sub-study, based on interviews, confirms these patterns and shows that relevance, simplicity, and perceived usefulness are central for individuals to engage with cybersecurity information. The project concludes that national programmes should combine broad, general initiatives with targeted efforts aimed at groups with specific needs, and that life situation is often a more meaningful basis for adaptation than traditional demographic categories. The report is written in Swedish and includes an English translation created with Generative AI.

Innehållsförteckning/Table of contents

1	Inledning	1
1.1	Cybersäkerhetsmedvetenhet för privatpersoner	1
1.2	Projekt mål och delstudier	3
2	Delstudier och resultat	4
2.1	Kartläggning av nationella program inom EU	4
2.1.1	Analys av nationella cybersäkerhetsstrategier inom EU	4
2.1.2	Översikt av relevant forskning	5
2.1.3	Slutsats delstudie 1	9
2.2	Identifiering av målgrupper	9
2.2.1	Sammanfattning delstudie 2	10
2.2.2	Delstudiens genomförande	11
2.2.3	Resultat delstudie 2	12
2.2.4	Analys av delstudie 2	13
2.3	Ökad förståelse för behov och preferenser	15
2.3.1	Sammanfattning delstudie 3	15
2.3.2	Delstudiens genomförande	16
2.3.3	Resultat delstudie 3	16
3	Diskussion och slutsatser	20
3.1	Huvudsakliga insikter	20
3.2	Råd vid utformning av nationella cybersäkerhetsprogram	21
4	ENGLISH Introduction	23
4.1	Cybersecurity awareness for private individuals	23
4.2	Project goals and sub-studies	25
5	Sub-studies and Results	26
5.1	Mapping of National Programmes within the EU	26
5.1.1	Analysis of National Cybersecurity Strategies within the EU	26
5.1.2	Overview of Relevant Research	27
5.1.3	Conclusion of Sub-study 1	31
5.2	Identifying Target Groups	31
5.2.1	Summary of Sub-study 2	32
5.2.2	Study Method	33
5.2.3	Results of Sub-study 2	34
5.2.4	Analysis of Sub-study 2	35

- 5.3 Increased Understanding of Needs and Preferences 37
 - 5.3.1 Summary of Sub-study 3 37
 - 5.3.2 Study Methodology 37
 - 5.3.3 Results of Sub-study 3 38

- 6 Discussion and Conclusions 41**
 - 6.1 Main Insights 41
 - 6.2 Recommendations for Designing National Cybersecurity Programmes 42

- 7 Appendix A - Tabeller 46**

- 8 Appendix B - Tables 51**

1 Inledning

När samhället blir allt mer digitalt ökar också risken för att vi utsätts för cyberattacker. Sverige hör till världens mest tekniskt utvecklade länder, vilket ger stora fördelar men även gör oss extra sårbara. För att stärka den nationella motståndskraften behöver alla som använder digitala tjänster, inte bara experter, förstå hur de kan skydda sig. Projektet ICANP har undersökt vilka behov olika grupper i samhället har när det gäller cybersäkerhet, och hur de själva helst vill få information och utbildning om cybersäkerhet. Detta görs för att kunna bidra till att förbättra hur cybersäkerhet kommuniceras i samhället. För att förenkla för läsaren är rapporten skriven så att projektets viktigaste resultat presenteras först, och metod och diskussion därefter. Därför förekommer vissa upprepningar i rapporten. För den som enbart vill ta del av projektets huvudsakliga resultat rekommenderas att först läsa kapitel 1.2 och därefter kapitel 3.

1.1 Cybersäkerhetsmedvetenhet för privatpersoner

Sveriges höga grad av digitalisering lyfts fram av både EU-kommissionen och OECD [6, 20]. Vi använder digital teknik till allt från bankärenden och shopping till myndighetskontakt och social interaktion. Samtidigt beskriver Nationellt cybersäkerhetscenter (NCSC) hur hotnivån har ökat, inte minst efter Rysslands invasion av Ukraina, som lett till en mer instabil geopolitisk situation [17]. Cyberhoten är dessutom varierade och omfattar bland annat:

- Bedrägerier som phishing, vishing och smishing [14].
- Desinformation med målet att destabilisera samhället [3].
- Ransomware, skadlig kod och attacker mot leveranskedjor.
- Cyberbrott riktade mot både individer och företag.

Gemensamt för cyberattacker är att de ofta riktar sig mot människors beteenden snarare än mot tekniska brister [8]. Branschrapporter visar att minst 75 % av lyckade cyberattacker involverar utnyttjande av mänskligt beteende [7, 18]. Det kan handla om att någon klickar på en skadlig länk, använder svaga lösenord eller luras att lämna ut känslig information [15].

För att minska dessa risker krävs inte bara tekniska skydd – människor behöver också ha kunskap, förståelse och färdigheter för att agera säkert [4, 12]. Därför är olika former av cybersäkerhetsutbildningar och medvetenhetshöjande insatser centrala.

De flesta får idag cybersäkerhetsutbildning via arbetsplatsen, där utbildningen fokuserar på policys och rutiner som är relevanta för arbetsgivaren [5]. Att låta arbetsgivare ansvara för cybersäkerhetsutbildning medför, på nationell nivå, tre problem:

- Utbildningen når inte alla. Många grupper, exempelvis pensionärer, studenter, nyanlända eller personer utanför arbetsmarknaden, får ingen strukturerad utbildning alls.
- Innehållet är ofta snävt såtillvida som det baseras på arbetsgivarens och inte nationens eller individens behov. Samhällsövergripande ämnen som desinformation, privat cyberhygien och förebyggande av bedrägerier är sällan inkluderade. Forskning pekar dessutom på att många organisationers insatser inte är tillräckligt effektiva [10].
- Nationella kampanjer måste fungera på en helt annan skala. Man kan inte samla miljontals människor i klassrum eller skicka riktad utbildning till alla. Därför behöver nationella program utformas på ett sätt som både skalar och fungerar för många olika typer av människor.

Det är välkänt i forskningen att personer med olika bakgrunder kan behöva olika typer av stöd. Vilka bakgrundsfaktorer som är viktigast är inte klarlagt, men kan inkludera:

- Demografi: ålder, kön och socioekonomi kan påverka hur man lär sig och uppfattar risk [13].
- Tillitsfrågor: människor tar till sig information olika beroende på vem som är avsändaren [9].
- Språk och teknisk nivå: alltför avancerat språk eller tekniska termer gör att vissa grupper inte kan tillgodogöra sig viktig information [16].

Problemet är att det finns för lite empirisk forskning om hur olika grupper faktiskt betar sig, lär sig och engagerar sig i cybersäkerhet [19]. Nationella initiativ, såsom MSB:s årliga kampanj Tänk Säkert, är viktiga steg på vägen. Men forskning visar att dagens kampanjer inte är så effektiva som de skulle kunna vara [19, 2]. En av de främsta orsakerna är att de inte tar tillräcklig hänsyn till skillnader mellan målgrupper där olika grupper:

- har olika digitala förmågor,

- använder internet på olika sätt,
- utsätts för olika typer av risker,
- litar på olika avsändare, och
- föredrar olika format.

Utan förståelse för dessa skillnader är det svårt att utveckla kampanjer som verkligen gör skillnad. Det är denna kunskapslucka ICANP adresserar.

1.2 Projektmål och delstudier

Projektets mål är att identifiera behov och preferenser hos olika målgrupper för nationella cybersäkerhetsprogram. Detta görs genom tre delstudier:

- Kartläggning av hur nationella program i EU utformas.
- Enkätundersökning med 2049 svenskar för att identifiera målgrupper.
- Intervjuer med representanter från dessa grupper för att förstå deras behov och preferenser.

Resultaten av delstudierna har legat till grund för rekommendationer om hur nationella utbildningsinitiativ kan riktas och utformas för att maximera effekten. Resterande del av denna rapport presenterar de tre delstudierna och de huvudsakliga resultaten av dessa. För den som vill fördjupa sig i detaljerna kring respektive studie kommer ett flertal vetenskapliga artiklar att publiceras. Merparten av dessa är ännu inte publicerade, men intresserade läsare kan få tillgång genom att kontakta rapportens författare.

2 Delstudier och resultat

I detta kapitel presenteras projektets delstudier i kronologisk ordning.

2.1 Kartläggning av nationella program inom EU

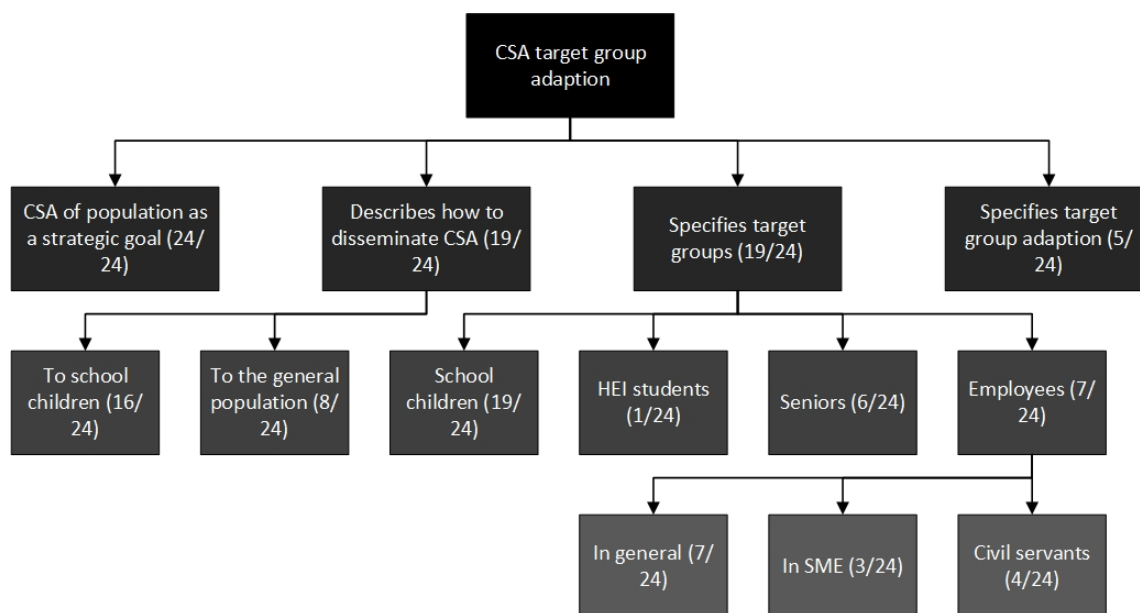
Den första delstudien analyserar hur EU:s medlemsländer adresserar cybersäkerhetsmedvetenhet (CSA) i sina nationella cybersäkerhetsstrategier (NCSS), samt hur dessa strategier förhåller sig till aktuell forskning om målgruppsanpassning av medvetandehöjande åtgärder. Resultaten visar att det finns en stark enighet om medvetenhetens betydelse, men att konkreta metoder för anpassning av medvetandehöjande åtgärder i hög grad saknas. Delstudien är publicerad i en vetenskaplig artikel där fullständiga detaljer om forskningsmetodik återges [11].

2.1.1 Analys av nationella cybersäkerhetsstrategier inom EU

Delstudien inleddes med en analys av strategier och prioriteringar i EUs medlemsländer, med utgångspunkt i medlemsländernas nationella cybersäkerhetsstrategier (NCSS). Analysen inkluderande NCSS från 24 EU-länder och visar att samtliga inkluderade länder lyfter cybersäkerhetsmedvetenhet som ett strategiskt mål. Studiens resultat presenteras i Figur 1, som en tematisk översikt över innehållet i strategierna.

Utöver att strategierna lyfter CSA som ett strategiskt mål identifierades följande tre huvudteman under analysen:

- Metoder för att sprida CSA: I 19 av strategierna beskrivs hur utbildningsinsatser ska distribueras. Det vanligaste tillvägagångssättet är att inkludera cybersäkerhet i skolverksamheten. Detta motiveras dels genom att barn betraktas som en sårbar grupp, dels genom att digitalt kunnande anses nödvändigt i det moderna samhället. Andra metoder inkluderar digitala utbildningsplattformar för den breda allmänheten.
- Identifierade målgrupper: 19 NCSS anger uttryckliga eller implicita målgrupper för cybersäkerhetsinsatser. Vanligast förekommande är barn och unga, följt av äldre, anställda och specifika yrkesgrupper såsom chefer inom små och medelstora företag (SMF). Motiven varierar: barn och äldre lyfts främst som utsatta grupper, medan vissa delar av arbetskraften lyfts på grund av sitt strategiska ansvar eller sin strukturella sårbarhet.



Figur 1: Översikt av nationella strategier

- Målgruppsanpassning: Endast fem strategier diskuterar hur utbildning bör anpassas efter målgruppen. Strategierna är övergripande och saknar specifika riktlinjer. Generellt så beskriver strategierna att målgruppsanpassning behöver göras men inte hur.

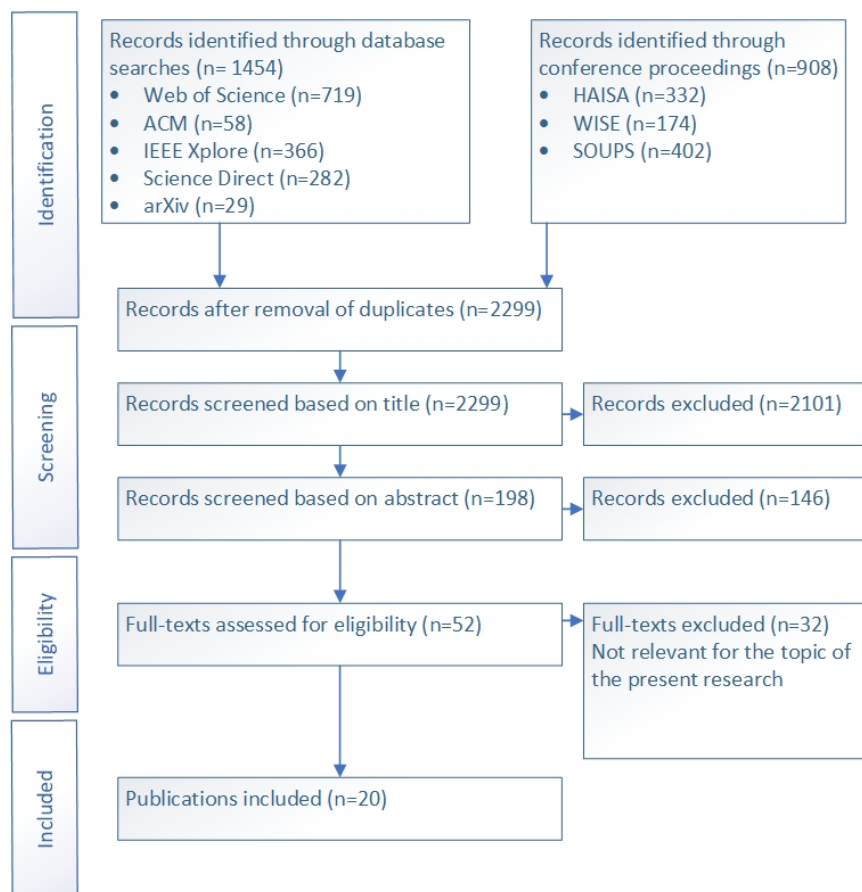
2.1.2 Översikt av relevant forskning

Forskningsöversikten baseras på en genomgång av 20 vetenskapliga studier. Dessa studier identifierades genom en sökprocess som inkluderade vetenskapliga databaser och konferenser och återges i Figur 2. Sökningen identifierade initialt över 2 000 studier som successivt filtrerades ned till 20 inkluderade studier.

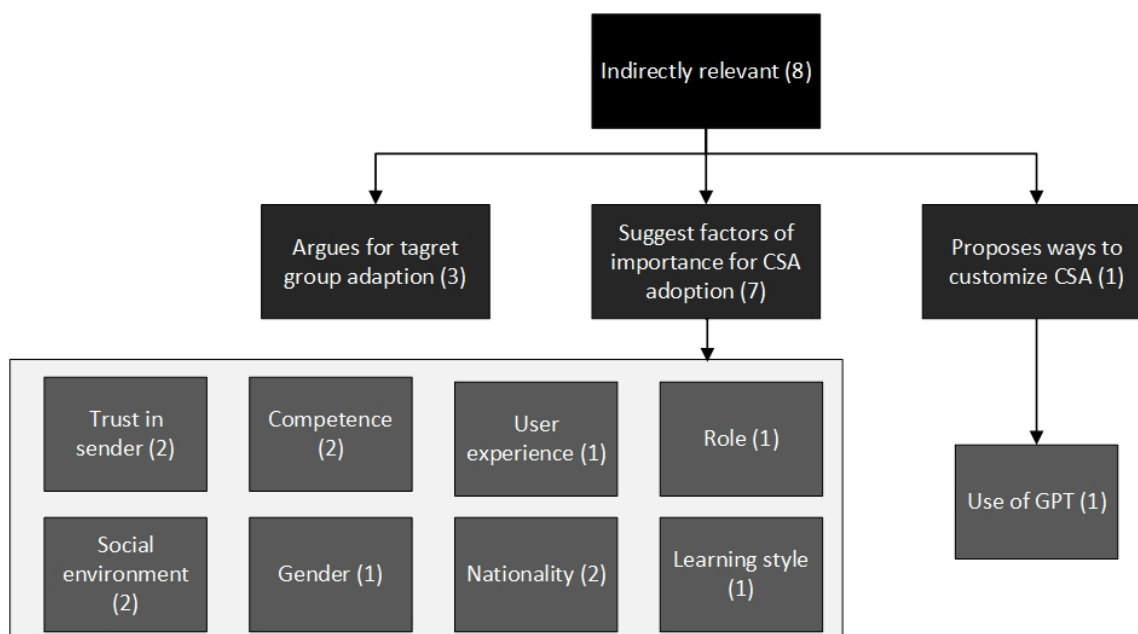
Studierna kategoriserades som indirekt eller direkt relevanta för nationella cybersäkerhetsinsatser, vilket visas i Figur 3 respektive Figur 4. direkt relevanta studier är studier som presenterar forskning kring CSA på nationell nivå och indirekta studier är studier som har en annan målgrupp men ändå bedömdes vara av relevans för medvetandehöjande åtgärder i nationell skala.

Indirekt relevant forskning (Figur 3)

Den indirekta forskningen behandlar cybersäkerhetsutbildning i organisationer. Resultaten visar att följande faktorer påverkar hur individer tar till sig utbildning:



Figur 2: Sökprocess forskningsöversikt



Figur 3: Forskning med indirekt relevans

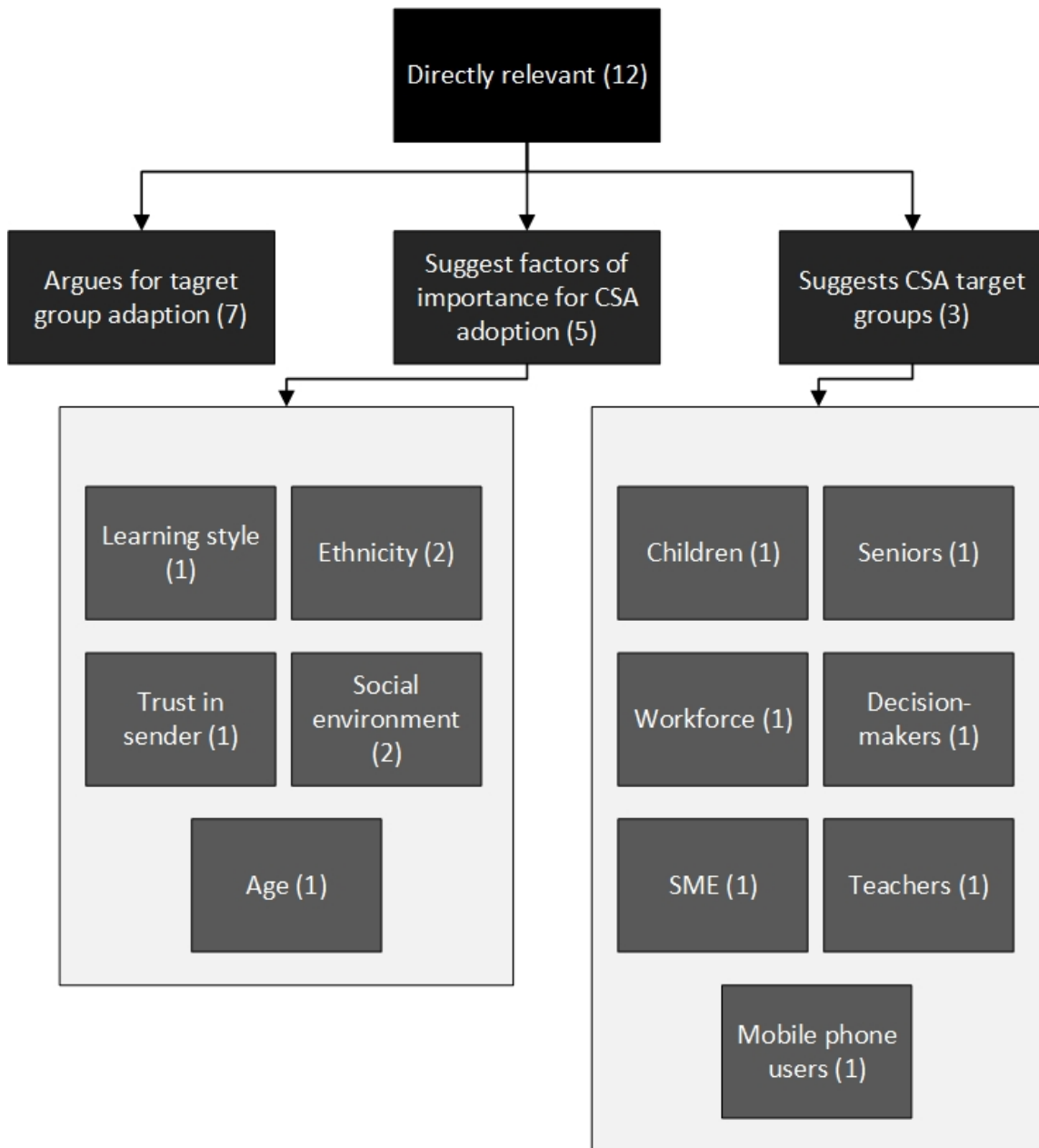
- Individuella faktorer: lärstil, kompetens, kön, tidigare erfarenheter och nationell kultur.
- Sociala faktorer: tillit till avsändaren och individens sociala miljö, exempelvis kollegor eller familj.
- Upplevd relevans och anpassning: studier visar att utbildning ofta uppfattas som irrelevant när den inte är anpassad till mottagarens roll eller tekniska nivå.

Dessa resultat visar att en standardiserad utbildningsmodell sällan är effektiv.

Direkt relevant forskning (Figur 4)

Den direkt relevanta forskningen fokuserar på personer i deras roll som privatpersoner och är baserad på nationella eller breda urvalsgrupper. Här framträder tre tydliga områden:

- Argument för målgruppsanpassning: Flera studier visar att olika grupper i samhället har skilda behov och sårbarheter. Exempelvis påverkar ålder, etnicitet och social kontext hur individer tolkar och agerar på cybersäkerhetsinformation.



Figur 4: Forskning med direkt relevans

- Faktorer viktiga för att anpassa utbildning: Studierna lyfter att effektiv utbildning bör ta hänsyn till lärostil, tillit till avsändaren och gruppens sociala strukturer. Detta överensstämmer med resultaten från den indirekta forskningen.
- Föreslagna målgrupper för nationella insatser: Forskningen identifierar grupper som barn, äldre, SMF, beslutsfattare, lärare och mobilanvändare som viktiga att nå.

2.1.3 Slutsats delstudie 1

Det finns en tydlig samsyn mellan forskning och policy om att en öne-size-fits-all-modell inte är tillräcklig. Samtidigt saknas implementerade metoder och empirisk evidens för hur målgruppsanpassning bör genomföras i praktiken. Denna delstudie visar att EU:s medlemsstater identifierar olika målgrupper, men ger mycket begränsad vägledning kring hur dessa grupper bör nås och hur utbildningsmaterial ska utformas. Studien identifierar tre huvudsakliga målgrupper, vilka dessutom pekas ut av olika anledningar:

- Barn och unga vilka pekas ut framförallt i nationella cybersäkerhetsstrategier med motiveringen att barn är i skyddsbehov och att cyberhygien är en viktig kunskap att lära sig i skolan.
- Yrkesverksamma som pekas ut antingen som möjliggörare för utbildning av andra (exempelvis lärare) eller för att de arbetar i utsatta branscher (exempelvis SMF).
- Äldre som pekas ut som en särskilt utsatt grupp.

Det är noterbart att målgruppsanpassning mer sällan motiveras av individernas olika behov vilket belyser behovet av ytterligare studier för att kartlägga olika individers behov och preferenser.

2.2 Identifiering av målgrupper

Den första delstudien fokuserade på tidigare forskning och nuvarande praktik i EUs medlemsländer. Den andra delstudien riktade istället in sig på Sverige och svenska medborgares preferenser gällande CSA aktiviteter. Syftet med denna delstudien var att bättre förstå *hur olika grupper i samhället upplever och vill ta del av information om cybersäkerhet*. Vi ville särskilt undersöka vilka demografiska faktorer

som är viktigast att ta hänsyn till när man utformar nationella satsningar på cybersäkerhetsmedvetenhet.

Studien fokuserade på följande fyra delfrågor kring svenskars upplevelse av CSA aktiviteter:

- Hur har svenskar tidigare fått information om cybersäkerhet?
- Vilka former av information uppskattar svenskar mest?
- Hur mycket tid är svenskar villiga att lägga?
- När och från vem vill svenskar helst få sådan information?

För att underlätta läsbarheten följer en sammanfattning av delstudiens genomförande och resultat innan en djupare genomgång av studiens statistiska underlag presenteras.

2.2.1 Sammanfattning delstudie 2

För att få en så representativ bild som möjligt genomfördes studien som en omfattande enkätundersökning bland den svenska befolkningen. Totalt deltog 2049 personer i olika åldrar, med varierande utbildningsnivåer, yrken, boendeformer och IT-kunskaper. Det gör studien ovanlig i sitt slag, eftersom många tidigare undersökningar främst fokuserat på anställda i organisationer eller på studenter. Deltagarna fick svara på frågor om både tidigare erfarenheter och framtida preferenser när det gäller cybersäkerhetsinformation. Exempel på informationsformer som ingick var e-postutskick, digitala kurser, föreläsningar, spel, simuleringar och tips som dyker upp direkt i relevanta situationer, till exempel när man skapar ett lösenord.

Resultaten visar tydligt att det inte finns någon universallösning som passar alla. Ålder, utbildning, yrke och IT-vana har stor betydelse för hur människor vill ta till sig information om cybersäkerhet. Däremot spelar kön och bostadsort en mindre roll än vad man ibland antar. Samtidigt framträder några gemensamma mönster hos befolkningen:

- Många föredrar kortfattad information som går att ta del av vid behov.
- Innehåll på det egna språket och utan tekniska facktermer upplevs som särskilt viktigt.
- Förtroendet för avsändaren spelar stor roll. Myndigheter och välkända tjänsteleverantörer uppfattas ofta som mest trovärdiga.

2.2.2 Delstudiens genomförande

Studien genomfördes som en webbaserad enkät och riktade sig till vuxna personer i Sverige. Datainsamlingen skedde med hjälp av ett undersökningsföretaget SYNO som använder etablerade webbpaneler [21]. Detta för att säkerställa att deltagarna speglade befolkningen i stort, snarare än att endast nå särskilt intresserade eller tekniskt kunniga personer. Totalt deltog 2049 personer som alla lämnade fullständiga och giltiga svar. Urvalet stratifierades utifrån ålder och kön, vilket innebär att man i förväg bestämde hur många deltagare som skulle ingå i varje grupp. På så sätt minskade risken för snedfördelning, till exempel att yngre eller mer teknikintresserade personer skulle dominera materialet.

För att göra det möjligt att identifiera olika målgrupper samlades bakgrundsinformation om deltagarna in. Deltagarna fick svara på de bakgrundsfrågor som listas i Tabell 1 som återfinns i Appendix A tillsammans med alla andra tabeller i denna rapport.

Enkäten innehöll frågor om både tidigare erfarenheter och framtida preferenser. Deltagarna fick bland annat ange:

- vilka typer av cybersäkerhetsinformation de tidigare tagit del av, till exempel via e-post, kurser eller informella samtal,
- hur de upplevt dessa erfarenheter, exempelvis om informationen varit begriplig och relevant,
- hur de helst vill få sådan information i framtiden,
- hur mycket tid de är villiga att lägga per vecka,
- samt från vilka aktörer de helst tar emot information (till exempel myndigheter eller tjänsteleverantörer).

Frågorna utformades efter etablerade riktlinjer för enkätutveckling och testades i flera steg. Bland annat genomfördes intervjuer där personer fick resonera högt kring hur de tolkade frågorna. Detta var särskilt viktigt för att säkerställa att även personer med låg IT-vana eller begränsade kunskaper i svenska kunde förstå enkäten på avsett sätt. För att säkerställa hög datakvalitet användes flera kontrollmekanismer under datainsamlingen. Enkäten innehöll kontrollfrågor för att identifiera oseriösa svar. Svar som gavs orimligt snabbt eller i tydliga mönster granskades och togs bort vid behov. Även fritextsvar kontrollerades för att säkerställa att de var relevanta.

2.2.3 Resultat delstudie 2

Här presenteras de frågor som ställdes till studiens deltagande samt deltagarnas svar. Notera att många av frågorna hade fler alternativ än de som presenteras i denna rapport. Kontakta rapportens författare för tillgång till det kompletta dataunderlaget.

Vad har människor redan varit med om? (Tidigare exponering)

Den första frågan var *på vilka sätt deltagarna tidigare fått cybersäkerhetsinformation*. Resultatet, som återges i Tabell 2, visar att många har haft någon form av kontakt med cybersäkerhetsinformation, men att det också finns en tydlig grupp som uppger att de *inte* fått sådan information alls. I nästa steg, Tabell 3, analyserades medelskillnaden inom varje bakgrundsvariabel i studien för att se vilken påverkan bakgrundsvariablerna hade på resultatet. Personer med låg IT-kompetens och kort utbildning rapporterar betydligt oftare att de aldrig fått cybersäkerhetsinformation.

Hur upplevdes tidigare information? (Uppskattning och effekt)

Deltagarna fick också värdera sina tidigare erfarenheter. Överlag ligger omdömena på en positiv men inte entusiastisk nivå: många tycker att informationen är hyfsat begriplig och relevant, men den beteendeförändrande effekten är svagare vilket visas i Tabell 5. Människor kan alltså tycka att insatserna är okej men att de trots det inte ändrar deras beteende. Det pekar mot ett glapp mellan information och handling: att förstå ett råd är inte samma sak som att tillämpa det i vardagen. Skillnaderna i svar baserat på bakgrundsvariablerna presenteras i Tabell 5 som visar att utbildningsnivå har högst påverkan följt av IT-kompetens och Ålder.

Vad vill människor ha framåt?

När deltagarna i stället fick välja hur de helst vill ta del av cybersäkerhetsinformation framträder ett tydligt mönster. Folk vill ha sådant som är enkelt, flexibelt och går att konsumera när det passar, vilket framgår av Tabell 6. När vi tittar på skillnader mellan grupper följer de liknande mönster som förut där Kön och Bostadsort har mindre påverkan än andra variabler som har en högre påverkan, se Tabell 7.

När vill man få informationen?

Nästa fråga behandlade när deltagarna vill ta del av cybersäkerhetsinformation och som synes i Tabell 8 ger svaren på denna fråga ytterligare stöd till bilden att personer fördrar att få tillgång till information på sina egna villkor, när de önskar eller när de är i behov av den. Tabell 9 visar skillnaden mellan bakgrundsvariablerna där vi åter kan se att kön påverkar minst. Vi börjar kunna se ett tydligt mönster där ålder, IT-kompetens, sysselsättning och utbildningsnivå har en klart högre påverkan på

resultaten än bostadsort och kön. För att öka rapportens läsbarhet presenteras inga tabeller över skillnader härnäst.

Vem litar man på som avsändare?

I denna fråga fick deltagarna besvara vilken avsändare de föredrog framträder en stark preferens för två typer av aktörer: (1) *den centrala offentliga avsändaren* och (2) *de tjänster man använder i vardagen*. Resultaten syns i Tabell 9. Vad gäller skillnader baserat på bakgrundfrågor så påverkar utbildningsnivå och ålder mest medans kön och bostadsort har minst påverkan.

Hur mycket tid vill man lägga?

En väldigt konkret indikator på engagemang är tid. därför frågade vi deltagarna hur mycket tid de är villiga att lägga på att ta till sig cybersäkerhetsinformation, per vecka. Som synes i Tabell 11 är resultatet uppmuntrande: majoriteten är beredda att lägga *lite* tid regelbundet. Nästan 80% svarar att de vill lägga fem minuter eller mer. "5–15 minuter" är det typiska tidsspännat. Det är en viktig signal för alla som designar material: man måste tänka mikrolärande snarare än långa kurser för att nå brett. Återigen påverkar kön och bostadsort minst medans sysselsättning, IT-kompetens och ålder har en större påverkan.

Vad måste informationen vara för att folk ska vilja ta del av den?

Slutligen skattade deltagarna olika möjliga egenskaper hos cybersäkerhetsutbildning. Tre saker sticker ut som viktiga: *språk*, *korta format* och *möjlighet att fördjupa sig vid behov*, se Tabell 12. För denna fråga påverkar IT-kompetens resultaten mest medans bostadsort och kön har minst påverkan.

2.2.4 Analys av delstudie 2

På en övergripande nivå framträder en tydlig bild av delstudiens resultat, vilka kan sammanfattas som:

- **Människor vill ha flexibilitet:** on demand och kontextuellt slår schemalagt.
- **Människor vill ha kort format:** 5–15 minuter per vecka är normen.
- **Människor vill ha begriplighet:** modersmål, korthet och låg facknivå är centralt.
- **Förtroende är en nyckel:** myndigheter och tjänsteleverantörer är mest önskade avsändare.

Ett genomgående mål med delstudien var att identifiera vilka bakgrundsfaktorer som i praktiken har störst betydelse för hur människor upplever, värderar och vill ta del av information om cybersäkerhet. När resultaten från samtliga analysdelar vägs samman återkommer vissa faktorer och de med störst skillnader är:

Ålder framstår som den mest genomgående betydelsefulla faktorn i studien. Skillnader mellan åldersgrupper återfinns i nästan alla analyser: hur mycket tid man är villig att lägga, vilka format man föredrar, vilka avsändare man litar på och hur man upplever tidigare cybersäkerhetsinformation. Yngre deltagare föredrar kortare insatser och visar visst intresse för spel, medan äldre deltagare oftare accepterar längre format och i högre grad föredrar myndigheter som avsändare och visar en stark preferens för e-post.

IT-kompetens är den näst starkaste förklaringsfaktorn. Personer med hög IT-kompetens visar större förtroende för IT-företag och är generellt positiva till både digitala och fysiska föreläsningar de är också mer villiga att lägga tid på cybersäkerhetsinformation. Personer med låg IT-kompetens har däremot både lägre exponering och lägre uppskattning av tidigare insatser, de är också mer ovilliga att lägga tid på cybersäkerhetsinformation. Detta indikerar en tydlig risk för en självförstärkande klyfta, där de som redan är kunniga får mest stöd, medan de som har störst behov nås i mindre utsträckning och belyser vikten av att nå personer med låg kunskapsnivå.

Utbildningsnivå har också en tydlig påverkan som liknar den för IT-kompetens. Högre utbildning hänger samman med högre upplevd relevans, bättre förståelse av tidigare information och större vilja att engagera sig i cybersäkerhetsinformation. Skillnaderna tyder på att utbildning påverkar både förmågan att tolka generella råd och viljan att engagera sig i säkerhetsfrågor.

Sysselsättning visar en måttlig men konsekvent påverkan. Personer i arbetslivet har oftare tidigare erfarenhet av cybersäkerhetsinformation, vilket kan antas vara genom arbetsplatsrelaterade insatser. Studenter, arbetslösa och pensionärer uppvisar större variation i preferenser. Detta understryker att arbetsplatsen fortfarande är en central kanal för cybersäkerhetsutbildning, något som också riskerar att exkludera stora grupper i samhället.

I kontrast till ovanstående faktorer har **kön** och **bostadsort** genomgående liten påverkan på resultaten. Skillnader mellan män och kvinnor är små och inkonsekventa över frågorna, och boende i stad respektive landsbygd påverkar preferenser i låg utsträckning. Detta innebär inte att dessa faktorer är irrelevanta i alla sammanhang, men i denna studie förklarar de endast en liten del av variationen i hur cybersäkerhetsinformation uppfattas.

Sammantaget visar studien att bakgrundsfaktorer kopplade till livsfas och digital vana

är betydligt viktigare än traditionella demografiska kategorier. Ålder, IT-kompetens och utbildning formar både individers behov och deras förutsättningar att ta till sig cybersäkerhetsinformation. Kön och bostadsort har däremot begränsad förklaringskraft.

För utformningen av framtida cybersäkerhetsinsatser innebär detta att resurser bör fokuseras på att anpassa innehåll, format och avsändare efter hur människor lever och använder teknik, snarare än efter vem de är i snäv demografisk mening. En sådan omställning ökar sannolikheten att cybersäkerhetsinformation inte bara når ut utan också gör faktisk skillnad i människors digitala vardag.

2.3 Ökad förståelse för behov och preferenser

I projektets avslutande delstudie genomfördes intervjuer med 24 personer för att få en djupare förståelse för människors preferenser och behov och skillnader baserat på de demografiska faktorer som identifierats som betydelsefulla i delstudie 2. Återigen presenteras en sammanfattning av studien och dess resultat innan en djupare genomgång av genomförande och resultat presenteras.

2.3.1 Sammanfattning delstudie 3

Intervjuer genomfördes med 24 personer och dessa analyserades i två steg. Målet med den första analysen var att identifiera allmänna behov och preferenser för medvetandegörande åtgärder. I det andra analyssteget fokuserade analysen på skillnader mellan personer i olika ålder, sysselsättning, utbildningsnivå och IT-kunskaper.

Det första analyssteget underströk resultaten från delstudie två och visade en bred enighet bland deltagarna kring att information om cybersäkerhet ska vara så kortfattad och enkel att ta till sig som möjligt. Även relevans lyftes och flera deltagare menade att information måste vara av betydelse för dem. Deltagarna uttryckte också att information on-demand eller när den är användbar är positivt samt att det är viktigt att informationen upplevs trovärdig.

Den andra analyssteget fokuserade på skillnader mellan olika grupper och underströk skillnader identifierade i delstudie två men med tillägget att dessa skillnader kanske kan kopplas till livssituation snarare än en enskild demografisk faktor. Detta tar sig exempelvis uttryck i att flera deltagare exemplifierar sina behov utifrån sig själva och vilken typ av information de har behov av att skydda. Föräldrar hänvisar exempelvis till sina barn, och personer som arbetar till säkerhet på arbetsplatsen.

2.3.2 Delstudiens genomförande

Intervjuer genomfördes med 24 personer i olika ålder och med olika sysselsättning och utbildningsnivå. Intervjuerna genomfördes via telefon eller som videomöte (beroende på deltagarens önskemål) och anonymiserades. Intervjuerna transkriberades och analyserades tematiskt i två steg. Målet med den första analysen var att identifiera allmänna behov och preferenser för medvetandegörande åtgärder. I det andra analyssteget fokuserade analysen på skillnader mellan personer i olika ålder, sysselsättning, utbildningsnivå och IT-kunskaper.

2.3.3 Resultat delstudie 3

I det första analyssteget identifierades fem teman som beskriver aspekter av deltagarnas preferensen avseende cybersäkerhetsinformation. De teman som identifierades är följande.

- **Minimera kognitiv belastning:** Cybersäkerhetsinformation beskrivs genomgående som för omfattande och komplicerad. Deltagarna beskriver att detta leder till att de ignorerar information eller blir stressade. Även relevans är en del av detta tema där flera deltagare uttryckte att det är viktigt att information upplevs vara för dem.
- **Information ska vara konkret och situationsanpassad:** Deltagarna beskriver att det är viktigt att ha tillgång till information när den är relevant och att den är användbar för dem. Användbar kan både syfta till att den ska upplevas som möjlig att använda och att den ska fungera i deras miljö. Det är exempelvis viktigt att råd som ges av en arbetsgivare går att använda i arbetsmiljön. Att informationen är tillgänglig när den är relevant beskrivs som viktigt för att få stöd i att hantera situationer som uppstår snarare än att behöva memorera fakta.
- **Förtroende och legitimitet är avgörande:** Deltagarna beskriver att det är viktigt att information upplevs som legitim och förtroendeingivande. Detta tar sig uttryck på två sätt. För det första är avsändaren viktig och flera deltagare beskriver att de litar på information från sin arbetsgivare eller en myndighet. För det andra kan informationens format påverka legitimiteten och flera deltagare beskriver exempelvis att en legitim länk lätt kan misstas för Phishing.
- **Ansträngning måste stå i relation till upplevd risk:** Detta tema har med relevans att göra där flera deltagare ger uttryck för att det är en ansträngning

att engagera sig i cybersäkerhet och den ansträngningen måste stå i proportion till upplevs risk, det behöver finnas en anledning att engagera sig. Därför är det viktigt att cybersäkerhetsinformation är relevant för läsaren på så sätt att läsaren kan använda den inhämtade informationen i sin vardag.

- **Preferenser varierar med självförtroende och erfarenhet:** Avslutningsvis är det tydligt att erfarenhet och självförtroende påverkar vilken typ av information man vill ha. Deltagare som upplever sig som IT-kunniga beskriver en större acceptans för komplex information medan deltagare med lägre kunskap istället vill ha tydlig och enkel guidning.

Därefter genomfördes ytterligare analys av intervjuerna där deltagarna grupperades baserat på ålder, utbildningsnivå. IT-kompetens och sysselsättning. Analysen fokuserade på skillnader mellan grupperna.

Skillnader baserat på ålder

Vid analys baserat på åldersgrupper delades deltagarna in i tre grupper:

- 18-30 år
- 31-55 år
- 56+ år

Den yngsta gruppen karaktäriseras av digital vana och en viss skepsis mot auktoritet. Gruppen föredrar system som ger råd automatiskt och de har en viss acceptans för komplex information, men tappar samtidigt intresset fort. Gruppen visar en generell skepsis både vad gäller digital information och kunskap om digitala risker. Flera deltagare uttrycker dock en uppgivenhet inför vad som upplevs som många risker eller att riskerna inte gäller dem.

Mellangruppen beskriver ett mer pragmatiskt förhållningssätt till säkerhet som är styrt av tid och applicerbarhet. Gruppen efterfrågar tydliga och direkt applicerbara råd som är lätta att ta till sig. Flera deltagare uttrycker att auktoritära källor såsom arbetsgivare och banker är trovärdiga och knyter sitt säkerhetsbehov till livserfarenheter såsom barn och jobb.

Den äldsta gruppen uttrycker behov av stöd och instruktioner med låg komplexitet, gärna i form av stegvisa guider med mänskligt stöd. När det gäller förtroende för avsändaren beskriver flera deltagare i gruppen formatet som viktigt snarare än avsändaren och nämner fysiska produkter som mer pålitliga än digitala. Osäkerhet är ett genomgående tema som leder till att man undviker riskfyllda situationer.

Skillnader baserat på utbildningsnivå och IT-kompetens

Vid analys baserat utbildningsnivå delades deltagarna in i tre grupper:

- Gymnasieutbildning eller lägre
- Eftergymnasial utbildning
- Eftergymnasial utbildning längre än tre år

Deltagare i gruppen med lägst utbildningsnivå beskrev sig själva som otekniska och upplevde det som jobbigt med komplex information. Man föredrar enkla, tydliga beskrivningar och upplever stress när det blir för mycket information. Flera deltagare beskriver en rädsla för att göra fel och litar på information från källor man känner igen.

Medelgruppen präglas av behov av relevans och nytta är ständigt åtkommande. flera deltagare beskriver att det är okej med komplex information så länge den är relevant för dem. Deltagarna beskriver säkerhet som ett verktyg och vill veta vad de ska göra men behöver inte veta hur eller varför, man är snarare problemfokuserad och vill veta hur man ska lösa en situation. "Jag gör det för att jag måste" är ett återkommande citat där deltagare hänvisar till krav från arbete eller familj.

Den grupp med högst utbildningsnivå visar ett större intresse för hur och varför och efterfrågar djupare beskrivningar och motiveringar till varför man ska göra på ett visst sätt. Samtidigt återkommer en ovilja mot att ta till sig information som inte känns relevant. Flera deltagare beskriver att säkerhetsinformation ofta känns som att den är för generell eller enkel för att de ska vara intresserade.

En ytterligare analys baserat på IT-kompetens genomfördes och deltagarna delades in i tre grupper, låg, medel och hög. Låg och medel motsvarar nybörjare och genomsnittlig användare i delstudie 2. Hög motsvarar avancerade eller professionella användare från delstudie 2. Resultaten av denna analys liknade resultaten för utbildningsnivå där låg IT-kompetens hade samma resultat som gruppen med lägst utbildningsnivå, mellangrupperna motsvarade varandra och grupperna med hög utbildning och hög IT-kompetens motsvarade varandra.

Skillnader baserat på sysselsättning

Slutligen delades deltagarna upp baserat på sysselsättning i grupperna studenter, arbetande och icke arbetande (som också innehåller personer som inte heller studerar). Denna uppdelning framträdde naturligt under analysen genom att deltagare i gruppen arbetande konsekvent hänvisade till säkerhetsbehov styrt av arbetet, studenter till tjänster och uppgifter relaterade till studier och icke arbetande privat användning. Mellan dessa grupper fanns en tydlig skillnad i hur man exponeras för

säkerhetsinformation där arbetande hänvisar till information genom arbetet och ofta beskriver jobbet som en motivation för att lära sig om cybersäkerhet. Studenter beskriver oftare ett eget ansvar för att hitta information även om viss information tillhandahålls av exempelvis lärosätet medans de som inte arbetar eller studerar upplever att de inte har någon som ger dem information utan får ta ansvar för sin egen utbildning. Även vad gäller motivation för att ta till sig säkerhetsinformation och faktorer som bidrar till ovilja mot information så är det tydliga skillnader mellan grupperna. Både arbetande och studerande beskriver relevans och tid som viktiga faktorer. Arbetande framförallt framhåller tidspress som gör att informationen måste vara relevant för dem och studerande prioriterar snarare betrodda källor och är mer selektiva i vilka källor de vill lyssna på. En önskan om autonomi kan ses i båda dessa grupper där man vill ha information som gör att man kan hantera sin säkerhet på egen hand. Gruppen med icke-arbetande söker i högre grad stöd och uppmuntran, och beskriver att cybersäkerhet upplevs som överväldigande. Gruppen visar också en vilja att lägga mer tid på att förstå cybersäkerhet och söker trygghet och säkerhet i sitt digitala användande.

3 Diskussion och slutsatser

Utgångspunkten i detta projekt var att det finns för lite empirisk forskning om hur olika grupper beter sig, lär sig och engagerar sig i cybersäkerhet. Detta samtidigt som vi vet att det är stora skillnader mellan olika gruppers preferenser och förutsättningar. Som avslutning på denna rapport presenteras först projektets huvudsakliga insikter och därefter råd vid utformning av nationella cybersäkerhetsprogram.

3.1 Huvudsakliga insikter

Inledningsvis understryker detta projekt vikten av att anpassa informationsinsatser till den tänkta mottagaren. Projektet visar att det är stora skillnader i personers tillgång till cybersäkerhetsinformation som till stor del ger av arbetsgivare. Det är också stora skillnader i hur olika personer vill ta till sig cybersäkerhetsinformation, framförallt avseende informationens sakliga innehåll.

När det kommer till föredragna format för säkerhetsinformation är det tydligt att det på gruppnivå finns gemensamma prioriteringar som delas av en stor del av studiens deltagare:

- Det är önskvärt att själv bestämma när man tar del av information, alternativt att stöd automatiskt presenteras i situationer när information är relevant.
- Tiden man kan tänka sig att lägga på cybersäkerhet är begränsad till cirka 5–15 minuter som norm.
- Enkel och tydlig information är viktigt - detta avser både språk och facknivå.
- Det är viktigt att information kommer från en betrodd avsändare och här ses myndigheter, tjänsteleverantörer och arbetsgivare som mest trovärdiga.
- Informationen måste upplevas som relevant och det finns tydliga skillnader i vad olika grupper upplever som relevant.

Studien visar också att det finns skillnader på detaljnivå där det exempelvis kan nämnas att personer som har låg kunskap om cybersäkerhet också uppvisar en större ovilja att ta del av cybersäkerhetsinformation. Detta kan tolkas som att det finns en problematisk grupp som både är svår att nå och som har låg kunskap. En annan grupp som särskiljer sig är personer som inte arbetar som beskriver en högre acceptans mot information som tar mer tid att konsumera. Studien understryker också att många deltagare får information genom arbetsgivare samtidigt som andra inte får det vilket påvisar en informationsojämlikhet. En möjlig tolkning av det är

att nationella cybersäkerhetsprogram bör fokusera på målgrupper som inte redan täcks av existerande initiativ. Vilka dessa grupper är har inte varit ett fokus för detta projekt utan behöver kartläggas i framtida arbete.

Från ett samhällsperspektiv är olika personer olika utsatta. Förutom att vissa grupper i dagsläget har svårt att få tillgång till cybersäkerhetsträning så är vissa grupper av särskild betydelse för samhällets säkerhet. Man kan exempelvis anta att personer i politiskt utsatt ställning är mer utsatta för cyberhot, eller att lärare är särskilt viktiga då de har en möjlighet att påverka barn och ungas säkerhetskunskaper. Det senare kan liknas vid tanken om *champions* i organisationer [1]. Det saknas i allt väsentligt forskning kring vilka dessa grupper är och hur de ska hanteras i nationella cybersäkerhetsprogram och det utgör ett distinkt kunskapsglapp som framtida forskning kan adressera.

3.2 Råd vid utformning av nationella cybersäkerhetsprogram

Som avslutning på denna rapport presenteras fyra råd för utformning av nationella cybersäkerhetsprogram.

Råd 1: Dela upp informationsinsatser i generella och specifika. Projektet visar dels att det finns många gemensamma nämnare i hur personer vill ta till sig information samtidigt som vissa grupper behöver anpassade insatser. För att täcka en så stor del av befolkningen som möjligt kan ett nationellt cybersäkerhetsprogram delas upp i en generell och en specifik del. Den generella delen kan utgå från de gemensamma prioriteringar som presenteras i sektion 3.1 och förväntas ge goda resultat för en stor del av befolkningen. Den specifika delen behöver arbeta mer med målgruppsanpassning både avseende metodik och innehåll.

Råd 2: Fokusera på grupper som inte redan täcks av existerande initiativ. Många medborgare får redan cybersäkerhetsinformation via exempelvis arbetsgivare och för att säkerställa effektivitet är det relevant att fokusera på målgrupper som inte redan täcks av existerande initiativ. Vikten av denna prioritering understryks av studiens resultat som visar att personer med låg kunskapsnivå också förefaller mindre intresserade av cybersäkerhet vilket indikerar att detta är en problemgrupp.

Råd 3: Fokusera på livssituation snarare än demografi vid utformning av informationsinsatser. Projektet visar att det finns stora skillnader i vilken information människor efterfrågar. Skillnaderna grundar sig på personers livssituation snarare än demografi och därför är det relevant att fokusera på livssituation vid

utformning av nationella cybersäkerhetsprogram. Detta kan exempelvis innebära riktad information mot pensionärer, föräldrar, personer med låg IT-vana eller studenter.

Råd 4: Identifiera grupper som har en stor påverkan på den nationella säkerhetsnivån. Det avslutande rådet utgår från insikten att olika personer bidrar till nationens säkerhet på olika sätt. Genom att identifiera grupper som i sin tur bidrar till kunskapsspridning, exempelvis lärare, kan en högre nivå av kunskap byggas i samhället på sikt. Dessutom kan samhällets motståndskraft ökas genom att personer som kan antas vara speciellt utsatta ges extra fokus.

4 ENGLISH Introduction

Note that the english version of the report is a translation of the Swedish version. It was created using Generative AI and has been proof-read by the author.

As society becomes increasingly digital, the risk that we are exposed to cyberattacks also increases. Sweden is among the most technologically advanced countries in the world, which brings major advantages but also makes us especially vulnerable to digital threats. To strengthen national resilience, everyone who uses digital services, not only experts, needs to understand how to protect themselves.

The ICANP project has examined what needs different groups in society have regarding cybersecurity, and how they prefer to receive information and training. This is done to help improve how cybersecurity is communicated in society. To simplify things for the reader, the report is written so that the project's most important results are presented first, followed by methodology and discussion. Therefore, some repetition occurs in the report. Readers who only want to read the project's main results are recommended to first read Chapter 4.2 and then Chapter 6.

4.1 Cybersecurity awareness for private individuals

Sweden's high degree of digitalization is highlighted by both the EU Commission and the OECD [6, 20]. We use digital technology for everything from banking and shopping to contact with authorities and social interaction. At the same time, the National Cyber Security Centre (NCSC) describes how the threat level has increased, not least after Russia's invasion of Ukraine, which has led to a more unstable geopolitical situation [17]. Cyber threats are also varied and include:

- Fraud such as phishing, vishing, and smishing [14].
- Disinformation aimed at destabilizing society [3].
- Ransomware, malware, and supply chain attacks.
- Cybercrime targeting both individuals and companies.

What these have in common is that they often target human behavior rather than technical weaknesses [8]. Industry reports show that at least 75 % of successful cyberattacks involve exploitation of human behavior [7, 18]. This may involve someone clicking a malicious link, using weak passwords, or being tricked into revealing sensitive information [15].

To reduce these risks, technical protections alone are not sufficient — people also need knowledge, understanding, and skills to act securely [4, 12]. Therefore, various forms of cybersecurity training and awareness-raising efforts are essential.

Most people today receive cybersecurity training through their workplace, where the training focuses on policies and routines relevant to the employer [5]. Letting employers be responsible for cybersecurity training leads, at the national level, to three problems:

- The training does not reach everyone. Many groups, for example retirees, students, newly arrived immigrants, or people outside the labor market, receive little or no structured training at all.
- The content is often narrow in that it is based on the employer’s needs rather than the nation’s or the individual’s needs. Society-wide topics such as disinformation, personal cyber hygiene, and fraud prevention are rarely included. Research also indicates that many organizational efforts are not sufficiently effective [10].
- National campaigns must function on an entirely different scale. It is not possible to gather millions of people in classrooms or send targeted training to everyone. Therefore, national programs must be designed in a way that both scales and works for many different types of people.

It is well known in research that people with different backgrounds may need different types of support. Which background factors are most important is not fully established, but may include:

- Demographics: age, gender, and socioeconomic status can influence how one learns and how one perceives risk [13].
- Trust factors: people accept information differently depending on the sender [9].
- Language and technical level: overly advanced language or technical terms prevent some groups from absorbing important information [16].

The problem is that there is too little empirical research on how different groups actually behave, learn, and engage in cybersecurity [19]. National initiatives, such as MSB’s annual campaign Think Secure (Tänk Säkert), are important steps forward. However, research shows that current campaigns are not as effective as they could be [19, 2]. One of the main reasons is that they do not sufficiently account for differences between target groups, where different groups:

- have different digital skills,
- use the internet in different ways,
- are exposed to different types of risks,
- trust different senders, and
- prefer different formats.

Without understanding these differences, it is difficult to develop campaigns that truly make a difference. This knowledge gap is what ICANP addresses.

4.2 Project goals and sub-studies

The project's goal is to identify needs and preferences among different target groups for national cybersecurity programs. This is done through three sub-studies:

- Mapping how national programs in the EU are designed.
- A survey of 2049 Swedes to identify target groups.
- Interviews with representatives from these groups to understand their needs and preferences.

The results of the sub-studies have formed the basis for recommendations on how national training initiatives can be targeted and designed to maximize impact. The remainder of this report presents the three sub-studies and their main results. For readers who want to explore the details of each study, several scientific articles will be published. Most of these are not yet published, but interested readers can gain access by contacting the report's authors.

5 Sub-studies and Results

This chapter presents the project’s sub-studies in chronological order.

5.1 Mapping of National Programmes within the EU

The first sub-study analyses how EU Member States address cybersecurity awareness in their National Cybersecurity Strategies (NCSS), and how these strategies relate to current research on target-group adaptation of awareness-raising measures. The results show that there is strong agreement on the importance of awareness, but concrete methods for adapting awareness-raising measures are largely missing. This sub-study is published in a scientific article in which full details of the research methodology are provided [11].

5.1.1 Analysis of National Cybersecurity Strategies within the EU

The sub-study began with an analysis of the strategies and priorities in EU Member States, based on their National Cybersecurity Strategies (NCSS). The analysis included NCSS from 24 EU countries and shows that all included countries highlight cybersecurity awareness as a strategic objective. The results of the study are presented in Figure 5, which provides a thematic overview of the contents of the strategies.

In addition to identifying cybersecurity awareness as a strategic objective, the analysis revealed the following three main themes:

- **Methods for spreading cybersecurity awareness:** Nineteen of the strategies describe how awareness-raising initiatives should be distributed. The most common approach is to incorporate cybersecurity into school education. This is motivated partly by children being considered a vulnerable group and partly by the view that digital competence is necessary in modern society. Other methods include digital training platforms for the general public.
- **Identified target groups:** Nineteen NCSS specify explicit or implicit target groups for cybersecurity initiatives. The most common target groups are children and young people, followed by older adults, employees, and specific occupational groups such as managers in small and medium-sized enterprises (SMEs). The motivations vary: children and older adults are primarily highlighted as vulnerable groups, while some parts of the workforce are highlighted due to their strategic responsibility or structural vulnerability.

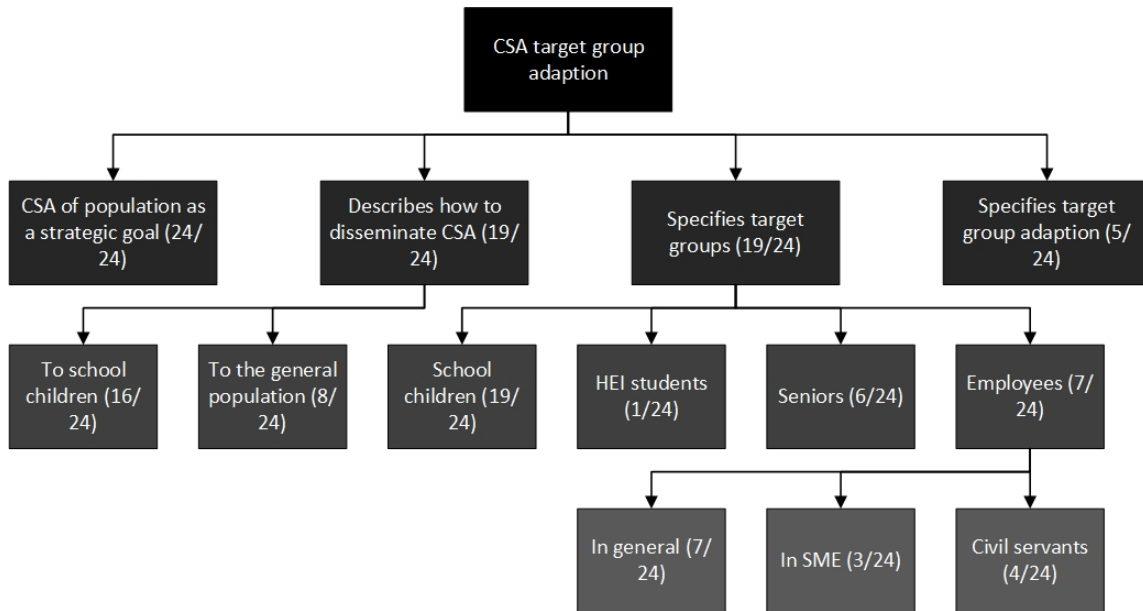


Figure 5: Overview of national strategies

- **Target-group adaptation:** Only five strategies discuss how training should be adapted to the target group. The discussions are high-level and lack specific guidelines. In general, the strategies state that adaptation is necessary but do not explain how it should be carried out.

5.1.2 Overview of Relevant Research

The research overview is based on a review of 20 scientific studies. These studies were identified through a search process that included scientific databases and conferences and are presented in Figure 6. The initial search identified more than 2,000 studies, which were gradually filtered down to 20 included studies.

The studies were categorised as indirectly or directly relevant for national cybersecurity initiatives, as illustrated in Figure 7 and Figure 8. Directly relevant studies present research on cybersecurity awareness at the national level, while indirectly relevant studies focus on other target groups but were still considered relevant for awareness-raising measures at national scale.

Indirectly relevant research (Figure 7)

The indirectly relevant research concerns cybersecurity training in organisations. The results show that the following factors influence how individuals absorb training:

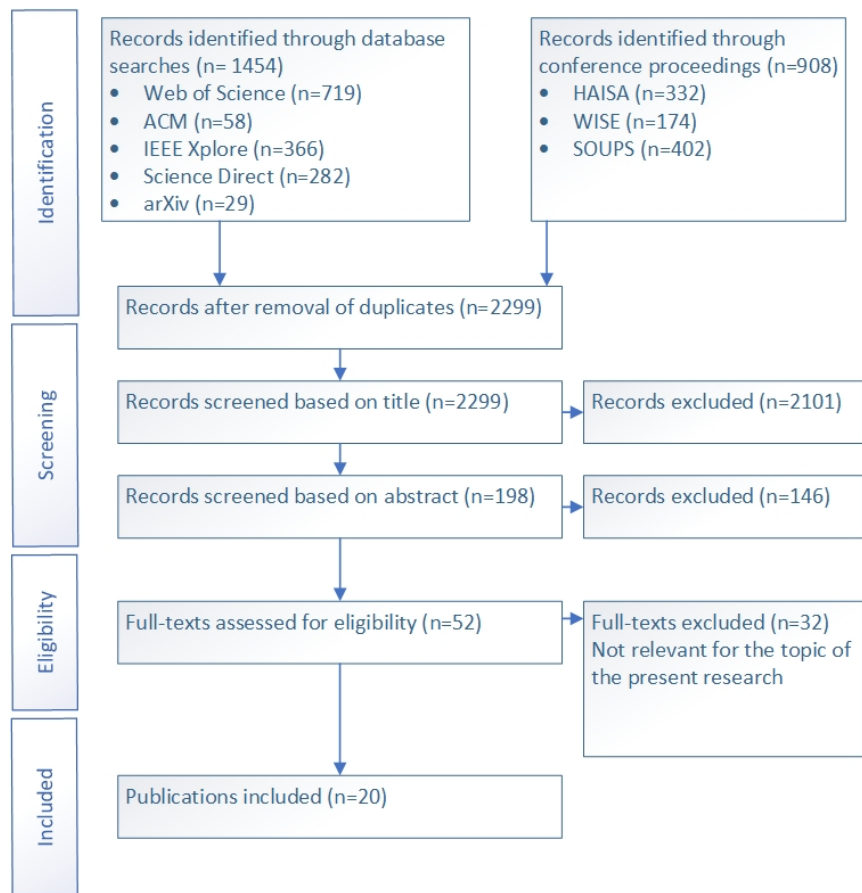


Figure 6: Search process for the research overview

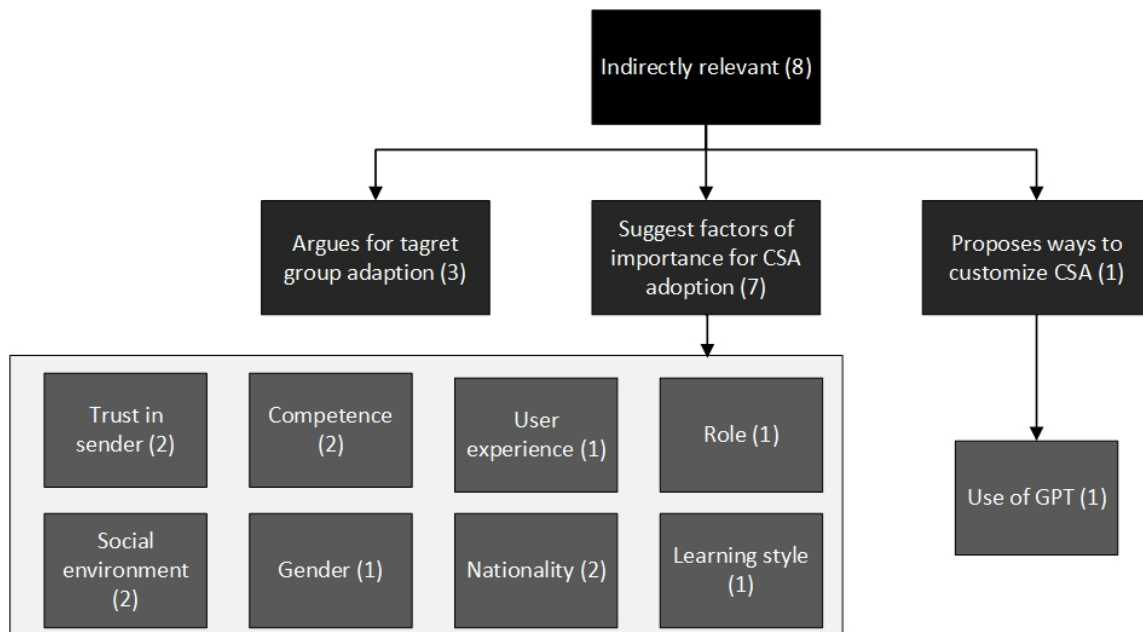


Figure 7: Research with indirect relevance

- **Individual factors:** learning style, competence, gender, previous experiences, and national culture.
- **Social factors:** trust in the sender and the individual’s social environment, such as colleagues or family.
- **Perceived relevance and adaptation:** studies show that training is often perceived as irrelevant when it is not adapted to the recipient’s role or technical level.

These findings show that a standardised training model is rarely effective.

Directly relevant research (Figure 8)

The directly relevant research focuses on national or broad population groups. Three clear themes emerge:

- **Arguments for target-group adaptation:** Several studies show that different groups in society have distinct needs and vulnerabilities. For example, age, ethnicity, and social context influence how individuals interpret and act on cybersecurity information.

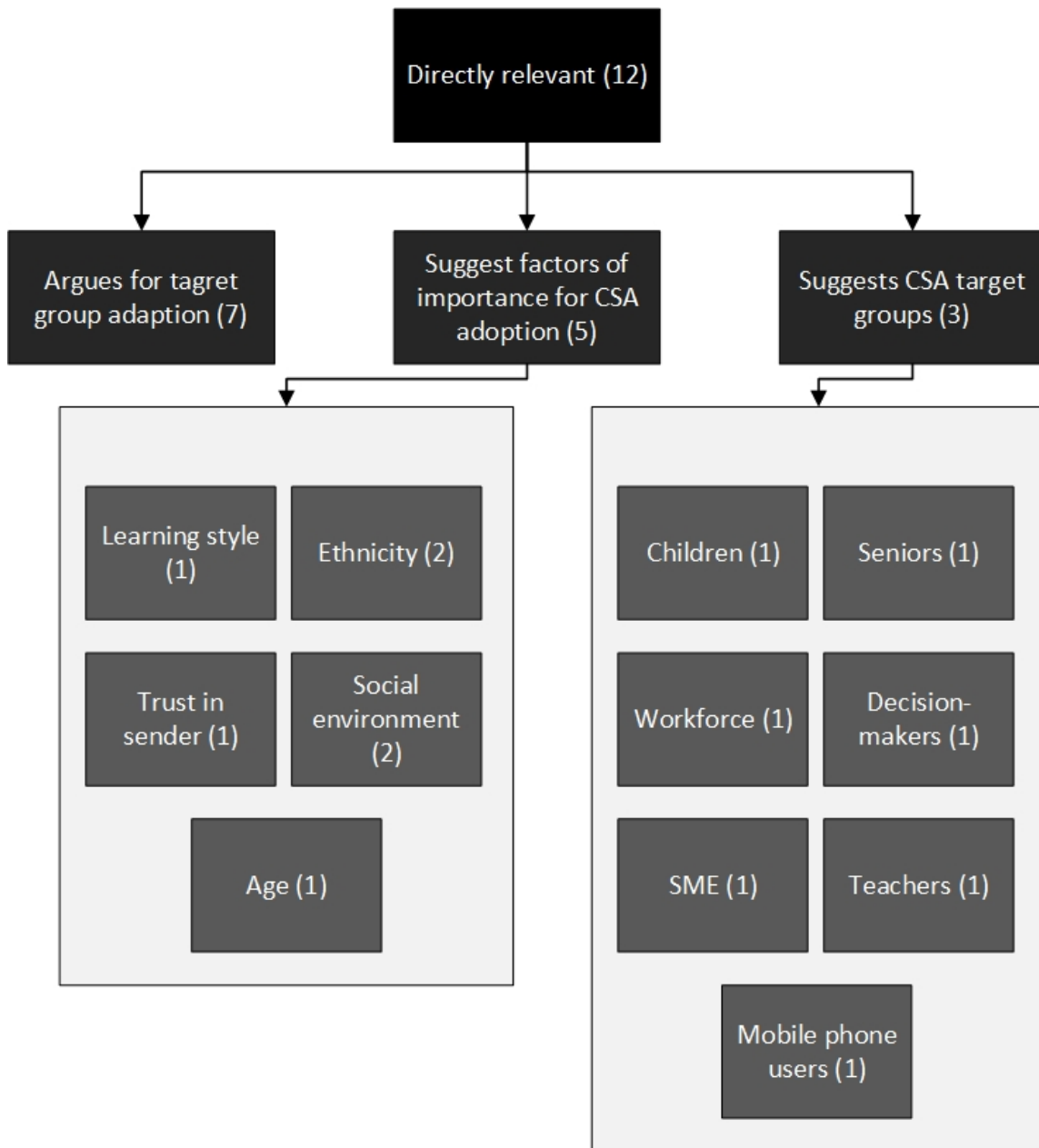


Figure 8: Research with direct relevance

- **Factors important for adapting training:** The studies emphasise that effective training should consider learning style, trust in the sender, and the group’s social structures. This aligns with the results of indirectly relevant research.
- **Proposed target groups for national efforts:** The research identifies groups such as children, older adults, SMEs, decision-makers, teachers, and mobile users as important to reach.

5.1.3 Conclusion of Sub-study 1

There is clear agreement between research and policy that a “one-size-fits-all” model is insufficient. At the same time, implemented methods and empirical evidence for how target-group adaptation should be carried out in practice are lacking. This sub-study shows that EU Member States identify various target groups but provide very limited guidance on how these groups should be reached or how educational materials should be designed. The study identifies three main target groups, highlighted for different reasons:

- Children and young people, primarily highlighted in national cybersecurity strategies based on the need for protection and the importance of learning cyber hygiene in school.
- Working adults, highlighted either as enablers of training others (e.g., teachers) or because they work in vulnerable sectors (e.g., SMEs).
- Older adults, highlighted as a particularly vulnerable group.

It is notable that target-group adaptation is rarely motivated by differences in individual needs, highlighting the need for additional studies to map such needs and preferences.

5.2 Identifying Target Groups

The first sub-study focused on previous research and current practices in EU Member States. The second sub-study instead focused on Sweden and Swedish citizens’ preferences regarding CSA activities. The purpose of this sub-study was to better understand *how different groups in society perceive and want to access information about cybersecurity*. We were particularly interested in identifying which demographic

factors are most important to consider when designing national cybersecurity awareness initiatives.

The study focused on the following four sub-questions regarding Swedes' experiences of CSA activities:

- How have they previously received information about cybersecurity?
- Which forms of information do they appreciate the most?
- How much time are they willing to spend?
- When, and from whom, would they prefer to receive such information?

To facilitate readability, a summary of the study's methodology and results is presented before providing a more detailed review of the statistical data.

5.2.1 Summary of Sub-study 2

To obtain as representative a picture as possible, the study was conducted as a large-scale survey of the Swedish population. A total of 2,049 individuals participated, varying in age, educational level, occupation, living environment, and IT competence. This makes the study unusual, as many previous surveys have mainly focused on employees within organisations or on students. Participants answered questions about both previous experiences and future preferences regarding cybersecurity information. Examples of information formats included email newsletters, digital courses, lectures, games, simulations, and contextual tips appearing directly in relevant situations—for example, when creating a password.

The results clearly show that there is no universal solution that suits everyone. Age, education, occupation, and IT familiarity have a major impact on how people prefer to receive cybersecurity information. In contrast, gender and type of living area play a smaller role than might be expected. At the same time, several patterns emerge across the population:

- Many prefer concise information that can be accessed when needed.
- Content in one's native language and free from technical jargon is perceived as especially important.
- Trust in the sender plays a major role. Government authorities and well-known service providers are often viewed as the most credible.

5.2.2 Study Method

The study was conducted as a web-based survey targeting adults in Sweden. Data collection was carried out with the help of the research company SYNO, which uses established web panels [21]. This ensured that participants reflected the broader population rather than only particularly interested or technically skilled individuals. In total, 2,049 participants provided complete and valid responses. The sample was stratified by age and gender, meaning quotas were set in advance to avoid overrepresentation of, for example, younger or more technologically inclined individuals.

To make it possible to identify different target groups, background information was collected from the participants. They answered the background questions listed in Table 13 which can be found in Appendix A together with all other tables referenced in this report. The questionnaire included questions about both previous experiences and future preferences. Participants were asked:

- which types of cybersecurity information they had previously received—for example via email, courses, or informal conversations,
- how they perceived these experiences, such as whether the information was understandable and relevant,
- how they would prefer to receive such information in the future,
- how much time they were willing to spend per week,
- and from which actors they would prefer to receive the information (e.g., authorities or service providers).

Questions were designed following established survey development guidelines and tested in several steps. For example, cognitive interviews were conducted where individuals verbalised how they interpreted the questions. This was particularly important to ensure that people with low IT proficiency or limited Swedish language skills could understand the questionnaire as intended. To ensure high data quality, several control mechanisms were used during data collection, such as attention checks and removal of suspiciously fast or patterned responses. Free-text answers were also reviewed to ensure relevance.

5.2.3 Results of Sub-study 2

This section presents the survey questions and participants' responses. Note that many questions included more response options than those shown in this report. Contact the report's author for access to the full dataset.

What have people previously experienced? (Previous exposure)

The first question asked *how participants had previously received cybersecurity information*. The results, shown in Table 14, indicate that many have encountered cybersecurity information in some form, but a substantial group reports having received no such information at all. Next, Table 15 shows the mean differences within each background variable to assess their influence on previous exposure. Individuals with low IT competence and short education reported significantly more often that they had never received cybersecurity information.

How was previous information perceived? (Appreciation and effect)

Participants were also asked to evaluate their earlier experiences. Overall, ratings were moderately positive: many found the information understandable and relevant, but the behavioural impact was weaker, as shown in Table 16. This suggests a gap between understanding and action: knowing a recommendation is not the same as applying it in everyday life. Differences in responses based on background variables are shown in Table 17, where education level had the strongest effect, followed by IT competence and age.

What do people want going forward?

When participants selected how they would *prefer* to receive cybersecurity information in the future, a clear pattern emerged: people want information that is simple, flexible, and accessible when it suits them, as shown in Table 18. Differences across groups follow similar patterns as earlier results. Gender and type of residence have the smallest influence, while age, IT competence, employment status, and education level have noticeably higher influence (Table 19).

When do people want to receive information?

The next question asked when participants prefer to receive cybersecurity information. As shown in Table 20, respondents preferred information on their own terms—either on demand or in relevant situations. Table 21 again shows that gender has the least influence, while age, IT competence, employment status, and education level have stronger effects.

Who do people trust as senders?

Participants were asked which type of sender they preferred. Two types clearly stood out: (1) *central public authorities* and (2) *everyday digital services*. The results are shown in Table 22. Differences were again most influenced by education level and age, with gender and residence showing the smallest effects.

How much time are people willing to spend?

A clear indicator of engagement is the time people are willing to spend. As shown in Table 23, most participants were willing to spend *a small but regular amount of time*. Nearly 80% were willing to spend five minutes or more per week. “5–15 minutes” was the most common choice. This is an important signal for those designing materials: micro-learning formats are preferable to long courses.

What must the information be like for people to want to engage with it?

Finally, participants rated the importance of various characteristics of cybersecurity information. Three factors stood out as most important: *language*, *short formats*, and *the ability to deepen one’s knowledge if desired*, as shown in Table 24. For this question, IT competence had the strongest impact, while residence and gender had the least.

5.2.4 Analysis of Sub-study 2

At an overarching level, a clear picture of the sub-study’s results emerges, which can be summarised as follows:

- **People want flexibility:** on-demand and contextual delivery is preferred over scheduled information.
- **People want short formats:** 5–15 minutes per week is the norm.
- **People want comprehensibility:** native language, brevity, and low technical complexity are essential.
- **Trust is key:** authorities and service providers are the most preferred senders.

A central aim of the sub-study was to identify which background factors most strongly influence how people perceive, value, and want to receive cybersecurity information. When results from all analyses are combined, a few factors consistently show the strongest differences:

Age emerges as the single most important factor. Differences between age groups appear in nearly all analyses: how much time people are willing to spend, which formats they prefer, who they trust as senders, and how they perceive previous cybersecurity information. Younger participants prefer short interventions and show some interest in gamified formats, while older participants are more accepting of longer formats, prefer email, and place greater trust in authorities.

IT competence is the second strongest explanatory factor. Individuals with high IT competence show greater trust in IT companies and are generally more positive toward both digital and physical lectures. They are also more willing to spend time on cybersecurity information. Individuals with low IT competence tend to have had less exposure, appreciate previous information less, and are more reluctant to spend time on cybersecurity learning. This indicates a self-reinforcing gap in which those who already have the most knowledge also benefit most, while those who need support the most receive it the least—highlighting the importance of reaching individuals with low prior knowledge.

Education level also has a clear impact, showing patterns similar to IT competence. Higher education is associated with greater perceived relevance, better understanding of previous information, and higher willingness to engage with cybersecurity content. These differences indicate that education influences both the ability to interpret general guidelines and the willingness to engage with security issues.

Employment status has a moderate but consistent influence. People in employment more frequently report previous exposure to cybersecurity information, likely due to workplace training. Students, unemployed individuals, and retirees demonstrate more varied preferences, highlighting that the workplace remains a central channel for cybersecurity education—yet one that risks excluding large parts of the population. In contrast, **gender** and **type of residence** consistently show very limited influence on results. Differences between men and women are small and inconsistent, and whether someone lives in a city or rural area has little impact on their preferences. This does not mean these factors are irrelevant in all contexts, but in this study, they explain only a small portion of the variation in how cybersecurity information is perceived.

Taken together, the results show that background factors related to life situation and digital literacy are far more important than traditional demographic categories. Age, IT competence, and education shape both individuals' needs and their ability to absorb cybersecurity information. Gender and residence play a much smaller role.

For the design of future cybersecurity initiatives, this means that resources should focus on adapting content, format, and sender based on how people live and use technology, rather than who they are in narrow demographic terms. Such a shift

increases the likelihood that cybersecurity information not only reaches people but also makes a meaningful difference in their digital everyday lives.

5.3 Increased Understanding of Needs and Preferences

In the final sub-study of the project, interviews were conducted with 24 individuals to gain a deeper understanding of people's preferences, needs, and differences based on the demographic factors identified as significant in Sub-study 2. As before, a summary of the study and its results is presented first, followed by a more detailed account of the methodology and findings.

5.3.1 Summary of Sub-study 3

Interviews were conducted with 24 participants and analysed in two stages. The aim of the first stage was to identify general needs and preferences regarding awareness-raising measures. The second stage focused on differences between individuals based on age, employment status, education level, and IT competence.

The first stage of analysis reinforced the results of Sub-study 2 and showed broad agreement among participants that cybersecurity information should be as brief and easy to understand as possible. Relevance was also emphasised, with several participants stating that information must matter to them personally. Participants also expressed that on-demand information, or information provided at the moment it is useful, is beneficial, and that credibility is important.

The second stage of analysis focused on differences between individuals and reinforced the patterns found in Sub-study 2, with the addition that these differences may be linked to life situation rather than a single demographic factor. For example, several participants described their needs in terms of the type of information they personally needed to protect: parents referenced their children, while working individuals referenced workplace security.

5.3.2 Study Methodology

Interviews were conducted with 24 individuals of different ages, employment statuses, and education levels. The interviews were conducted by telephone or video call (depending on participant preference) and were anonymised. All interviews were transcribed and analysed thematically in two stages. The aim of the first analysis stage was to identify general needs and preferences related to awareness-raising activities. The second stage focused on differences between individuals with regard to age, occupation, education level, and IT competence.

5.3.3 Results of Sub-study 3

In the first stage of analysis, five themes were identified that describe different aspects of participant preferences regarding cybersecurity information:

- **Minimising cognitive load:** Cybersecurity information was consistently described as too extensive and complicated. Participants stated that this often leads them to ignore the information or feel stressed by it. Relevance is also part of this theme, with several participants emphasising that information must feel personally applicable.
- **Information should be concrete and context-specific:** Participants stressed the importance of having access to information when it is relevant and in a form that is useful to them. “Useful” may refer both to being understandable and to being functional in their specific environment. For example, advice provided by an employer must be feasible to use in the workplace. The ability to access information when it is relevant was highlighted as important for managing situations as they arise, rather than having to memorise facts.
- **Trust and legitimacy are crucial:** Participants emphasised that information must feel legitimate and trustworthy. This was expressed in two ways. First, the sender matters—many participants said they trust information from their employer or public authorities. Second, the format influences legitimacy—for example, several participants noted that a link can easily be mistaken for spam.
- **Effort must correspond to perceived risk:** This theme relates to relevance. Several participants expressed the view that engaging with cybersecurity requires effort, and this effort must be proportionate to the perceived risk; there must be a clear reason to engage. For this reason, cybersecurity information must be relevant to the reader in a way that supports their everyday digital life.
- **Preferences vary with confidence and experience:** Finally, it was clear that experience and confidence influence the type of information people want. Participants who consider themselves IT-competent are more accepting of complex information, whereas those with lower competence prefer clear and simple guidance.

A further analysis was conducted in which participants were grouped based on age, education level, IT competence, and employment status. The analysis focused on differences between groups.

Differences based on age

Participants were divided into three age groups:

- 18–30 years
- 31–55 years
- 56+ years

The youngest group was characterised by digital familiarity and a certain scepticism toward authority. They preferred systems that offer automatic guidance and were more tolerant of complex information, but also lost interest quickly. They expressed general scepticism toward digital information and knowledge about digital risks. Several participants also expressed resignation or the belief that risks did not apply to them personally.

The middle group described a more pragmatic approach to security, driven by time constraints and practical applicability. They requested clear and directly actionable advice that was easy to absorb. Many stated that authoritative sources, such as employers and banks, are credible, and linked their security needs to life experiences such as having children or work responsibilities.

The oldest group expressed a need for support and low complexity, ideally in the form of step-by-step guides with human assistance. When it came to trust in the sender, several participants emphasised format over sender, and stated that physical materials felt more trustworthy than digital ones. Uncertainty was a recurring theme, often leading them to avoid risky digital situations.

Differences based on education level and IT competence

Participants were divided into three groups based on education level:

- Upper secondary education or lower
- Post-secondary education
- Post-secondary education longer than three years

Participants in the lowest education group described themselves as non-technical and found complex information overwhelming. They preferred simple, clear descriptions and reported feeling stressed when presented with too much information. Several described a fear of making mistakes and relied on information from familiar sources. The middle group emphasised relevance and usefulness. Many stated that complex information was acceptable as long as it was directly relevant to their needs. They

viewed security as a practical tool and wanted to know what to do, rather than how or why. A recurring phrase in this group was: “I do it because I have to,” often referring to requirements from work or family.

The group with the highest level of education demonstrated greater interest in the underlying reasoning and often requested deeper explanations of why certain practices are necessary. At the same time, they expressed reluctance to engage with information they considered too general or simplistic. Many said that cybersecurity information often feels too generic to be meaningful.

A further analysis based on IT competence was conducted, dividing participants into three groups: low, medium, and high. Low and medium correspond to beginners and average users from Sub-study 2, while high corresponds to advanced and professional users. The results mirrored the patterns found in the education-level analysis: low IT competence aligned with the group with the lowest education, medium groups aligned with each other, and highly educated participants mirrored those with high IT competence.

Differences based on employment status

Finally, participants were grouped by employment status: students, employed individuals, and non-employed individuals (including those neither employed nor studying). This grouping emerged naturally in the analysis, as employed participants consistently linked security needs to their workplace, students linked theirs to study-related tools and platforms, and non-employed individuals described needs related to personal digital use.

Clear differences were also found regarding exposure to cybersecurity information. Employed participants described receiving information through their workplace and often considered work a motivation for learning about cybersecurity. Students reported a greater personal responsibility to find information, although some guidance was provided by educational institutions. Non-employed individuals felt that they had no one to provide them with information and were responsible for their own learning. Motivational factors also varied. Both employed participants and students emphasised relevance and time as key factors. Employed participants cited time pressure, requiring information to be immediately relevant, while students preferred trusted sources and were more selective about whom they listened to. A desire for autonomy was present in both groups—participants wanted information that enabled them to manage their digital services independently.

The non-employed group sought support and encouragement to a greater extent and described security as overwhelming. They also expressed a willingness to spend more time learning and sought reassurance and safety in their digital use.

6 Discussion and Conclusions

The starting point of this project was the observation that there is too little empirical research on how different groups behave, learn, and engage with cybersecurity. This is despite the fact that we know there are substantial differences between groups in terms of their preferences and conditions. As a conclusion to this report, the project's main insights are first presented, followed by recommendations for the design of national cybersecurity programmes.

6.1 Main Insights

To begin with, this project emphasises the importance of adapting informational efforts to the intended audience. The project shows that there are large differences in people's access to cybersecurity information, where cybersecurity information is predominantly provided through employers. There are also considerable differences in how individuals prefer to receive cybersecurity information, especially regarding the content.

When looking at preferred formats for security information, it is clear that, at the group level, there are shared priorities among a large portion of the study's participants:

- It is desirable to decide for oneself when to access information, or alternatively to receive automatic support in situations where the information is relevant.
- The amount of time people are willing to spend on cybersecurity is limited, with 5–15 minutes per week as the norm.
- Simple and clear information is important—this refers both to plain language and low technical complexity.
- It is important that the information comes from a trusted sender, with authorities, service providers, and employers considered credible.
- The information must be perceived as relevant, and different groups have distinct views on what is relevant.

The study also shows differences at a more detailed level. For example, individuals with low cybersecurity knowledge also demonstrate a greater reluctance to engage with cybersecurity information. This can be interpreted as indicating a problematic group that is both difficult to reach and has low knowledge. Another group that stands out consists of individuals who are not employed, who describe a higher acceptance of information that takes more time to consume. The study also highlights that many

participants receive information through their employers while others do not receive any, illustrating an information inequality. One possible interpretation is that national cybersecurity programmes should focus on target groups that are not already covered by existing initiatives. Identifying these groups was not the focus of this project, however, and needs to be addressed in future work.

From a societal perspective, different individuals face different levels of exposure. In addition to some groups currently having limited access to cybersecurity training, certain groups are also of particular importance for national security. For example, individuals in politically exposed positions may be more vulnerable to cyber threats, or teachers may be especially important because they have the ability to influence the cybersecurity knowledge of children and young people. The latter can be likened to the idea of *champions* in organisations [1]. There is a significant lack of research on which these groups are and how they should be approached in national cybersecurity programmes, representing a clear knowledge gap for future research to address.

6.2 Recommendations for Designing National Cybersecurity Programmes

As a conclusion to this report, four recommendations for the design of national cybersecurity programmes are presented.

Recommendation 1: Divide informational efforts into general and specific initiatives. The project shows that there are many commonalities in how people want to receive information, while some groups require more tailored efforts. To reach as large a proportion of the population as possible, a national cybersecurity programme can include both a general and a specific component. The general component can build on the shared priorities presented in Section 3.1 and is expected to yield good results for a large part of the population. The specific component needs to work more extensively with target-group adaptation in both methodology and content.

Recommendation 2: Focus on groups not already covered by existing initiatives. Many citizens already receive cybersecurity information through, for example, their employers. To ensure efficiency, it is therefore relevant to focus on groups that are not already reached by existing initiatives. This priority is reinforced by the study's finding that individuals with low knowledge levels also appear less interested in cybersecurity—indicating that this is a difficult but important target group.

Recommendation 3: Focus on life situation rather than demographics when designing information efforts. The project shows that there are large differences in the types of information people need. These differences are based on life situation rather than demographic categories. Therefore, it is relevant to focus on life situation when designing national cybersecurity programmes. This could, for example, involve targeted information for pensioners, parents, individuals with low IT literacy, or students.

Recommendation 4: Identify groups that have a significant impact on national security levels. The final recommendation is based on the insight that different groups contribute to national security in different ways. By identifying groups that in turn contribute to the spread of knowledge—such as teachers—a higher level of security can be built in society over time. In addition, societal resilience can be strengthened by giving extra attention to individuals who may be particularly exposed.

Referenser

- [1] Moneer Alshaikh. "Developing cybersecurity culture to influence employee behavior: A practice perspective". I: *Computers & Security* 98 (2020), s. 102003.
- [2] Maria Bada, Angela M Sasse och Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?" I: *arXiv preprint arXiv:1901.02672* (2019).
- [3] Mario Baumann. "'Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations". I: *Contemporary Politics* 26.3 (2020), s. 288–307.
- [4] Melissa Carlton, Yair Levy och Michelle Ramim. "Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills". I: *Information & Computer Security* 27.1 (2019), s. 101–121.
- [5] Nabin Chowdhury, Sokratis Katsikas och Vasileios Gkioulos. "Modeling effective cybersecurity training frameworks: A delphi method-based study". I: *Computers & Security* 113 (2022), s. 102551.
- [6] European Commission. *The Digital Economy and Society Index (DESI) / Shaping Europe's digital future*. <https://digital-strategy.ec.europa.eu/en/policies/desi>. 2022.
- [7] Deloitte. *91% of all cyber attacks begin with a phishing email to an unexpected victim | Deloitte Malaysia | Risk Advisory | Press releases*. <https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html>. 2020.
- [8] Wesam Fallatah, Joakim Kävrestad och Steven Furnell. "Establishing a model for the user acceptance of cybersecurity training". I: *Future Internet* 16.8 (2024), s. 294.
- [9] Julie M Haney och Wayne G Lutters. "'It's {Scary... It's}{Confusing... It's} Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security". I: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 2018, s. 411–425.
- [10] Wu He och Zuopeng Zhang. "Enterprise cybersecurity training and awareness programs: Recommendations for success". I: *Journal of Organizational Computing and Electronic Commerce* 29.4 (2019), s. 249–257.

- [11] Joakim Kävrestad, Erik Bergström och Nathan Clarke. "Thematic Analysis of Cybersecurity Awareness Strategies and Approaches". I: *International Symposium on Human Aspects of Information Security and Assurance*. Springer. 2025, s. 3–16.
- [12] Joakim Kävrestad, Erik Bergström, Eliana Stavrou och Marcus Nohlberg. "Useful but for Someone Else-An Explorative Study on Cybersecurity Training Acceptance". I: *International Symposium on Human Aspects of Information Security and Assurance*. Springer. 2024, s. 47–60.
- [13] Joakim Kävrestad, Martin Gellerstedt, Marcus Nohlberg och Jana Rambusch. "Survey of users' willingness to adopt and pay for cybersecurity training". I: *International Symposium on Human Aspects of Information Security and Assurance*. Springer. 2022, s. 14–23.
- [14] Joakim Kävrestad, Alex Hagberg, Marcus Nohlberg, Jana Rambusch, Robert Roos och Steven Furnell. "Evaluation of contextual and game-based training for phishing detection". I: *Future Internet* 14.4 (2022), s. 104.
- [15] Joakim Kävrestad, Marcus Nohlberg och Steven Furnell. "A taxonomy of SETA methods and linkage to delivery preferences". I: *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 54.4 (2023), s. 107–133.
- [16] Eva Nagyfejeo och Basie Von Solms. "Why do national cybersecurity awareness programmes often fail". I: *International Journal of Information Security and Cybercrime* 9.2 (2020), s. 18–27.
- [17] NCSC. *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*. <https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf>. 2022.
- [18] Norton. *115 cybersecurity statistics + trends to know in 2023*. <https://us.norton.com/blog/emerging-threats/cybersecurity-statistics>. 2022.
- [19] Jason Nurse. *Cybersecurity Awareness*. https://dx.doi.org/10.1007/978-3-642-27739-9_1596 – 1. 2021.
- [20] OECD. *Digital Government Review of Sweden: Towards a Data-driven Public Sector | en | OECD*. <https://www.oecd.org/gov/digital-government/digital-government-review-of-sweden-4daf932b-en.htm>. 2019.
- [21] SYNO. *SYNO - About us*. <https://www.synoint.com/about-us/>. Accessed: 2025-12-12.

7 Appendix A - Tabeller

Tab. 1: Bakgrundsvariabler som användes i studien

Bakgrundsvariabel	Beskrivning och svarsalternativ
Ålder	18–24 år, 25–34 år, 35–44 år, 45–54 år, 55–64 år samt 65–80 år.
Kön	Deltagarna angav upplevt kön.
Utbildningsnivå	Den högsta avslutade utbildningen: ingen avslutad utbildning, grundskola, gymnasium, eftergymnasial utbildning kortare än tre år samt eftergymnasial utbildning tre år eller längre.
Sysselsättning	Deltagarnas huvudsakliga sysselsättning: anställd, egenföretagare, student, pensionär, sjukskriven, arbetslös eller annat.
Bostadsort	Typ av bostadsort baserat på befolkningsstorlek: storstad (minst 300 000 invånare), större stad (100 000–299 999), mellanstor stad (10 000–99 999), mindre stad (1 000–9 999) eller landsbygd (färre än 1 000 invånare).
IT-kompetens	Nybjörjare – har ofta svårt att använda IT och behöver hjälp, Genomsnittlig användare – klarar vardaglig IT men behöver ibland stöd, Avancerad användare – tekniskt intresserad och hjälper ofta andra, Professionell användare – arbetar med, studerar eller är formellt utbildad inom IT.

Tab. 2: Vanligaste tidigare sätt att få cybersäkerhetsinformation (andel av alla respondenter)

Typ av tidigare information	Andel (%)
E-postinformation (t.ex. nyhetsbrev)	38,8
Tips i relevanta situationer (“kontextuellt”)	26,9
Information från vänner/familj	27,7
Digital föreläsning (distans)	24,5
Digitala moduler vid behov (on demand)	25,5
Ingen tidigare exponering alls	15,2

Tab. 3: Största skillnader i tidigare erfarenhet av cybersäkerhetsinformation

Bakgrundsvariabel	Genomsnittlig skillnad mellan grupper (%)
IT-kompetens	20,2
Utbildningsnivå	14,2
Sysselsättning	13,4
Ålder	12,8
Kön	4,2
Bostadsort	5,4

Tab. 4: Hur tidigare cybersäkerhetsinformation upplevdes (1–6 där 6 är högst)

Påstående om tidigare erfarenheter	Medelvärde
Det var relevant för mig	4,32
Det ökade min kunskap	4,26
Det var lätt att delta	4,22
Det var lätt att förstå	4,15
Det gjorde mig intresserad av att agera säkrare	4,13
Det fick mig att ändra beteende	3,78

Tab. 5: Skillnader i upplevelse av tidigare cybersäkerhetsinformation (index)

Bakgrundsvariabel	Skillnad i medelvärde
Utbildningsnivå	1,00
IT-kompetens	0,64
Ålder	0,43
Sysselsättning	0,27
Kön	0,15
Bostadsort	0,29

Tab. 6: Mest föredragna former av cybersäkerhetsinformation (andel av alla respondenter)

Föredraget format	Andel (%)
E-postinformation	23,4
Digital föreläsning (distans)	18,0
Digitala moduler vid behov (on demand)	13,0
Fysisk föreläsning/workshop	11,9
Tips i relevanta situationer ("kontextuellt")	7,1

Tab. 7: Skillnader i föredraget informationsformat

Bakgrundsvariabel	Genomsnittlig skillnad (%)
Ålder	8,8
IT-kompetens	8,1
Sysselsättning	7,9
Utbildningsnivå	7,7
Kön	2,8
Bostadsort	3,6

Tab. 8: När deltagarna helst vill ta del av cybersäkerhetsinformation

Timing	Andel (%)
När jag vill (on demand)	51,5
I relevanta situationer (kontextuellt)	24,0
På schemalagd tid	12,5
Automatiskt med intervall	10,2

Tab. 9: Skillnader avseende timing

Bakgrundsvariabel	Genomsnittlig skillnad (%)
Sysselsättning	8,9
Utbildningsnivå	8,3
Ålder	7,7
IT-kompetens	7,7
Kön	2,2
Bostadsort	5,5

Tab. 10: Föredragen avsändare av cybersäkerhetsinformation

Avsändare	Andel (%)
Myndigheter/stat	31,6
Digitala tjänster (t.ex. bank, plattformar, operatörer)	28,2
Vänner och familj	15,4
IT-företag	12,4

Tab. 11: Tid per vecka som deltagarna är villiga att lägga på cybersäkerhetsinformation

Tid	Andel (%)
Ingen tid alls	5,5
1 minut	8,1
5 minuter	33,0
15 minuter	30,5
30 minuter	17,3
60 minuter eller mer	5,6

Tab. 12: Viktigaste egenskaper hos cybersäkerhetsinformation (1–6 där 6 är viktigast)

Informationen bör vara...	Medelvärde
Kort, men med möjlighet att läsa mer	4,65
På mitt modersmål	4,61
Kortfattad	4,52
Anpassad till min kunskapsnivå	4,49
Fri från tekniskt fackspråk	3,93

8 Appendix B - Tables

Tab. 13: Background variables used in the study

Background variable	Description and response options
Age	18–24 years, 25–34 years, 35–44 years, 45–54 years, 55–64 years, and 65–80 years.
Gender	Participants indicated their perceived gender.
Education level	Highest completed education: no completed education, primary school, upper secondary school, post-secondary education shorter than three years, or post-secondary education three years or longer.
Employment status	Main occupation: employee, self-employed, student, retiree, on sick leave, unemployed, or other.
Type of residence	Based on population size: metropolitan area (at least 300,000 inhabitants), large city (100,000–299,999), medium-sized town (10,000–99,999), small town (1,000–9,999), or rural area (fewer than 1,000 inhabitants).
IT competence	Beginner – often struggles with IT and needs help, Average user – handles everyday IT but sometimes needs support, Advanced user – technically interested and often helps others, Professional user – works with, studies, or is formally educated in IT.

Tab. 14: Most common previous ways of receiving cybersecurity information (percentage of all respondents)

Type of previous information	Percentage (%)
Email information (e.g., newsletters)	38.8
Contextual tips (“in relevant situations”)	26.9
Information from friends/family	27.7
Digital lecture (remote)	24.5
Digital modules on demand	25.5
No previous exposure at all	15.2

Tab. 15: Largest differences in previous experience of cybersecurity information

Background variable	Average difference between groups (%)
IT competence	20.2
Education level	14.2
Employment status	13.4
Age	12.8
Gender	4.2
Type of residence	5.4

Tab. 16: How previous cybersecurity information was perceived (1–6 where 6 is fully agree and 1 is do not agree)

Statement about previous experiences	Mean value
It was relevant to me	4.32
It increased my knowledge	4.26
It was easy to participate in	4.22
It was easy to understand	4.15
It made me interested in acting more securely	4.13
It made me change my behaviour	3.78

Tab. 17: Differences in perception of previous cybersecurity information (index)

Background variable	Difference in mean value
Education level	1.00
IT competence	0.64
Age	0.43
Employment status	0.27
Gender	0.15
Type of residence	0.29

Tab. 18: Most preferred forms of cybersecurity information (percentage of all respondents)

Preferred format	Percentage (%)
Email information	23.4
Digital lecture (remote)	18.0
Digital modules on demand	13.0
Physical lecture/workshop	11.9
Contextual tips (“in relevant situations”)	7.1

Tab. 19: Differences in preferred information format

Background variable	Average difference (%)
Age	8.8
IT competence	8.1
Employment status	7.9
Education level	7.7
Gender	2.8
Type of residence	3.6

Tab. 20: When participants prefer to receive cybersecurity information

Timing	Percentage (%)
On demand (when I want)	51.5
In relevant situations (contextual)	24.0
At scheduled times	12.5
Automatically at intervals	10.2

Tab. 21: Differences regarding preferred timing

Background variable	Average difference (%)
Employment status	8.9
Education level	8.3
Age	7.7
IT competence	7.7
Gender	2.2
Type of residence	5.5

Tab. 22: Preferred sender of cybersecurity information

Sender	Percentage (%)
Government/State authorities	31.6
Digital services (e.g., banks, platforms, operators)	28.2
Friends and family	15.4
IT companies	12.4

Tab. 23: Time per week participants are willing to spend on cybersecurity information

Time	Percentage (%)
No time at all	5.5
1 minute	8.1
5 minutes	33.0
15 minutes	30.5
30 minutes	17.3
60 minutes or more	5.6

Tab. 24: Most important characteristics of cybersecurity information (1–6 where 6 is most important)

The information should be...	Mean value
Short, but with the option to read more	4.65
In my native language	4.61
Concise	4.52
Adapted to my level of knowledge	4.49
Free from technical jargon	3.93