JÖNKÖPING UNIVERSITY
School of Engineering

CYBERCAMPUS SVERIGE

Research Report

Kartläggning av folkbildande initiativ i Cybersäkerhet

Joakim Kävrestad, Viktor Nilsson & Erik Bergström

Jönköping University
School of Engineering
Research Reports No. 12 • 2026

JÖNKÖPING UNIVERSITY
School of Engineering

Research Report

Kartläggning av folkbildande initiativ i Cybersäkerhet

Joakim Kävrestad, Viktor Nilsson & Erik Bergström

Jönköping University
School of Engineering
Research Reports No. 12 • 2026

Kartläggning av folkbildande initiativ i Cybersäkerhet

Research Reports No. 12

© 2026 Joakim Kävrestad, Viktor Nilsson & Erik Bergström

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

Finansiering: Rapporten har finansierats genom bidrag från Cybercampus Sverige.

ISSN 1404-0018

Sammanfattning

Denna rapport kartlägger och analyserar folkbildande cybersäkerhetsinitiativ i Sverige på uppdrag av Cybercampus Sverige. Under studien identifierades 40 initiativ som kartlades utifrån olika indikatorer och målgrupper. Som en delstudie genomfördes även en enkätundersökning där den svenska allmänhetens åsikter, vanor och beteenden inom cybersäkerhet analyserades. Även en tidslinje utvecklades under studien.

Kartläggningen utfördes som en avgränsningsöversikt och använde PRISMA-ScR [28] som generell vägledning. En systematisk datainsamling genomfördes där folkbildande cybersäkerhetsinitiativ identifierades utifrån grå litteratur (t.ex. myndighetsrapporter, utredningar och tekniska rapporter). Därefter identifierades indikatorer samt målgrupper. Datainsamlingen för enkätundersökningen i studien utfördes med hjälp av ett datainsamlingsföretag. Därefter utvecklades även en tidslinje över de identifierade initiativen. Studien visar att en stor andel av dagens aktiva initiativ kan spåra sitt ursprung till tidigt 2020-tal.

Kartläggning och analys av initiativens målgrupper visar att de identifierade målgrupperna har bred tillgång till anpassat material, men med vissa undantag. Personer med begränsade svenskkunskaper, invandrare samt personer med funktionsvariationer har en begränsad täckning. Dessa målgrupper identifierades även som sårbara. Initiativen bedrivs ofta på nationell skala och erbjuder omfattande material med en mer grundläggande inriktning. Materialet bedöms ha goda förutsättningar att nå en stor del av befolkningen. Trots detta visar enkätundersökningen att få personer känner till de identifierade initiativen, samt att de har bristande kännedom om olika informationskällor de kan vända sig till. Resultaten indikerar att den största barriären för att stärka allmänhetens cyberkunskaper inte är den befintliga tillgängligheten av folkbildande material. Utmaningen ligger snarare i att nå ut till folket, hålla sig kvar i deras medvetande och få dem att använda befintligt material. Enkätundersökningen visar, i linje med tidigare forskning, att detta är ett särskilt stort problem för grupper med lägre kunskapsnivå.

Rapporten drar slutsatsen att vissa sårbara målgrupper behöver ett större utbud av anpassat material medan övriga målgrupper har en godtagbar täckning. Studien bedömer att ett ökat fokus på att nå allmänheten med befintligt material är ett effektivare sätt att öka allmänhetens kunskap om cybersäkerhet än att utveckla ytterligare material.

Studien har genomförts med finansiering från Cybercampus Sverige.

Innehållsförteckning

Sammanfattning **iii**

1 Inledning **1**
1.1 Arbetssätt . . . 1

2 Analys och resultat **5**
2.1 Kartläggning av initiativ. . . . 5
2.2 Analys - Målgrupper . . . 7
2.3 Enkätstudie . . . 10
2.3.1 Beskrivning av respondenterna . . . 10
2.3.2 Allmänhetens kunskap . . . 11
2.3.3 Beteende och attityd . . . 13
2.4 Analys - Tidslinje . . . 19
2.5 Resultatsammanfattning . . . 20

3 Diskussion och slutsats **21**
3.1 Slutsats . . . 21

4 Begränsningar och vidare studie **23**

A Appendix A - Diagram **25**

B Appendix B - Tabeller **29**

C Appendix C - Enkät **37**

1 Inledning

Den ökande digitaliseringen i samhället innebär att en allt större del av människors vardag är digital, bland annat bankärenden, kommunikation och arbete. Detta bidrar också till ett ökat antal attackvektorer för cyberbrott. Europol [9] förklarar att nätbedrägerier är det snabbast växande området inom organiserad brottslighet. Samtidigt fortsätter ransomware att vara ett stort hot, och nätverk som handlar och sprider material som visar sexuella övergrepp mot barn ökar i omfattning. Ett utökat hot från cyberstödda brott gör det viktigare för allmänheten att utrustas med kunskap och färdigheter för att skydda sig.

Europeiska kommissionen rapporterar år 2022, genom ”Digital Economy and Society Index” [8] att Sverige är ett av EU:s mest digitaliserade länder. Eftersom en hög grad av digitalisering ökar riskerna och den potentiella skadan från cyberbrott, blir det viktigt att utveckla svenska medborgares försvar med folkbidning som en nyckelaktivitet. Yeo LH m.fl. [31] observerade att nätfiskebedrägeri var den vanligaste anledningen till att patienters journaldata kom att äventyras. Tamboly m.fl. [27] förklarar att social engineering (social manipulation) är en stor drivkraft bakom incidenter med hög allvarlighetsgrad. Dessa attackvektorer utnyttjar människor snarare än tekniska brister, vilket stärker behovet av utbildning för allmänheten. Phishing, en typ av social engineering, identifieras även som den vanligaste attackvektorn i inledningen av en cyberattack [20, 29].

Åtgärder för att skapa en säkrare digital miljö har genomförts både på EU-nivå och nationell nivå, bland annat genom NIS2-direktivet [19] och cybersäkerhetslagen [6]. Flera aktörer i Sverige arbetar med att utbilda allmänheten i cybersäkerhet. Trots detta saknas en samlad översikt över vilka initiativ som finns, deras målgrupper och eventuella luckor.

Syftet med studien var därför att kartlägga befintliga folkbildande cybersäkerhetsinitiativ i Sverige. Ett delmål var även att identifiera potentiella brister och luckor i folkbildande material. Kartläggningen kunde därmed bidra till en mer ändamålsenlig och effektiv resursfördelning. Studien omfattade även en enkätundersökning av allmänhetens kunskap, beteenden och medvetenhet om digital säkerhet, med syfte att ge en bild av allmänhetens upplevelser. Studien utfördes som ett utredningsuppdrag via Cybercampus där syftet var att undersöka om det fanns ett nationellt behov av folkbildande insatser från Cybercampus. Om ett sådant behov konstaterades skulle studien även undersöka vilken roll Cybercampus eventuellt kunde ha i det svenska landskapet för folkbildande insatser inom cybersäkerhet. Studien genomfördes med finansiering från Cybercampus Sverige.

1.1. Arbetssätt

Studien genomfördes som en översiktstudie med ”The Preferred Reporting Items for Systematic reviews and Meta-Analyses - Scoping Reviews” [28] som vägledning. Arbetet inleddes med en systematisk datainsamling med syfte att identifiera olika folkbildande cybersäkerhetsinitiativ. För att åstadkomma detta användes en sökmatris där söksträngar och resultaten av dessa dokumenterades. AI-modeller användes som stöd för att generera söksträngar. Efter detta användes söksträngarna för att kartlägga initiativ. Datainsamlingsprocessen dokumenterades i en söklogg där datum, söksträng,

databas/sökmotor, antal träffar och identifierade initiativ registrerades. Processen ägde rum mellan första och åttonde april 2026. Majoriteten av datainsamlingen genomfördes med hjälp av sökmotorer (Google, DuckDuckGo) för att undersöka grå litteratur. Grå litteratur är publikationer som produceras utanför traditionella vetenskapliga publiceringskanaler och som inte nödvändigtvis genomgår peer review (t.ex. myndighetsrapporter, utredningar, standarder och tekniska rapporter). De första 100 källdokumenten per sökning granskades. Viss litteratursökning genomfördes även i databaser hos Myndigheten för civilt försvar [17] och Myndigheten för digital förvaltning [7]. Totalt utfördes 34 olika sökningar och 193 källdokument identifierades. För att göra identifieringen av potentiella initiativ effektivare användes även AI-verktyg för att granska om en källa eventuellt kunde räknas som ett folkbildande cybersäkerhetsinitiativ. De identifierade initiativen granskades därefter manuellt i en screeningprocess.

I screeningen granskades potentiella initiativ, som uteslöts om de inte uppfyllde de förutbestämda kriterierna. För att inkluderas krävdes bland annat att de riktade sig till svenska medborgare och att de bedömdes vara aktiva vid tidpunkten för datainsamlingen. Det säkerställdes även att de kunde betraktas som initiativ. Företag som exempelvis erbjöd utbildningar i cybersäkerhet som en tjänst eller drevs i kommersiellt syfte sorterades därför bort. Initiativ som verkade globalt men som annars uppfyllde kriterierna togs även bort eftersom studien fokuserade på initiativ som var direkt inriktade mot Sverige. Under screeningen dokumenterades alla initiativ som uppfyllde kriterierna, och eventuella dubletter togs bort.

För att undersöka ytterligare potentiella folkbildande cybersäkerhetsinitiativ användes snowballing, där tidigare kartlagda initiativ användes för att identifiera ytterligare initiativ som kunde inkluderas i studien. Dessutom genomfördes en enkätstudie där där yrkesverksamma ombads att besvara frågan om vilka initiativ de känner till. Enkäten spreds via LinkedIn, Cybercampus och Cybdernoden. Initiativ som identifierades i denna process gick sedan igenom samma screeningprocess som tidigare nämnts.

De identifierade initiativen kartlades med fokus på vilka målgrupper de adresserade samt kvalitetsindikatorer. Detta resulterade i framtagandet av olika bilagor, diagram och tabeller som sammanställde relevant data på ett tydligt och överskådligt sätt. En fullständig lista över samtliga identifierade initiativ återfinns i tabell B.1 i appendix B.

Som en delstudie genomfördes även en enkätstudie i syfte att ge en översikt över den svenska allmänhetens åsikter, vanor och behov. Syftet med enkäten var att kunna jämföra bilden av tillgängliga initiativ med allmänhetens uppfattning om tillgång till cybersökerhetsinformation. Enkätundersökningen presenteras närmare i kapitel 2.3.

Under den senare delen av projektet utvecklades ytterligare en delstudie där en tidslinje skapades. Delstudien genomfördes genom att samla in data om aktiviteten i de identifierade initiativen. Under datainsamlingen kartlades tre olika variabler för varje identifierat initiativ:

- Tidigast tidpunkten då initiatives fanns synligt online.
- Senaste cybersäkerhetsrelaterade aktiviteten.
- Senaste uppdateringen av hemsidan.

För att åstadkomma detta användes ett antal metoder. När den tidigaste aktiviteten dokumenterades användes en kombination av Internet Archives Wayback Machine[1] samt granskning av initiativets hemsida. Om inget pålitligt resultat kunde hittas användes webbplatsen WhoIs för att identifiera när domännamnet registrerades, vilket då användes som indikator på den tidigaste aktiviteten. WhoIs[2] användes vid ett tillfälle. För att dokumentera den senaste aktiviteten samt den senaste uppdateringen av webbsidan användes också Wayback Machine, samt en granskning av webbplatsens webbplatskarta för att identifiera den senaste redigeringen. Även den senaste cyberrelaterade närvaron i sociala medier dokumenterades. Efter datainsamlingen bearbetades informationen för vidare analys.

[1] https://web.archive.org/
[2] https://who.is/

Sammanfattningsvis användes en semiautomatiserad process där automatiseringsverktyg användes för att samla in och bearbeta data från identifierade källdokument med syfte att sortera ut initiativ. Därefter genomfördes en manuell kvalitetskontroll av de identifierade initiativen för att verifiera materialets korrekthet. De insamlade initiativen sammanställdes i två dataset, vilka tillsammans låg till grund för den översiktliga analysen av Sveriges landskap av folkbildande initiativ inom cybersäkerhet. Studien kompletterades senare med två delstudier: en tidslinje och en enkätundersökning.

2

Analys och resultat

Följande avsnitt presenterar resultatet av projektets delstudier samt den analys som genomförts utifrån dessa.

2.1. Kartläggning av initiativ

Under sökningsprocessen identifierades 40 unika initiativ som på olika sätt bidrar till att öka cybersäkerhetsmedvetenheten hos den svenska befolkningen. Dessa listas i appendix B, tabell B.1. Följande avsnitt presenterar en analys av de 40 identifierade initiativen i syfte att ge en övergripande bild av utbudet avseende folkbildande insatser i cybersäkerhet i Sverige.

Inledningsvis kartlades initiativens räckvidd med fokus på avsedd målgrupp (se tabell 2.1). En hög räckvidd visar på en ambition att nå flera eller breda målgrupper. Analysen visade att majoriteten av initiativen bedömdes ha en hög räckvidd. Detta tyder på att majoriteten av initiativen hade ett brett fokus, eftersom de syftar till att nå en bred målgrupp.

Räckvidd	Låg	Medel	Hög
Antal	4	11	25
Procent	10 %	27,5 %	62,5 %

Tabell. 2.1: Räckvidd av identifierade initiativ. Visar antal och procent av de identifierade initiativen.

Den geografiska räckvidden (se tabell 2.2) visar geografiska begränsningar hos de identifierade initiativen. Initiativen arbetade främst på en nationell nivå (77,5 %) vilket indikerades av en digital närvaro på svenska. De lokala och regionala initiativen bestod som regel av olika evenemang med en geografisk begränsning.

Geografisk spridning	Lokal	Regional	Nationell	Internationell
Antal	2	4	31	3
Procent	5 %	10 %	77,5 %	7,5 %

Tabell. 2.2: Geografisk räckvidd av identifierade initiativ. Visar antal och procent av de identifierade initiativen.

Finansieringen av de folkbildande cybersäkerhetsinitiativen varierade, men offentlig finansiering var vanligast (se tabell 2.3). Även samverkan mellan flera aktörer och ideell finansiering var vanliga finansieringsformer. En mindre andel av initiativen finansierades av privata aktörer (17,5 %), medan vissa finansierades av EU och en ytterst liten andel var självfinansierade. Resultaten visade att statliga myndigheter hade en central roll i finansieringen och driften av de identifierade initiativen.

Finansiering	Självfinansierad	Privat	Samverkan	Ideell	Offentlig	EU
Antal	2	7	14	8	23	4
Procent	5 %	17,5 %	35 %	20 %	57,5 %	10 %

Tabell. 2.3: Fördelning av olika finansieringsmetoder inom de identifierade initiativen. Visar antal och procent av de identifierade initiativen.

De flesta initiativ erbjöd grundläggande information och riktade sig till användare med lägre kunskapsnivå (se tabell 2.4). Detta tydde på att initiativens primära fokus låg på att öka allmänhetens medvetenhet. En mindre men betydande andel av initiativen riktade sig till användare med medel- eller avancerad kunskapsnivå. Dessa initiativ arbetade ofta med att koordinera allmän utbildning på företag eller att utveckla och stärka befintlig kompetens genom utbildning, projekt och evenemang.

Kunskapsnivå	Grundläggande	Medel	Avancerad
Antal	27	15	8
Procent	67,5 %	37,5 %	20 %

Tabell. 2.4: Identifierad kunskapsnivå av material och resurser som distribueras av initiativ. Visar antal och procent av de identifierade initiativen.

Granskningen av initiativen visade att omfånget av det material som erbjöds varierade (se tabell 2.5). Hälften av cybersäkerhetsinitiativen bedömdes erbjuda ett mellanliggande omfång. Detta kunde tolkas som att initiativen vanligtvis erbjöd information som täckte flera aspekter av cybersäkerhet, men inte var tillräckligt omfattande för att kunna ge användare en helhetsbild av området.

Omfång av material	Litet	Medel	Stort
Antal	6	20	14
Procent	15 %	50 %	35 %

Tabell. 2.5: Omfång som erbjuds av initiativen. Visar antal och procent av de identifierade initiativen.

Användarcentrering inom initiativen bedömdes överlag som hög, vilket framgår av tabell 2.6. Flera initiativ använde språk och upplägg som var anpassade efter sin målgrupp. Det finns en stor variation i hur olika personer vill ha information förmedlad och överlag läggs stor vikt vid enkel och tydlig information som även upplevs som relevant [13]. Detta indikerar att användarcentrering har en viktig roll i utbildningen av allmänheten.

Användarcentrering	Låg	Medel	Hög
Antal	3	12	25
Procent	7,5 %	30 %	62,5 %

Tabell. 2.6: Klassificering av hur anpassat material är för användare inom initiativen. Visar antal samt procent av de identifierade initiativen.

Av de identifierade initiativen erbjöd majoriteten material utan kostnad. Resultaten från en tidigare studie [15] visar att villigheten att delta i cybersäkerhetsträning är betydligt större när tjänsten är gratis (se tabell 2.7). Detta tyder på att kostnadsfri träning har bättre förutsättningar att nå ut till allmänheten.

Kostnad	Gratis	Delvis	Betald
Antal	32	6	2
Procent	80 %	15 %	5 %

Tabell. 2.7: Användarkostnad för de identifierade initiativen. Visar antal samt procent av de identifierade initiativen.

Graden av anpassningsbarhet hos samtligt material varierade mellan initiativen. En jämn fördelning mellan de tre kategorierna i kartläggningen observerades (se tabell 2.8). Majoriteten av materialet som initiativen erbjöd kunde anpassas på något sätt. Däremot är nästan hälften av dessa bara delvis anpassningsbara, och närmare en tredjedel av initiativen erbjöd inget anpassningsbart material. Anpassningsbart material fanns, men i begränsad omfattning, vilket försvårade återanvändning, spridning och lokal anpassning.

Anpassningsbart material	Ja	Delvis	Nej
Antal	14	13	13
Procent	35 %	32,5 %	32,5 %

Tabell. 2.8: Visar om innehållet kan anpassas efter olika behov och målgrupper. Visar antal samt procent av de identifierade initiativen.

2.2. Analys - Målgrupper

Under studien identifierades 38 olika målgrupper som organiserades i 10 bredare målgruppskategorier. Data sammanställdes i tabeller, där målgrupperna sorterades efter antalet initiativ som hade en specifik målgrupp. Även andelen av de 40 identifierade initiativen som hade respektive målgrupp dokumenterades. Notera att flera initiativ genomgående adresserar flera målgrupper och att den totala andelen initiativ i varje kategori därför överstiger 100 %, se exempelvis tabell 2.10.

Flera tidigare studier visar att ålder har en signifikant effekt på cybersäkerhetsbeteende och behov av säkerhetsinformation [3, 5, 13, 30]. Kartläggningen visade på en spridning i vilka åldrar som adresseras av existerande initiativ (se tabell 2.9). Analysen visade att 75 % av de folkbildande cybersäkerhetsinitiativen riktade sig mot vuxna (18–64 år). Då denna grupp utgör ett mycket brett åldersintervall var resultatet någorlunda förväntat. Cirka 38 % riktade sig till äldre. Många av initiativen hade en tydlig koppling till denna åldersgrupp, eftersom de ofta riktade sig till pensionärer. 22,5 % riktade sig till barn mellan 7–17 år och endast två initiativ (5 %) identifierades för barn mellan 0–6 år. Analysen ges stöd för att det finns initiativ som tillsammans täcker åldrarna 7+ väl, men det ska tilläggas att en merpart av initiativen adresserar breda målgrupper utan tydlig anpassning av material till olika åldrar.

Målgrupp	Barn (0-6)	Barn (7-17)	Vuxna (18-64)	Äldre (65+)
Antal	2	9	30	15
Procent	5 %	22,5 %	75 %	37,5 %

Tabell. 2.9: Andel av identifierade initiativ som riktade sig mot en specifik åldersgrupp. Visar antal samt procent av de identifierade initiativen.

Utbildningsnivå är en bakgrundsfaktor med en tydlig påverkan på cybersäkerhetsrelaterat beteende [11, 13]. Analysen av folkbildande cybersäkerhetsinitiativ visade en relativt jämn fördelning mellan de tre olika utbildningsnivåerna (se tabell 2.10). Lägst andel, 42,5 % , ansågs rikta sig mot personer med gymnasial utbildning eller lägre. 60 % riktade sig till personer med eftergymnasial utbildning på 3 år eller kortare och 50 % till eftergymnasial utbildning längre än 3 år.

Målgrupp	Gymnasial utbildning eller lägre	Eftergymnasial utbildning	Eftergymnasial utbildning längre än 3 år
Antal	17	24	20
Procent	42,5 %	60 %	50 %

Tabell. 2.10: Andel av identifierade initiativ som riktade sig till en viss utbildningsnivå. Visar antal samt procent av de identifierade initiativen.

Analysen av data för vilka IT-kompetensnivåer olika initiativ riktade sig mot visade att majoriteten fokuserade på användare med låg IT-kompetens (70 %), medan 47,5 % riktade sig mot en mellanliggande kompetens, och 27,5 % mot en hög. Data visade att antalet initiativ gradvis minskade med stigande IT-kompetens (se tabell 2.11).

Målgrupp	Låg	Medel	Hög
Antal	28	19	11
Procent	70 %	47,5 %	27,5 %

Tabell. 2.11: Andel av identifierade initiativ som riktade sig till personer med viss IT-kompetens. Notera: ett initiativ kan täcka flera kompetensnivåer. Visar antal samt procent av de identifierade initiativen.

Granskningen av de identifierade initiativens målgrupper inom underkategorin sysselsättning visade att 67,5 % av de identifierade initiativen riktade sig mot arbetande (se tabell 2.12). Detta utgjorde den klart största gruppen och skillnaderna mellan den näst största gruppen, pensionärer (32,5 %), var tydliga. Bland utbildningsformerna riktade sig 11 initiativ (27,5 %) mot gymnasial-, vuxen- eller yrkesvuxenutbildning samt postgymnasial utbildning. Därefter riktade sig 22,5 % av initiativen till grundskolan medan endast 15 % av initiativen identifierades som riktade sig mot personer utanför arbetsmarknaden.

Målgrupp	Arbetande	Arbetslös	Pensionär	Grundskola	Gymn/vux/ yrkesvux	Post-gymnasial (Lärosäten/YH)
Antal	27	6	13	9	11	11
Procent	67,5 %	15 %	32,5 %	22,5 %	27,5 %	27,5 %

Tabell. 2.12: Andel identifierade initiativ med en specifik sysselsättning som målgrupp. Visar antal samt procent av de identifierade initiativen.

En relativt liten andel av initiativen identifierades som att ha en specifik storlek på bosättningsområdet som målgrupp. De initiativ som bedömdes rikta sig mot dessa kategorier var initiativ med fysisk närvaro som kunde kopplas till en specifik plats. Analysen visade en jämn fördelning av initiativ. Dessa var vanligtvis olika evenemang eller föreningar med fysisk närvaro på en eller flera platser. Resultaten i tabell 2.13 visar att städer med mellan 100 000 och 299 999 hade den största andelen riktade initiativ (25 %), medan lantliga bostadsorter (cirka 12,5 %) var minst representerade i projektets dataset.

Analysen av de olika boendesituationerna visade en jämn fördelning (se tabell 2.14). 40 % av initiativen hade ensamboende som målgrupp, 35 % för boende med partner och 37,5 % för familjeboende som målgrupp. Notera att den största majoriteten av initiativen identifierades implicit som att ha dessa som en indirekt målgrupp, bland annat genom informationsresurser till föräldrar osv. Resultaten visade ingen tydlig snedfördelning mellan de olika boendeformer som initiativen riktade sig till.

Målgrupp	Storstads-område (300 000>)	Stad (100 000-299 999)	Stad (10 000-99 999)	Stad (1 000-9 999)	Lantlig (<1 000)
Antal	7	10	7	6	5
Procent	17,5 %	25 %	17,5 %	15 %	12,5 %

Tabell. 2.13: Visar andelen initiativ med en specifik storlek på bosättningsområde som målgrupp. Visar antal samt procent av de identifierade initiativen.

Målgrupp	Ensam	Partner	Familj
Antal	16	14	15
Procent	40 %	35 %	37,5 %

Tabell. 2.14: Andel av identifierade initiativ som riktade sig mot en specifik boendesituation. Visar antal samt procent av de identifierade initiativen.

7,5 % av initiativen identifierades som riktade till invandrare och personer med begränsade kunskaper i svenska (se tabell 2.15). När initiativen gav stöd till dessa målgrupper framgick detta bland annat genom att de erbjöd information på vanligt förekommande modersmål samt text på lättläst svenska.

Målgrupp	Nyanlända / Invandrare	Personer med bristande svenskkunskaper
Antal	3	3
Procent	7,5 %	7,5 %

Tabell. 2.15: Andel av initiativen som riktade sig till invandrare och personer med begränsade svenskkunskaper. Visar antal samt procent av de identifierade initiativen.

En mycket begränsad andel av de identifierade initiativen hade explicit dokumenterade insatser för att anpassa materialet specifikt till kognitiva eller neuropsykiatriska funktionsnedsättningar (tabell 2.16). Inga av initiativen identifierades explicit ha personer med sensoriska eller motoriska funktionsnedsättningar som målgrupp. Däremot noterades det att flera av initiativen erbjöd material som inte hade tagits fram specifikt för denna målgrupp, men som kan fungera väl som material för personer med en lättare neuropsykologisk eller kognitiv funktionsnedsättning. Trots detta bedömdes tillgängligheten till resurser för dessa målgrupper vara mycket begränsad.

Målgrupp	Kognitiv	Neuropsykiatrisk	Sensorisk	Motorisk
Antal	1	1	0	0
Procent	2,5 %	2,5 %	0 %	0 %

Tabell. 2.16: Andel av identifierade initiativ som riktade sig mot en specifik klassificering av funktionsnedsättning. Visar antal samt procent av de identifierade initiativen.

NIS2-direktivet ökar kraven på organisationer inom flera sektorer att upprätthålla en högre standard för cybersäkerhet [19]. Direktivet har genomförts i svensk rätt genom cybersäkerhetslagen [6]. Folkbildande resurser riktade mot dessa organisationer får då en viktigare roll genom att utbildningen av personal och ledning ökas. Studier uppmärksammar även att arbetsplatsen påverkar medvetenheten om cybersäkerhet [13, 23, 26]. För att förenkla analysen delades arbetsplatser in i den offentliga och den privata sektorn.

Analysen av folkbildningsinsatser som riktade sig mot den offentliga sektorn visade att hälften av de identifierade initiativen hade kommuner som målgrupp, följt av regioner och statliga myndigheter på 22,5 % och därefter högre utbildning på 15 % (tabell 2.17). Fördelningen stämde generellt överens

med antalet anställda i den offentliga sektorn inom kommuner, regioner och statliga myndigheter utifrån SCB:s statistik för 2026 [24]. Det fanns dock en viss överrepresentation av kommuner, eftersom de utgör en större andel av de anställda än vad som representeras inom de identifierade initiativen, medan högre utbildning inte representeras i statistiken.

Målgrupp	Utbildning (lärosäten)	Kommuner	Regioner	Statliga myndigheter
Antal	6	20	9	9
Procent	15 %	50 %	22,5 %	22,5 %

Tabell. 2.17: Andel av identifierade initiativ som riktade sig till en specifik offentlig sektor. Visar antal samt procent av de identifierade initiativen.

Inom den privata sektorn existerar viss överrepresentation av små och medelstora företag: 42,5 % av initiativen täcker dessa, medan mikroföretag och stora företag med över 250 anställda båda täcktes av 32,5 % av initiativen (tabell 2.18). Detta kan relateras till att gruppen Små och medelstora företag tillsammans sysselsätter flest personer på den privata arbetsmarknaden [25].

Målgrupp	Mikroföretag (<10)	Småföretag (10-49)	Medelstora företag (50-249)	Storföretag (250>)
Antal	13	17	17	13
Procent	32,5 %	42,5 %	42,5 %	32,5 %

Tabell. 2.18: Andel av identifierade initiativ riktade mot en specifik storlek på företag. Visar antal samt procent av de identifierade initiativen.

2.3. Enkätstudie

Analysen av existerande initiativ kompletterades med en enkätstudie i syfte att undersöka svenskars uppfattning och kännedom om de folkbildande insatserna. Totalt besvarades enkäten av 1186 personer och 186 svar filtrerades bort i kvalitetskontroll. Totalt 1000 unika svar ingick i analysen. Datainsamlingen skedde med stratifierat urval, främst med hjälp av webbpaneler, för att nå en bred representation av svenskar. Datainsamlingen genomfördes med hjälp av datainsamlingsföretaget Syno[1]. Den genomsnittliga svarstiden var cirka 4,88 minuter med en median på 2,15 minuter. Respondenterna svarade på 13 frågor, varav 6 inkluderade svarsalternativ i fritext. Samtliga enkätfrågor återfinns i Appendix C.

2.3.1. Beskrivning av respondenterna

Av de svarande uppgav 49,4 % att de identifierade sig som män, 50,1 % kvinnor, 0,3 % ville ej uppge och 0,2 % angav annat. Eftersom de två sistnämnda svarsalternativen endast inkluderande tre respektive två respondenter beaktades de inte i analysen. De svarande var också jämt spridda i ålder.

Respondenterna angav sin högsta avslutade utbildning och resultaten visade att 5,6 % svarade “grundskola/motsvarande”, 40,3 % “gymnasium/motsvarande”, 17,2 % “eftergymnasial utbildning kortare än 3 år” och 36,4 % “eftergymnasial utbildning minst 3 år”. Endast fem respondenter (0,5 %) svarade att de saknade en avslutad utbildning. Detta bedömdes vara en för liten urvalsstorlek för att ge underlag för vidare analys. Majoriteten av respondenterna svarade att de var anställda (59,5 %), följt av pensionärer (15,9 %), studerande (8,9 %), arbetssökande (7,7 %), egenföretagare (4,5 %), sjukskrivna (2,1 %) och annat (1,4 %). De senare två av dessa bedömdes ha en för liten urvalsstorlek för att ge underlag för analys då det lilla delurvalet kunde minska resultatens tillförlitlighet. Vidare angav respondenterna vilken enhet de huvudsakligen använde för att interagera med digitala medier. Majoriteten (81,6 %) använde huvudsakligen mobiltelefon, medan 13,2 % använde dator och 5,2 % surfplatta.

[1] https://synoint.com/

2.3.2. Allmänhetens kunskap

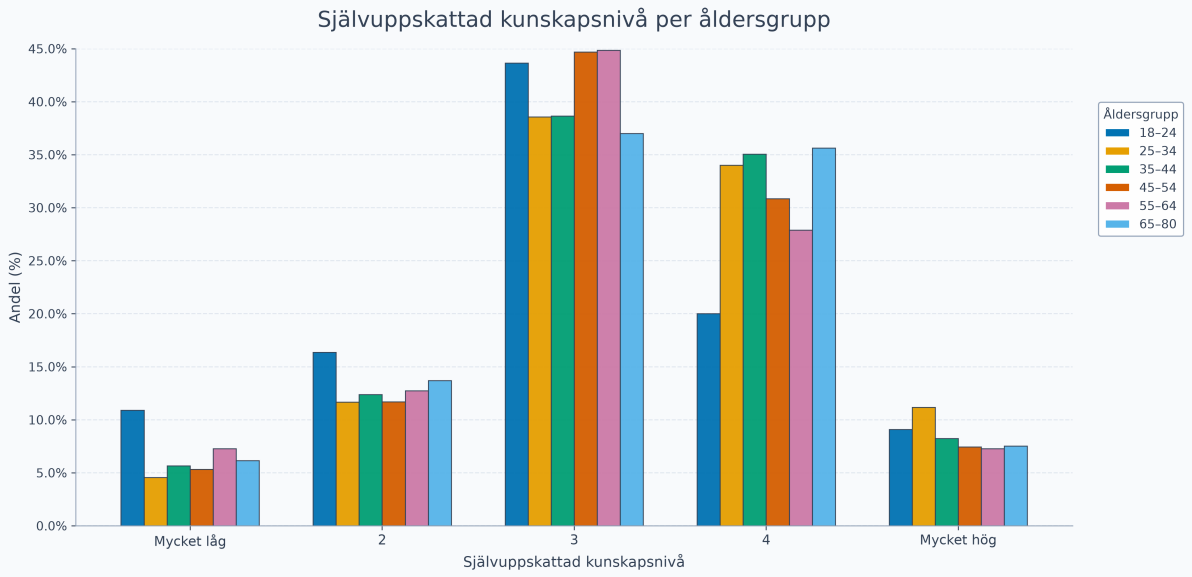
Hur skulle du bedöma din kunskap om cybersäkerhet?

Respondenterna fick inledningsvis uppskatta sin egen cybersäkerhetskunskap och angav i genomsnitt en försiktig men positiv bedömning av sin egen kunskapsnivå inom cybersäkerhet, vilket framgår av tabell 2.19.

Svarsalternativ	1-Mycket låg	2	3	4	5-Mycket hög
Antal	63	128	411	313	85
Procent	6,30 %	12 %	41,1 %	31,3 %	8,5 %

Tabell. 2.19: Deltagare självskattning av sin kunskap om cybersäkerhet.

Korsanalys utifrån åldersgrupper visade att det fanns viss variation mellan grupperna (se figur 2.1). I samtliga grupper bedömde respondenterna oftast att de hade en medelnivå av kunskap om cybersäkerhet. Samtidigt observerades en trend där vissa grupper hade en något högre självbedömd kunskapsnivå. Respondenter i åldersgruppen 18–24 år självuppskattade att de jämförelsevis hade mindre kunskap, medan deltagare i åldersgruppen 25–34 år samt 35–44 år hade högre självförtroende för sina kunskaper än de övriga grupperna. Självbedömd kunskapsnivå sjönk sedan gradvis tills åldersintervallet 65–80 år, där självbedömningen blev något mer positiv.

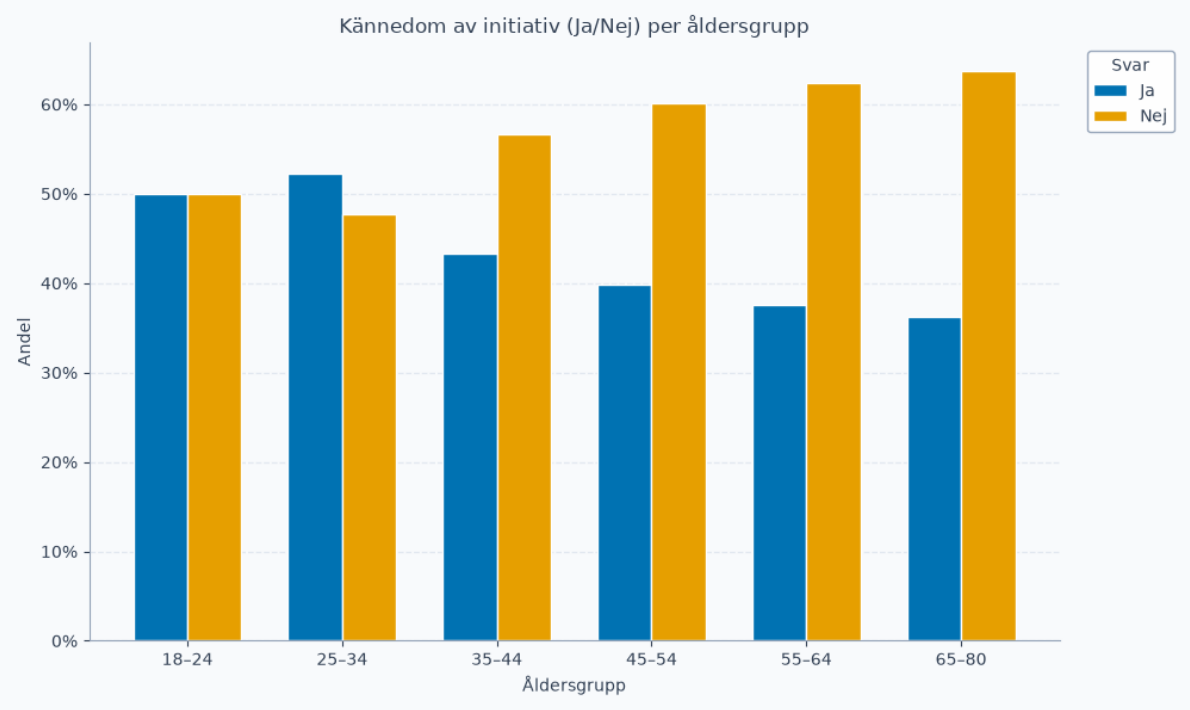


Figur. 2.1: Diagram över självrapporterad kunskapsnivå inom cybersäkerhet. Visar procenten av populationen i åldersgruppen som har rapporterat en specifik kunskapsnivå.

Vidare visade korsanalysen att män i genomsnitt hade en något högre självuppskattning av sin kunskapsnivå än kvinnor. Respondenter med eftergymnasial utbildning visade också en mer positiv bedömning jämfört med deltagare med gymnasial eller lägre utbildning. Spridningen av självuppskattad kunskapsnivå visade en större variation bland personer med grundskola eller motsvarande som högsta utbildning jämfört med övriga utbildningsnivåer. Korsanalysen utifrån respondenternas sysselsättning visade att majoriteten hade en något positiv genomsnittlig bedömning av sin kunskapsnivå. Ett undantag var arbetssökande, som hade en något negativ genomsnittlig bedömning. Egenföretagare utmärkte sig även från andra grupper, då de visade en högre självbedömd kunskapsnivå än samtliga andra grupper. Cirka 24 % av egenföretagarna uppskattade att de hade en mycket hög kunskapsnivå. Ytterligare en korsanalys utifrån den huvudsakligen använda enheten visade även här att alla grupper hade en något positiv genomsnittlig självbedömning. Däremot var datoranvändare mer positiva än andra.

Har du hört talas om något/några initiativ som informerar allmänheten om cybersäkerhet?

56,8 % av respondenterna angav att de inte kände till något folkbildande cybersäkerhetsinitiativ (se figur 2.2). Respondenterna som svarade “Ja” ombads att i fritext benämna det initiativ som de kände till. Fritextsvaren granskades manuellt och svar som inte nämnde något konkret exkluderades, vilket innebar att cirka 28 % återstod. Därefter exkluderades svar som inte hänvisade till relevanta myndigheter, aktörer eller initiativ. Efter detta återstod cirka 18 % av respondenternas svar. Slutligen observerades det att endast 3 % av enkätens respondenter kunde nämna ett initiativ utifrån samma kriterier som användes inom denna studie.



Figur. 2.2: Diagram som visar kännedom om initiativ i förhållande till åldersgrupper.

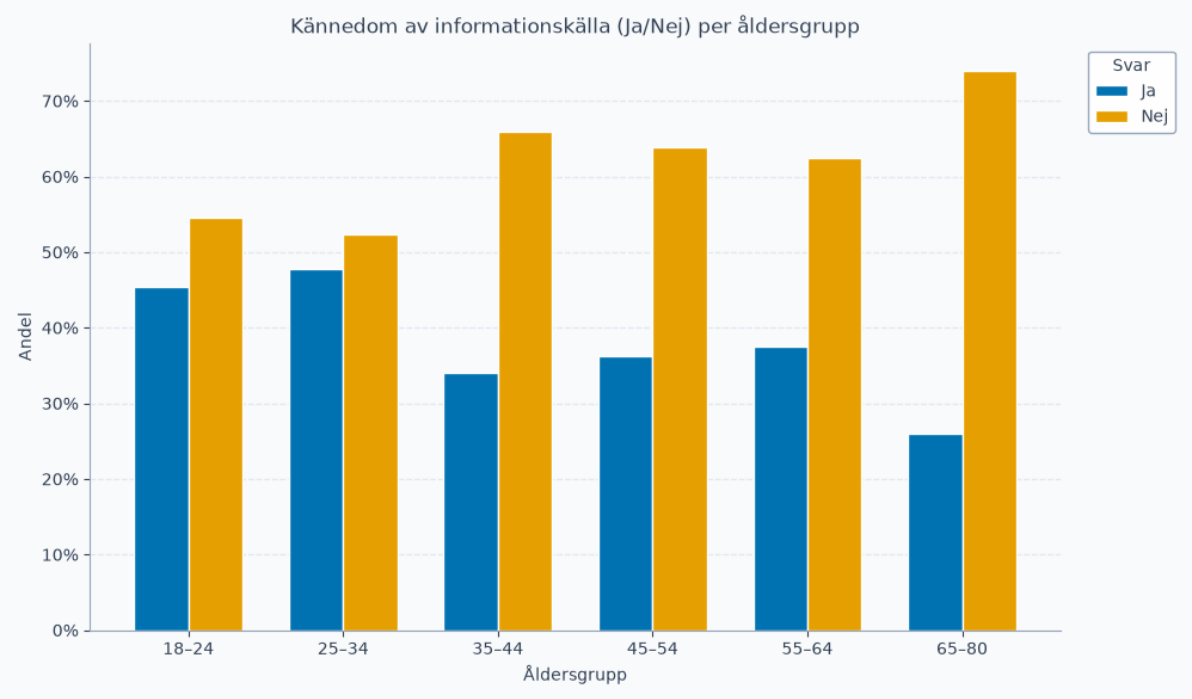
Korsanalyser visade att specifika grupper var mer benägna att svara “Ja”. Omkring hälften, 49,2 % av männen uppgav att de kände till minst ett initiativ jämfört med 37,1 % av kvinnorna. Ett samband mellan åldersgrupper och kännedom om initiativ observerades. Åldersgruppen 25–34 var den enda gruppen där respondenterna angav ett större antal “ja” än “nej”. Kännedom om olika initiativ minskade sedan successivt med ökad ålder, vilket kan observeras i figur 2.2. Korsanalys utifrån sysselsättning visade att pensionärer hade lägst kännedom om olika cybersäkerhetsinitiativ (36,5 %). Respondenter som huvudsakligen använde surfplatta visade också lägre kännedom jämfört med de övriga grupperna. Enkätresultatet visade att äldre respondenter använde surfplattor som huvudsaklig enhet i större proportion, vilket möjligen kunde förklara sambandet. Vidare visade korsanalysen även ett tydligt samband mellan självuppskattad kunskapsnivå och kännedom om olika initiativ. Andelen deltagare som svarade ’Ja’ ökade successivt med den självskattade kunskapsnivån, från cirka 11 % till 72 %.

Känner du till någonstans du kan vända dig om du vill ha information om cybersäkerhet?

Majoriteten av respondenterna i enkätundersökningen (62,2 %) svarade att de inte kände till någon informationskälla som de kunde vända sig till (se figur 2.3). Respondenter som svarade “Ja” angav sedan i fritext kända informationskällor. Av de cirka 38 % som svarade detta återstod cirka 33 % när oseriösa fritextsvar exkluderades. Vid restriktivare filtrering, där informationsverktyg såsom sökmotorer togs bort, återstod cirka 29 %. Analys av fritextsvaren visade att respondenterna främst

angav myndigheter och offentliga organisationer som informationskällor, vilket förekom i cirka 43 % av fritextsvaren. Övriga kategorier som vanligtvis förekom inkluderade: sökning via internet (cirka 16 %), kommersiella företag (cirka 14 %), arbetsplatsen (cirka 12 %) och personliga kontakter (cirka 11 %). Resten av de kategorier som identifierades översteg aldrig 10 %. Notera att respondenterna hade möjlighet att ange flera olika informationskällor, vilket innebär att procentsatserna inte summerar till 100 %.

Korsanalys av resultaten visade ett liknande mönster som i föregående fråga. Kvinnor svarade “Nej” något oftare (68,6 %) jämfört med män (56,3 %). Pensionärer hade lägst kännedom, 28,3 %, medan anställda hade den högsta motsvarande andelen 46,2 %. En större skillnad utifrån korsanalys med huvudsakligt använda enheter observerades i denna fråga jämfört med föregående: datoranvändare (53,8 %), mobilanvändare (35,9 %) och surfplatteanvändare (26,9 %). I samtliga åldersgrupper var ”Nej” det vanligaste svaret, men marginalerna mellan antalet ”Ja/Nej” varierade mellan grupperna. Figur 2.3 visar att yngre åldersgrupper har en mindre marginal än äldre. Minskningen av kännedom skedde däremot inte gradvis, utan i tydliga steg mellan vissa åldersgrupper. Likt den tidigare frågan ökade andelen respondenter som svarade “Ja” gradvis vid högre självbedömd kunskapsnivå, från cirka 10 % till 68 %.



Figur. 2.3: Enkätrespondenternas rapporterade kännedom om informationskällor om cybersäkerhet efter åldersgrupp.

2.3.3. Beteende och attityd

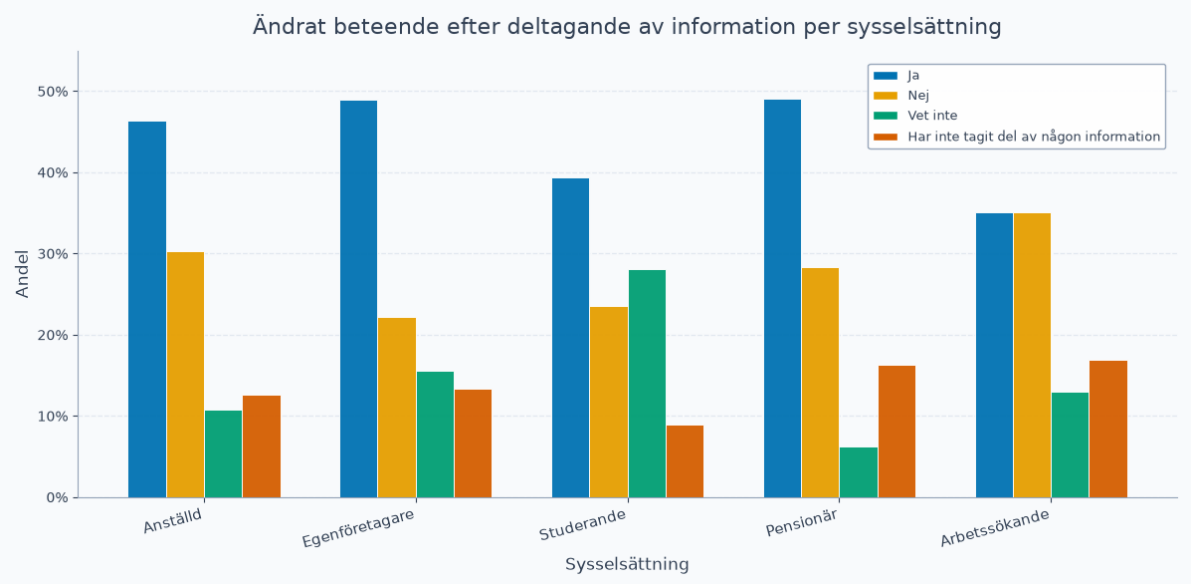
Har du ändrat något beteende online efter att ha tagit del av information om cybersäkerhet?

Enkätresultaten visade att 45 % av respondenterna hade ändrat sitt beteende efter att ha tagit del av cybersäkerhetsinformation. 29,2 % svarade att de inte hade ändrat sitt beteende, 12,4 % visste inte och 13,4 % svarade att de inte hade tagit del av någon information.

Resultaten varierade något mindre mellan åldersgrupperna än för de övriga frågorna. Yngre respondenter svarade oftare att de inte visste om cybersäkerhetsinformation hade påverkat deras beteende online. Den största skillnaden (16,1 %) för detta alternativ observerades mellan den yngsta och äldsta åldersgruppen då mindre än 5 % av de äldsta svarade att de ej visste. Äldre åldersgrupper svarade däremot i högre grad att de inte hade tagit del av någon cybersäkerhetsinformation. Den

största skillnaden i procenten av personer som inte hade tagit del av någon information var mellan åldersgrupperna 25–34 och 55–64 år (11,2 %). Andelen kvinnor som svarade att de inte visste eller att de inte hade tagit del av någon cybersäkerhetsinformation var cirka 7,5 procentenheter högre än motsvarande andel bland män. Enkätresultaten visade också att andelen respondenter som uppgav att de hade ändrat sitt beteende ökade med utbildningsnivån.

Anställda (46,4 %), egenföretagare (48,9 %) och pensionärer (49,1 %) svarade oftare att de hade ändrat sitt beteende jämfört med studerande (39,3 %) och arbetssökande (35,1 %). Studerande respondenter svarade även oftare att de inte visste om deras beteende hade förändrats, vilket kan ses i Figur 2.4. Respondenter med datorn som primär enhet svarade “Nej” något oftare, med ett lägre antal deltagare som svarade “Vet inte”. Surfplatteanvändare svarade oftare att de inte hade tagit del av någon cybersäkerhetsinformation. Skillnaderna var dock små.

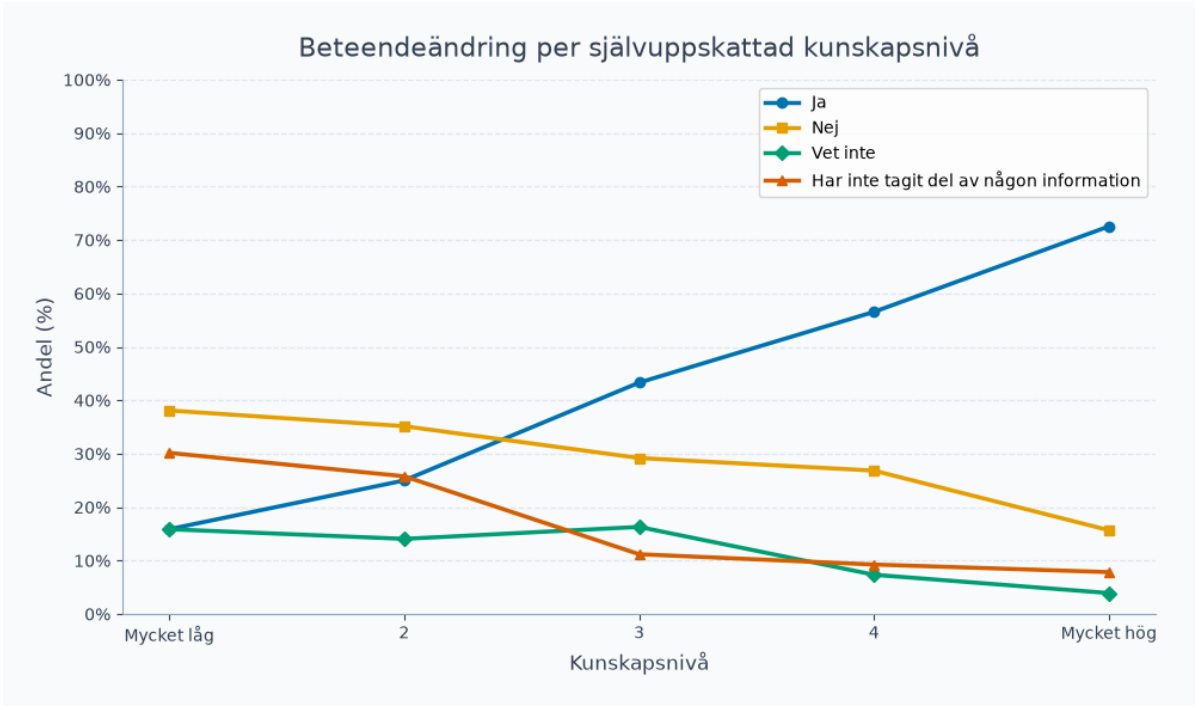


Figur. 2.4: Diagram över ändrat beteende efter deltagande, sorterat efter sysselsättning.

Korsanalys av enkätdata visade att det fanns ett starkt samband mellan förändring i beteende efter deltagande i cybersäkerhetsinformation och självbedömd kunskapsnivå. Andelen respondenter som hade ändrat sitt beteende ökade markant med högre rapporterad kunskapsnivå (se Figur 2.5).

Vilka av följande säkerhetsåtgärder använder du om de finns tillgängliga?

Enkätdata (se tabell 2.20) visade att användningen av olika säkerhetsåtgärder varierade. 23 % av respondenterna använde VPN när det var tillgängligt, vilket var den minst använda åtgärden. Användningen av starka lösenord var den vanligaste åtgärden. 4,4 % svarade att de inte använde någon av de angivna säkerhetsåtgärderna. Endast sex respondenter (0,6 %) svarade ’Annat’.



Figur. 2.5: Procent av respondenter inom en specifik självbedömd kunskapsnivå som valde det ovanstående alternativet när de frågades om de hade ändrat sitt beteende efter att ha deltagit i information om cybersäkerhet.

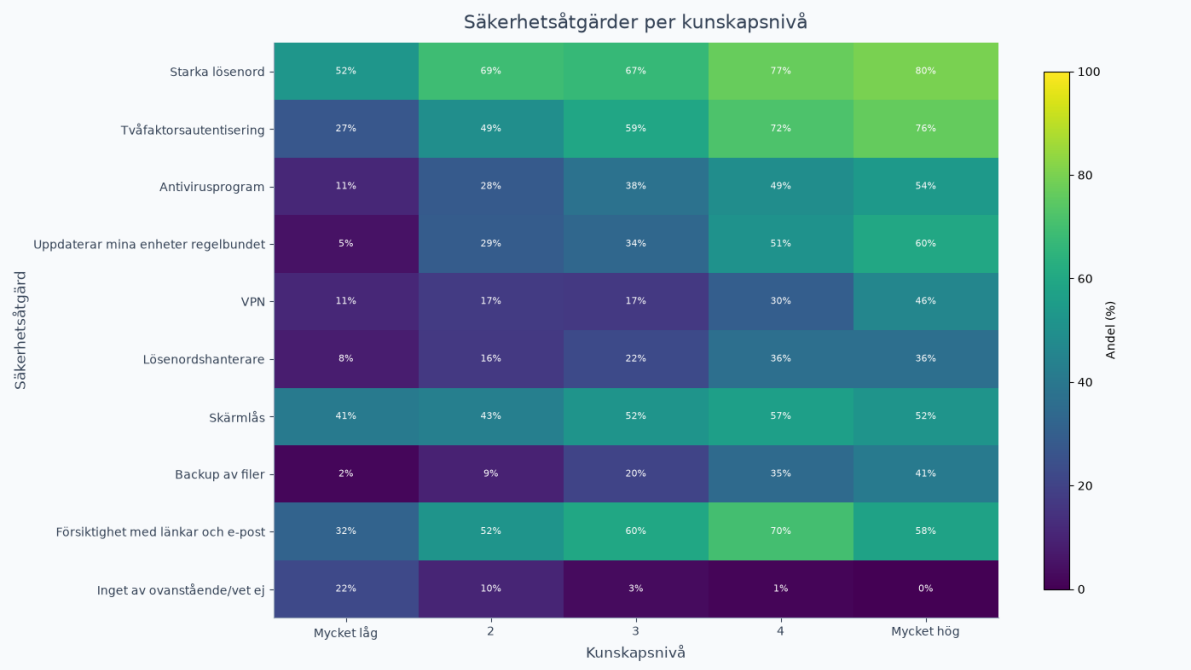
Säkerhetsåtgärd	Antal	Procent
Starka lösenord	704	70,4 %
Tvåfaktorsautentisering	614	61,4 %
Antivirusprogram	397	39,7 %
Uppdaterar mina enheter regelbundet	389	38,9 %
VPN	230	23 %
Lösenordshanterare	263	26,3 %
Skärmlås	515	51,5 %
Backup av filer	240	24 %
Försiktighet med länkar och e-post	599	59,9 %
Inget av ovanstående/vet ej	44	4,4 %
Annat, nämligen:	6	0,6 %

Tabell. 2.20: Andel deltagare som valde ett specifikt alternativ när de frågades vilka säkerhetsåtgärder som användes när de var tillgängliga.

Korsanalys utifrån åldersgrupper visade ett samband mellan respondenternas ålder och användningen av vissa säkerhetsåtgärder. Antivirusprogram, regelbunden uppdatering av enheter, säkerhetskopiering av filer samt försiktighet med länkar och e-post rapporterades generellt oftare i äldre åldersgrupper. Andelen som gjorde säkerhetskopior minskade dock från 30,9 % i åldersgruppen 55-64 år till 25,3 % i gruppen 65-80 år. Deltagare i åldersgruppen 18-24 år rapporterade den högsta användningen av VPN (28,2 %). I de mellanliggande åldersgrupperna låg användningen mellan 21,65 och 24,4 %, för att därefter minska till 16,4 % i den äldsta åldersgruppen. Användningen av starka lösenord var relativt jämnt fördelad mellan åldersgrupperna, medan resultaten för tvåfaktorsautentisering och skärmlås varierade utan något tydligt mönster. Endast små skillnader mellan könen observerades i användningen av säkerhetsåtgärder, med undantag för VPN, som användes av 27,3 % av männen och 18,6 % av kvinnorna när det var tillgängligt. Högre avslutad utbildning visade också ett samband med mer frekvent användning av flera säkerhetsåtgärder. Ett undantag var lösenordshanterare: 33,9 % av deltagarna med grundskola eller motsvarande som

högsta avslutade utbildning rapporterade användning, jämfört med 19,4 % bland deltagare med gymnasieutbildning eller motsvarande och cirka 30-32 % bland deltagare med eftergymnasial utbildning. Pensionärer och egenföretagare rapporterade oftare användning av antivirusprogram, medan yrkesverksamma och studerande rapporterade användning av VPN i högre utsträckning än de övriga grupperna.

Självbedömd kunskapsnivå visade ett tydligt samband med användningen av säkerhetsåtgärder. Granskning av enkätdata visade att deltagare med högre kunskapsnivå oftare rapporterade att de använde olika säkerhetsåtgärder. Andelen respondenter som svarade “inget av ovanstående/vet ej” minskade när kunskapsnivån ökade, se Figur 2.6. Inom säkerhetsåtgärderna “Skärmlås” och “Försiktighet med länkar och e-post” observerades en minskning av andelen som använde dessa bland respondenter som uppskattade att de hade en “mycket hög” kunskapsnivå. För VPN observerades däremot en kraftig ökning i samband med högre självbedömd kunskapsnivå.



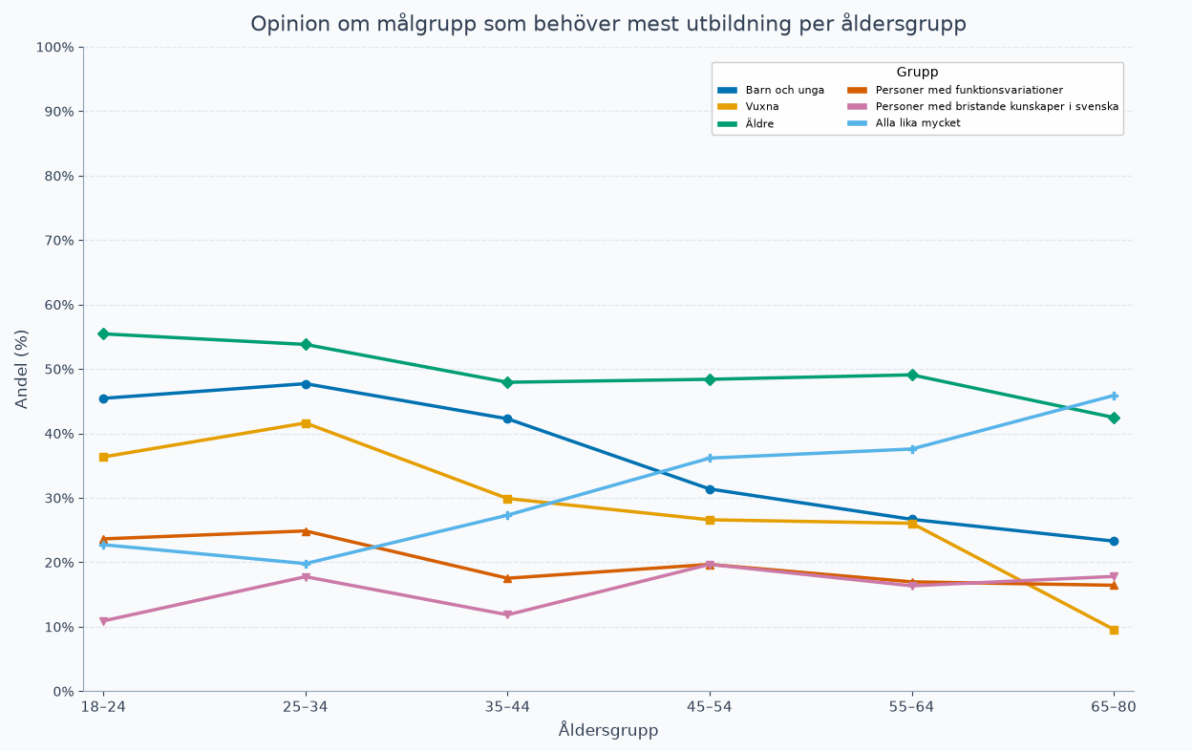
Figur. 2.6: Procent av respondenter i självbedömd kunskapsgrupp som använder en specifik säkerhetsåtgärd när den är tillgänglig.

Vilka målgrupper anser du har störst behov av cybersäkerhetsutbildning?

Enkätens respondenter ombads att välja den eller de målgrupper som de ansåg behövde utbildning mest. Syftet är inte att fastställa vilka målgrupper som faktiskt har störst utbildningsbehov, utan att undersöka allmänhetens uppfattningar om vilka grupper som anses behöva utbildning. Frågan ger också en indikation på om respondenterna uppfattar cybersäkerhetsutbildning som något som bör riktas mot specifika grupper eller om den bör omfatta befolkningen generellt. Av åldersgrupperna ansåg respondenterna att ”Äldre” hade störst behov av utbildning (49,4 %). Därefter valde 36,3 % av respondenterna “Barn och unga”, 28,7 % ”Vuxna”, 19,8 % “Personer med funktionsvariationer”, samt 16 % “Personer med bristande kunskaper i svenska”. Slutligen ansåg även 31,4 % att alla behövde lika mycket utbildning.

De två yngsta åldersgrupperna som representerades av intervallet 18–34 år visade en större benägenhet att markera “Personer med funktionsvariationer”, “Äldre”, “Vuxna”, samt “Barn och unga”. Andelen som valde ”Vuxna” samt ”Barn och unga” minskade mer än de övriga alternativen (figur 2.7). Andelen respondenter som svarade “Alla lika mycket” ökade i samband med stigande ålder, med undantag för de yngsta och näst yngsta åldersgrupperna, där en minskning på cirka tre procentenheter observerades. Korsanalys utifrån högsta avslutade utbildning visade inga grupper

som skiljer sig från den generella opinionen. Undantaget var respondenterna med grundskola/motsvarande som sin högsta utbildning. Dessa respondenter valde “Personer med bristande kunskaper i svenska” oftare än “Personer med funktionsvariationer” till skillnad från övriga grupper. Ett fåtal avvikelser observerades vid korsanalys utifrån respondenternas sysselsättning. Pensionärer var betydligt mer benägna att välja “Alla lika mycket” och valde “Vuxna” i betydligt mindre utsträckning än övriga grupper, 49,7 % och 10,7 % jämfört med genomsnittet på 31,4 % och 28,7 %.



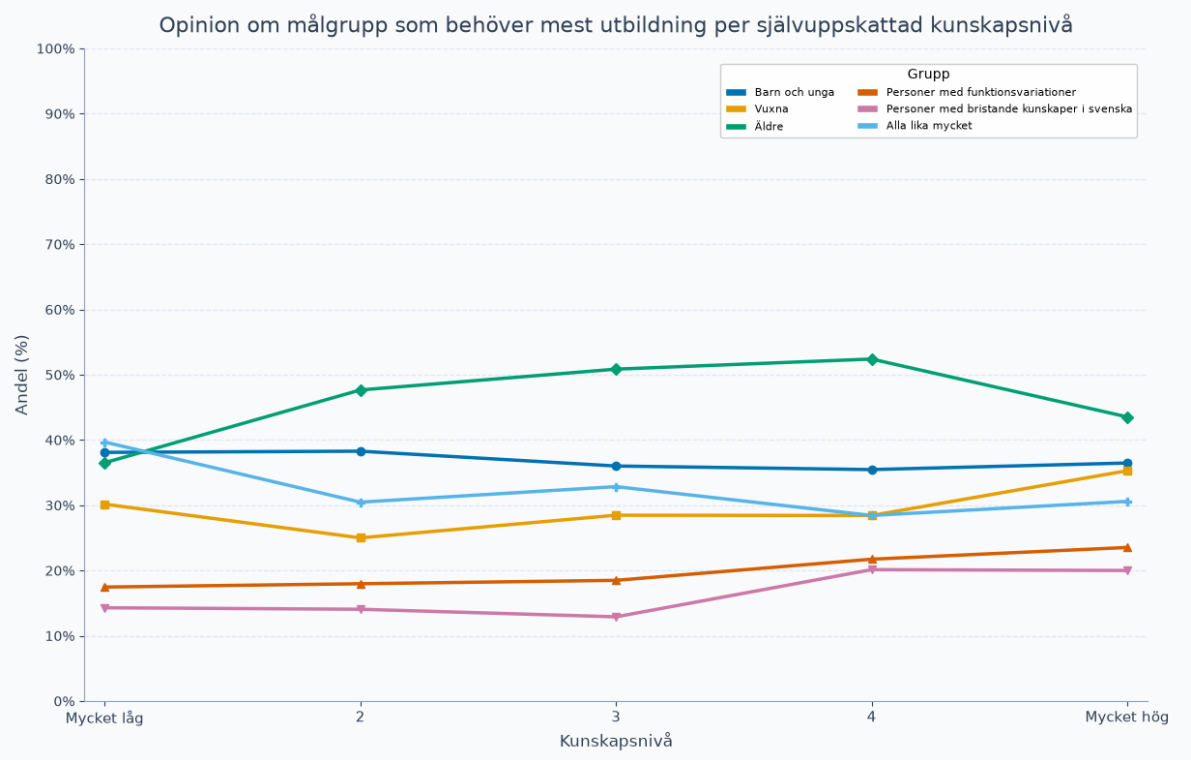
Figur. 2.7: Diagram över grupper som anses behöva mest utbildning, utifrån procent av populationen i respektive åldersgrupp.

Korsanalysen utifrån självbedömd kunskapsnivå visade endast små skillnader mellan grupperna (se figur 2.8). Den största variationen observerades i bedömningen av gruppen ”Äldre” där respondenter med lägst och högst kunskapsnivå prioriterade gruppen något mindre. Inom de två lägsta kunskapsnivåerna observeras även en något större tendens att välja barn och unga. Respondenter med en självbedömd kunskapsnivå som är ”Mycket hög” prioriterade vuxna något mer, medan de som hade näst lägst självbedömd kunskapsnivå prioriterade vuxna minst. Även en minimal successiv ökning av benägenheten att välja personer med funktionsvariationer observerades i samband med att självbedömd kunskapsnivå ökade. Respondenterna inom de två högre kunskapsnivåerna markerade personer med bristande kunskaper i svenska något oftare än övriga grupper. Slutligen visade data (figur 2.8) att respondenter med en mycket låg självbedömd kunskapsnivå hade en något större benägenhet att svara att alla behöver lika mycket utbildning.

Hur vill du helst lära dig mer om cybersäkerhet?

Avslutningsvis fick respondenterna svara på hur de helst vill lära sig med om cybersäkerhet. Analysen visade att respondenter föredrog att lära sig om cybersäkerhet via digitala lösningar. Digitala föreläsningar, självstudier via digitala plattformar samt information som skickas digitalt föredrogs av över 30 % av respondenterna. Minst attraktivt är att lära sig via spel, vilket framgår av tabell 2.21.

Respondenterna mellan 65–80 år visar störst vilja att lära sig via digitalt skickad information (48,6 %). Den näst mest föredragna inlärningsmetoden i gruppen är självstudier via digitala plattformar, vilket föredras av 27,4 %. Åldersgruppen 55–64 år hade också en hög andel respondenter som valde

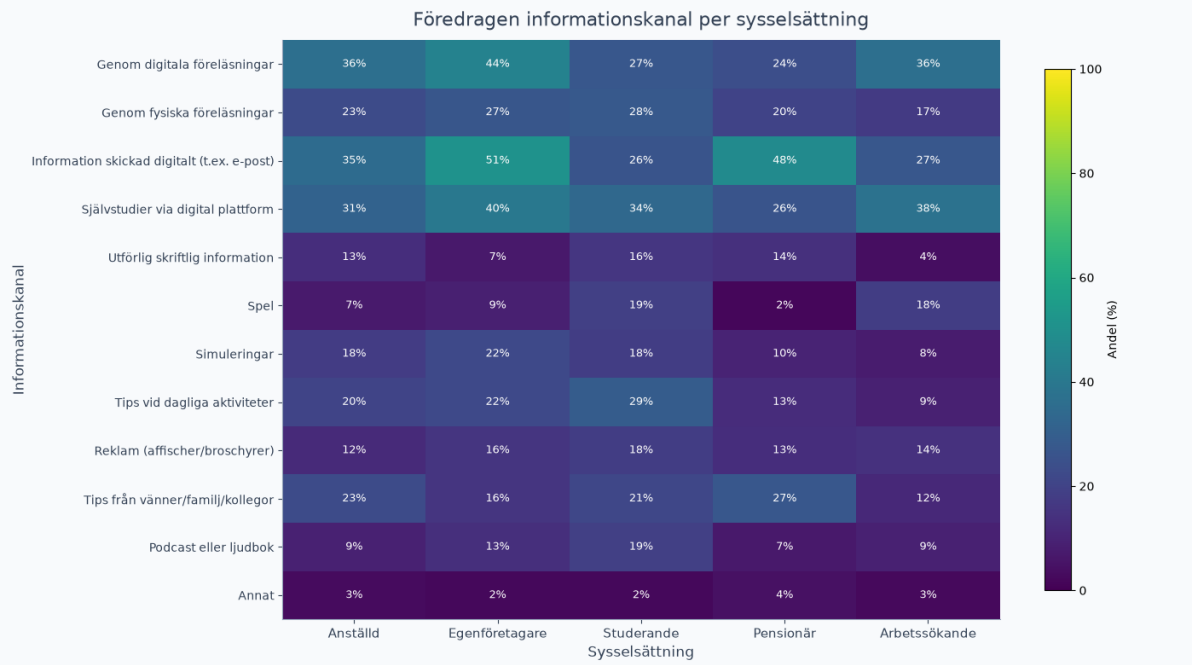


Figur. 2.8: Andel procent av respondenter inom självuppskattad kunskapsnivå som valde specifik målgrupp som att behöva mest utbildning.

Svarsalternativ	Antal	Procent
Genom digitala föreläsningar	340	34 %
Genom fysiska föreläsningar	223	22,3 %
Genom information som skickats till mig digitalt, exempelvis via e-post	365	36,5 %
Genom självstudier via en digital plattform, exempelvis YouTube eller en webbsida	311	31,1 %
Utförlig skriftlig information, exempelvis böcker	125	12,5 %
Genom att spela ett spel	86	8,6 %
Genom att delta i simuleringar (uppleva säkerhetsincidenter i en kontrollerad miljö)	159	15,9 %
Som tips vid mina dagliga aktiviteter, exempelvis lösenordstips när jag ska skapa ett konto	192	19,2 %
Reklam i form av exempelvis affischer eller broschyrer	131	13,1 %
Genom tips eller stöd från exempelvis vänner, familj eller kollegor	222	22,2 %
Lyssna på inspelat material, exempelvis en podcast eller ljudbok	102	10,2 %
Annat, nämligen:	31	3,1 %

Tabell. 2.21: Andel deltagare som valde ett specifikt alternativ när de ombads att svara på hur de helst vill lära sig om cybersäkerhet.

”digitalt skickad information” då 44,2 % av åldersgruppen markerade detta alternativ. Däremot observeras mindre skillnader mellan de andra alternativen jämfört med åldersgruppen 65–80 år. Digitala föreläsningar, självstudier via digital plattform och digitalt skickad information är de mest frekvent valda bland övriga åldersgrupper, med minimal variation mellan alternativen. Undantaget är åldersgruppen 18–24 år. Denna åldersgrupp var mindre benägen att föredra digitalt skickad information som inlärningsmetod. Även åldersgruppen 35–44 år visar en något minskad villighet att välja detta alternativ jämfört med andra grupper, dock i mindre utsträckning än ovan. Respondenter med eftergymnasial utbildning föredrog att få information skickad digitalt, medan respondenter utan eftergymnasial utbildning föredrog digitala föreläsningar något mer än digitalt skickad information och självstudier via en digital plattform. Slutligen valde respondenter med högre utbildning generellt de olika alternativen mer frekvent än andra, vilket indikerar en högre villighet att lära sig mer om cybersäkerhet. Noterbart är också att det är en stor spridning i resultat vilket visar på ett behov av flera olika informationsvägar, vilket är i linje med tidigare studier [13].



Figur. 2.9: Andelen av populationen inom en specifik sysselsättning som väljer en specifik inlärningsmetod när de frågades hur de helst ville lära sig om cybersäkerhet.

Korsanalysen visade att svaren varierade mest mellan olika sysselsättningsgrupper. Egenföretagare och pensionärer var mest benägna att lära sig genom digitalt skickad information (figur 2.9). Studerande, arbetande och arbetssökande var mycket mindre benägna att välja det här alternativet. Dessa grupper visade störst vilja att lära sig genom självstudier på digitala plattformar eller via digitala föreläsningar, förutom studerande som uppvisade en mindre preferens för digitala föreläsningar. Respondenter med högre kunskapsnivå var mer villiga att använda olika studiemetoder.

2.4. Analys - Tidslinje

I följande avsnitt analyserades de identifierade initiativens aktivitet ur ett tidsperspektiv. Syftet var att visa hur utbudet utvecklats över tid. Detta genomfördes utifrån tidigare insamlade data, vilket beskrivs i kapitel 1.1.

Analys av data (tabell 2.22) visade variation i initiativens tidigaste identifierade närvaro. I genomsnitt var den tidigaste närvaron för de identifierade initiativen slutet av 2019 med en median på 2022-02-28, vilket visade att majoriteten av initiativen skapades relativt nyligen. Detta framgår även av figurerna A.1 och A.2 i appendix A där det framgår att majoriteten hade sin tidigaste spårbara aktivitet i början av 2020-talet.

Variabel	Medel	Median	SD	IQR	Min	Max	n
Tidigast identifierad närvaro	2019-11-26	2022-02-28	–	–	1997-12-31	2026-01-30	40
Tid sedan tidigast identifierad närvaro (dagar)	2 509,2	1 684,0	2 595,5	1 739,25	252	10 509	40

Tabell. 2.22: Deskriptiv statistik för de identifierade folkbildande cybersäkerhetsinitiativen. Tabellen visar initiativens tidigast identifierade närvaro samt antal dagar från denna närvaro till referensdatumet 2026-10-09. Standardavvikelse och interkvartilavstånd redovisas för den andra variabeln.

För att uppskatta hur länge initiativen hade varit aktiva dokumenterades antalet dagar mellan variabel 1 (tidigast identifierad närvaro) och variabel 2 (senast spårbara cybersäkerhetsrelaterade aktivitet) för varje initiativ. Likt variabel 1 visade även denna en stor variation. Ett medelvärde på cirka 2500 dagar och en median på cirka 1700 dagar observerades. Även standardavvikelse (SD) och interkvartilavstånd (IQR) beräknades; se tabell 2.22.

2.5. Resultatsammanfattning

Totalt identifierades 40 folkbildande cybersäkerhetsinitiativ i studien. Initiativen omfattade en bred mångfald av målgrupper, men hade vissa brister. Invandrare, personer med begränsade språkkunskaper samt personer med funktionsvariationer hade ett begränsat antal riktade initiativ. Åldersgruppen 0–6 år hade också en mycket låg representation. Initiativen visade också en benägenhet att rikta sig till personer med lägre IT-kompetens. Slutligen observerades det att initiativen oftare riktade sig till vuxna och personer i arbetslivet än till andra grupper.

Studien visade att majoriteten av de identifierade folkbildande cybersäkerhetsinitiativen i Sverige hade ett nationellt fokus. Initiativen bedömdes ha en god möjlighet att nå många personer. Initiativens finansiering skedde vanligtvis genom offentliga medel, men även ideell finansiering och samverkan mellan olika aktörer förekom regelbundet.

De identifierade initiativen visade en tendens att innehålla och hantera kunskap på en grundläggande nivå. Materialet inom initiativen bedömdes generellt ha en medelstor omfattning, medan användarcentreringen var relativt hög och initiativen vanligtvis erbjöd tillgång till sitt material gratis. Materialet var däremot ofta begränsat vad gäller möjligheterna till återanvändning och anpassning.

Respondenterna i enkäten hade en något optimistisk självbedömning av sin kunskapsnivå. Samtidigt fanns ett samband mellan självbedömd kunskapsnivå och rapporterade beteenden som kunde indikera lägre sårbarhet, bland annat användning av säkerhetsåtgärder och förändrat beteende efter att ha tagit del av cybersäkerhetsinformation. Högre självbedömd kunskapsnivå var förknippad med rapporterade beteenden som kunde indikera lägre sårbarhet.

Kännedom om de initiativ och informationskällor som granskades var låg bland enkätrespondenterna. Även här fanns ett liknande samband med kunskapsnivå som ovan. Respondenternas ålder visade också ett samband med kännedom, där högre ålder generellt var förknippad med lägre kännedom. Nästan alla respondenter rapporterade att de använde någon form av säkerhetsåtgärd. De populäraste åtgärderna var tekniskt enkla. Respondenterna ansåg att äldre hade störst behov av utbildning i cybersäkerhet, följt av barn och unga.

De identifierade initiativen uppvisade stor variation i tidigast närvaro. Trots att ett fåtal av initiativen hade existerat under en mycket lång tid visade medianvärdet att majoriteten hade sitt ursprung i tidigt 2020-tal. Initiativens senast spårbara aktivitet låg i genomsnitt under 2026, vilket visade att de var aktiva vid tidpunkten för datainsamlingen. Livslängden för initiativen visade stor variation, men skillnaden mellan medelvärde, median, standardavvikelse och interkvartilavstånd visade att detta berodde på ett fåtal mycket gamla initiativ. Medianvärdet för livslängd visade att ett typiskt initiativ hade varit aktiv i cirka 4 år. Däremot visade interkvartilavståndet att det fanns en betydande variation även med ett urval av de mittersta 50 % av initiativen.

3

Diskussion och slutsats

I detta kapitel sammanfattas studiens resultat genom en presentation av studiens huvudsakliga slutsatser och presentation av rekommendationer riktade till Cybercampus.

3.1. Slutsats

Kartläggningen visade att Sverige har ett relativt stort antal folkbildande cybersäkerhetsinitiativ som täcker många kunskapsområden och flera målgrupper. Det kan också konstateras att flera av initiativen har funnits under flera år och förefaller vara aktiva. Andelen initiativ har ökat sedan 2020, vilket kan antas bero på ett allt större samhälleligt fokus på cybersäkerhet. Offentliga aktörer är en viktig källa till finansiering. Sammantaget kan slutsatsen dras att det generellt finns en god tillgång på aktiva och livskraftiga folkbildande initiativ. Det är oklart om och hur dessa koordineras och det är viktigt att belysa vikten av empiriskt validerat innehåll och beprövade metoder [1]. Om olika aktörer sprider olikartade råd kan det leda till säkerhetsutmattning, vilket kan vara kontraproduktivt [22]. Vidare visade resultaten att särskilda grupper, nämligen personer med begränsade svenskkunskaper samt personer med funktionsvariationer, hade begränsad tillgång till anpassat material, samtidigt som de beskrivs som särskilt utsatta i tidigare rapporter [4, 14].

Majoriteten av initiativen erbjöd gratis tillgång till material, fokuserade på grundläggande kunskap och bedömdes ha potential att nå en stor del av befolkningen. Trots detta visade enkätresultaten att allmänheten hade en mycket begränsad kännedom om folkbildande cybersäkerhetsinitiativ. Majoriteten hade dessutom ingen kännedom om vilka informationskällor de kunde vända sig till. Detta indikerar att den största barriären för att öka allmänhetens cybersäkerhetskunskap är att nå ut till allmänheten snarare än att se till att lärandematerial finns tillgängligt. Existerande material är dessutom ofta i den form som många respondenter föredrar, digitala föreläsningar och självstudiematerial. Utbildande material bidrar inte till allmänhetens kunskap om det inte syns eller används. Anpassningsbarheten hos befintligt material var även begränsad, vilket utgör ett hinder för spridning och återanvändning av materialet. Anpassningsbarheten till individens förutsättningar, kunskapsnivå eller behov av material är en nyckelfaktor enligt litteraturen [21, 12].

En ytterligare slutsats är att både yngre och äldre har lägre självupplevd kunskap och samtidigt lägre kännedom om befintliga initiativ. Detta i kombination med att ökad upplevd kunskap är kopplad till rapporterad användning av säkerhetsfunktioner visar på ett säkerhetsglapp. Respondenter med lägre självbedömd kunskapsnivå rapporterade beteenden som kunde indikera större sårbarhet, medan respondenter med högre självbedömd kunskapsnivå rapporterade fler skyddsåtgärder. Tidigare forskning indikerar att detta inte bara är en fråga om säkerhet utan även inkludering, då ökad kunskap ger trygghet som i sin tur kan leda till ökad digital delaktighet [10].

Avslutningsvis bedömer denna studie att det inte finns något generellt behov av mer material för hela befolkningen utan att eventuella initiativ från Cybercampus snarare kan rikta in sig på existerande glapp avseende både kännedom om initiativ, material för utsatta grupper och koordinering. Studien lämnar följande rekommendationer:

- **Cybercampus kan verka för att etablera en långsiktig koordinerande roll för folkbildande cybersäkerhetsinitiativ.** Studien visar att det finns ett stort antal initiativ och att offentlig finansiering är vanligt förekommande, samtidigt som det är oklart i vilken utsträckning initiativen koordineras. En koordinerande funktion skulle kunna innefatta att löpande skapa och upprätthålla en överblick över aktiva initiativ, identifiera överlappningar och luckor samt skapa former för erfarenhetsutbyte och samverkan mellan berörda aktörer. Rollen skulle även kunna innefatta att kanalisera stöd till folkbildande initiativ. Beroende på Cybercampus uppdrag och mandat skulle detta exempelvis kunna omfatta utlysningar, hantering och bedömning av ansökningar samt uppföljning av beviljat stöd. Den koordinerande funktionen bör i huvudsak betraktas som en löpande uppgift, eftersom både hotlandskapet och utbudet av folkbildande initiativ förändras över tid. Enskilda satsningar inom ramen för funktionen kan däremot vara tidsbegränsade.

- **Cybercampus kan utveckla en stödjande funktion för aktörer som bedriver folkbildning inom cybersäkerhet.** Syftet med en sådan funktion skulle vara att stärka befintliga initiativ snarare än att ersätta dem eller utveckla parallella utbildningsinsatser. Stödet skulle exempelvis kunna omfatta tillgång till aktuell kunskap om hotlandskapet, forskningsbaserad kunskap om cybersäkerhetsmedvetenhet och beteendeförändring samt stöd vid utveckling, anpassning och utvärdering av utbildningsmaterial. Funktionen skulle kunna bedrivas genom exempelvis kunskapsunderlag, seminarier, workshops, nätverk och möjligheter till rådgivning. Forskare och andra experter inom Cybercampus nätverk skulle kunna engageras utifrån behov, medan en central funktion eller stab kan svara för kontinuitet, koordinering, administration och förmedling av relevant kompetens. En sådan modell skulle kunna bidra till att befintliga initiativ i högre grad använder forskningsbaserade metoder och samstämmiga råd.

- **Cybercampus kan verka för att öka kännedomen om och spridningen av befintliga folkbildande cybersäkerhetsinitiativ.** Studien visar att det finns ett relativt omfattande utbud av folkbildande material, samtidigt som allmänhetens kännedom om både initiativen och relevanta informationskällor är låg. En spridningsfunktion skulle därför kunna fokusera på att göra befintliga resurser enklare att hitta och använda snarare än att i första hand utveckla nytt generellt material. Detta skulle exempelvis kunna ske genom att samla och synliggöra kvalitetssäkrade resurser, skapa gemensamma ingångar till befintliga initiativ och stödja aktörer i att nå relevanta målgrupper. Arbetet kan med fördel integreras med den koordinerande rollen, där Cybercampus fungerar som en sammanhållande länk mellan initiativ och aktörer med möjlighet att nå olika delar av befolkningen. Även denna funktion bör vara löpande, eftersom såväl initiativ som informationsbehov förändras över tid.

- **Cybercampus kan stödja utveckling och anpassning av material för målgrupper som i dag har begränsad tillgång till anpassade resurser.** Studien identifierar särskilt personer med begränsade kunskaper i svenska samt personer med funktionsvariationer som grupper med begränsad tillgång till anpassat material. I stället för att Cybercampus nödvändigtvis utvecklar och förvaltar eget material skulle rollen kunna vara att initiera, stödja eller finansiera utveckling och anpassning tillsammans med aktörer som har kompetens och etablerade kontaktytor mot respektive målgrupp. Detta kan exempelvis innefatta språklig och pedagogisk anpassning, tillgänglighetsanpassning samt utprovning av material tillsammans med den avsedda målgruppen. Insatserna bör utgå från identifierade behov och kan därför bedrivas som avgränsade projekt inom ramen för en mer långsiktig stödjande funktion.

4

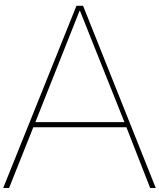
Begränsningar och vidare studie

Studien hade flera metodologiska begränsningar och studiens resultat ska tolkas med dessa som bakgrund. Den huvudsakliga begränsningen är att studien har analyserat vilka initiativ som existerar snarare än hur effektiva de är. En annan fundamental begränsning är att studien är begränsad till initiativ i Sverige, och resultaten kan inte generaliseras utanför Sverige. Datainsamlingen av folkbildande cybersäkerhetsinitiativ utfördes genom att söka på Internet. Detta innebar att initiativ som bedrevs helt offline kan ha exkluderats ur studien. Notera även att bedömningarna av vilka indikatorer och målgrupper som associerades med initiativen gjordes manuellt, vilket kan ha medfört subjektiva bedömningar och bedömarbias. När initiativ samlades in användes även AI-verktyg (GPT-5.3) för att identifiera relevanta källor. Detta kan ha medfört vissa risker, även om manuell screening gjordes efteråt. Viss litteratursökning gjordes även med hjälp av verktyget Elicit[1].

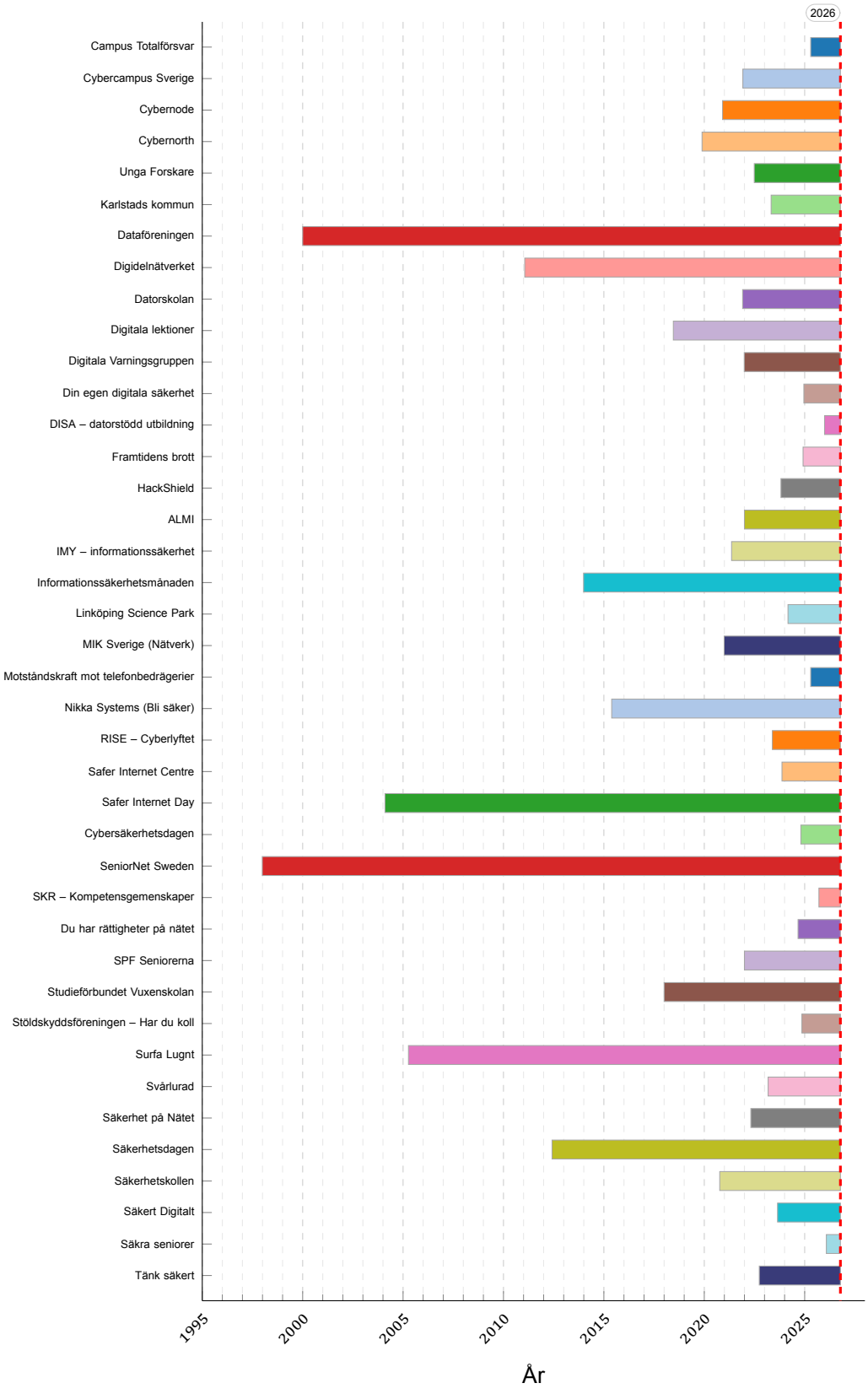
En ytterligare begränsning var att vissa svarskategorier i enkätundersökningen innehöll färre än 100 svar. Korsanalyserna för dessa kategorier baserades därför på små delurval, vilket kan ha minskat resultatens tillförlitlighet. En ytterligare begränsning i studien var mätningen av de identifierade initiativens tidigaste aktivitet. Eftersom en mindre andel av de identifierade initiativen (ofta de äldre) täckte ett större område än endast cybersäkerhet, representerade den tidigaste identifierade aktiviteten därför inte alltid den tidigaste cybersäkerhetsrelaterade aktiviteten för initiativet.

Ett flertal källor anger att vissa grupper är mer sårbara för cyberbrott [2, 3, 4, 5, 11, 14, 18, 30]. Trots detta saknas det studier som utför en översiktlig kartläggning av olika gruppers sårbarhet. Flera studier [2, 14, 16, 30] fokuserar på endast en enskild möjlig vektor för sårbarhet, vanligtvis phishing, vilket identifieras som ett mycket stort hot [29]. Andra [5, 11, 18] undersöker enbart en begränsad demografisk faktor, exempelvis ålder. Enkätundersökningen som genomfördes i denna studie gav också den en något begränsad insyn i vilka grupper och faktorer som påverkar sårbarheten mot cyberbrott. Det finns därför utrymme för framtida studier som undersöker olika faktorer och bedömer deras grad av påverkan på sårbarheten. Eftersom studien inte undersökte initiativens faktiska effekter finns det även behov av framtida studier av deras effektivitet i praktiken. Detta kan ge en bild av vilka metoder som fungerar i verkligheten och bidra till en bättre förståelse av hur en bra åtgärd bör utformas.

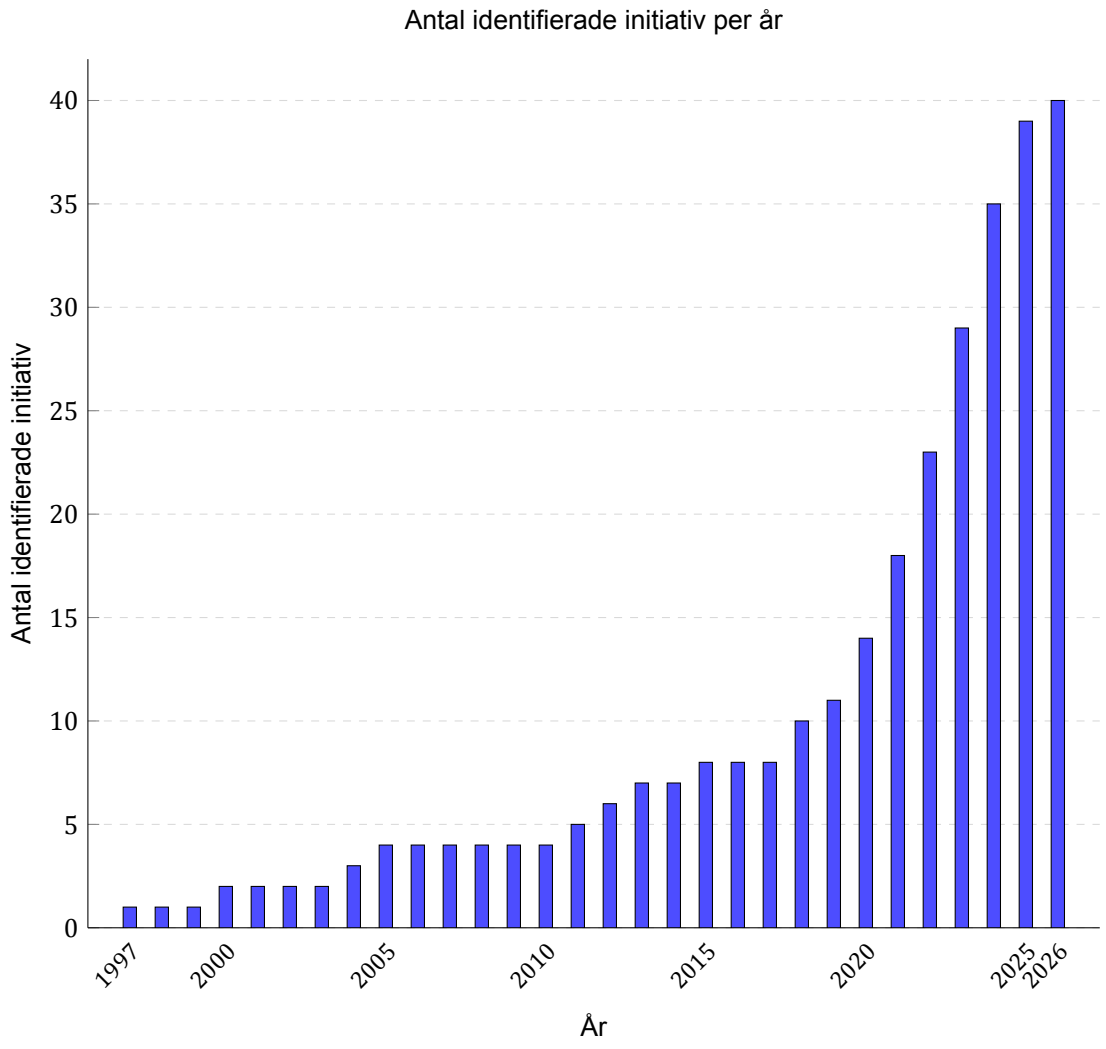
[1] https://elicit.com



Appendix A - Diagram



Figur. A.1: Tidpunkt för första identifierade aktivitet hos respektive initiativ.



Figur. A.2: Kumulativt antal identifierade initiativ per år, baserat på initiativens tidigast identifierade närvaro.

B

Appendix B - Tabeller

Initiativ	Organisation	Aktivitetstyp
	Campus Totalförsvar	Utbildning
	Cybercampus Sverige	Forskning, utbildning
	Cybernode	Nätverk
	Cybernorth	Samverkansinitiativ
Cybersecurity Academy	Unga Forskare	Utbildning
Cybersäkerhet genom ökad kunskap och beteendeförändring	Karlstad kommun (Smart Karlstad/CBCC-projekt)	Forskning, utbildning och beteendeförändring
	Dataföreningen i Sverige	Nätverk, utbildning, event
Digidel	Digidelnätverket	Digital inkludering, utbildning
Digiguiden	Datorskolan	Pedagogiskt material, stöd i handledning
Digitala lektioner	Internetstiftelsen	Utbildning
Digitala Varningsgruppen	Stöldskyddsföreningen	Varningssystem, informationsdelning
Din egen digitala säkerhet	Myndigheten för civilt försvar	Informationsresurs
DISA – datorstödd utbildning	Myndigheten för civilt försvar	E-utbildning
Framtidens brott	SSF Stöldskyddsföreningen	Rapportserie
HackShield	Tryggare Sverige	Spelbaserad utbildning, undervisningsmaterial
	ALMI	Workshop, seminarium
IMY – informationssäkerhet	IMY	Informationsresurs
Informationssäkerhetsmånaden	Myndigheten för civilt försvar	Kampanj
Grundläggande cybersäkerhet	Linköping Science Park	Utbildning
MIK Sverige	Mediemyndigheten	Informationsinsats
Motståndskraft mot telefonbedrägerier	Polismyndigheten	Brottsförebyggande kampanj, föreläsningar
Bli säker	Nikka Systems	Utbildning (podd, bok, artiklar)
Cyberlyftet	RISE	Utbildning
Safer Internet Centre	Mediemyndigheten, Bris, ECPAT)	Nationellt kunskapscenter, samverkansplattform
Safer Internet Day	Mediemyndigheten/Safer Internet Centre Sverige	Årlig temadag och kampanj
Cybersäkerhetsdagen	JTH, Science Park, Almi	Konferens
	SeniorNet Sweden	Digital folkbildning/studiecirklar
SKR – kompetensgemenskaper	SKR	Nätverk / kunskapsdelning
Du har rättigheter på nätet	Mediemyndigheten	Informationsresurs
Säker på nätet	SPF Seniorerna	Informationsinsats / utbildning
	Studieförbundet Vuxenskolan	Kurs / folkbildning
Har du koll	Stöldskyddsföreningen	Kampanj
	Surfa Lugnt	Informationsinsats
Svårlurad	Banker (samverkan)	Kampanj
Säkerhet på Nätet	Internetkunskap (Internetstiftelsen)	Informationsresurs
Säkerhetsdagen	Privata aktörer	Event / konferens
Säkerhetskollen	Stöldskyddsföreningen	Informationsinsats
Säkert Digitalt	Samverkan (banker, polis m.fl.)	Kampanj
Säkra seniorer	Samverkan	Informationsinsats
Tänk säkert	Myndigheten för civilt försvar, Internetstiftelsen m.fl.	Nationell kampanj

Tabell. B.1: Lista över initiativ, dess drivande organisation och typ av aktivitet. I flera fall driver organisationer icke-namngivna initiativ. I dessa fall är kolumnen initiativ tom.

Barn och unga	Seniorer	Yrkesverksamma	Generell
Cybersecurity Academy	Digiguiden	Campus totalförsvar	Cybersäkerhet genom ökad kunskap och beteendeförändring
Digitala lektioner	Motståndskraft mot telefonbedrägerier	Cybercampus Sverige	Dataföreningen
HackShield	SeniorNet Sweden	Cybernode	Digidel
Safer Internet Centre	SPF Seniorerna	Cybernorth	Digitala Varningsgruppen
Safer Internet Day	Studieförbundet Vuxenskolan	Framtidens brott	Din egen digitala säkerhet
Du har rättigheter på nätet	Svårlurad	Hur skapas fler affärer med cybersäkerhet i ditt företag?	DISA - datorstödd utbildning
Surfa Lugnt	Säkert Digitalt	Linköping Science Park - Grundläggande cybersäkerhet	IMY - informationssäkerhet
	Säkra seniorer	RISE - cybersäkerhet-sutbildning	informationssäkerhets-månaden
		Science Park Jönköping - cybersäkerhetsdagen	MIK Sverige
		Stöldskyddsföreningen - Har du koll	Nikka Systems ”Bli säker”
		Säkerhetsdagen	SKR - kompetensge-menskaper
			Säkerhet på nätet
			Säkerhetskollen
			Tänk säkert

Tabell. B.2: Kategorisering av huvudmålgrupp för varje initiativ.

Användarcentrering

Barn och unga	(1-3)	Seniorer	(1-3)	Yrkesverksamma	(1-3)	Generell	1-3
Cybersecurity Academy	3	Digiguiden	3	Campus totalförsvar	2	Cybersäkerhet genom ökad kunskap och beteendeförändring	2
Digitala lektioner	3	Motståndskraft mot telefonbedrägerier	3	Cybercampus Sverige	2	Dataföreningen	2
HackShield	3	SeniorNet Sweden	3	Cybernode	1	Digidel	3
Safer Internet Centre	3	SPF seniorerna	3	Cybernorth	2	Digitala Varningsgruppen	2
Safer Internet Day	3	Studieförbundet Vuxenskolan	3	Framtidens brott	1	Din egen digitala säkerhet	3
Du har rättigheter på nätet	3	Svårlurad	3	Hur skapas fler affärer med cybersäkerhet i ditt företag?	3	DISA – datorstödd utbildning	2
Surfa Lugnt	3	Säkert Digitalt	3	Linköping Science Park – Grundläggande cybersäkerhet	2	IMY – informationssäkerhet	3
		Säkra seniorer	3	RISE – cybersäkerhetsutbildningar	2	Informationssäkerhetsmånaden	2
				Science Park Jönköping – cybersäkerhetsdagen	2	MIK Sverige (Nätverk)	3
				Stöldskyddsförenin – Har du koll	3	Nikka Systems (”Bli säker”)	3
				Säkerhetsdagen	1	SKR – kompetensgemenskaper	2
						Säkerhet på Nätet	3
						Säkerhetskollen	3
						Tänk säkert	3
Medelvärde:	**3**	**Medelvärde:**	**3**	**Medelvärde:**	**1,91**	**Medelvärde:**	**2,57**

Tabell. B.3: Visar individuella värden samt medelvärdet av användarcentrering för initiativen i varje huvudmålgrupp. (låg - hög).

Räckvidd

Barn och unga	(1-3)	Seniorer	(1-3)	Yrkesverksamma	(1-3)	Generell	1-3
Cybersecurity Academy	2	Digiguiden	3	Campus totalförsvar	3	Cybersäkerhet genom ökad kunskap och beteendeförändring	2
Digitala lektioner	3	Motståndskraft mot telefonbedrägerier	2	Cybercampus Sverige	3	Dataföreningen	3
HackShield	2	SeniorNet Sweden	2	Cybernode	3	Digidel	3
Safer Internet Centre	3	SPF Seniorerna	2	Cybernorth	2	Digitala Varningsgruppen	3
Safer Internet Day	3	Studieförbundet Vuxenskolan	2	Framtidens brott	3	Din egen digitala säkerhet	3
Du har rättigheter på nätet	3	Svårlurad	3	Hur skapas fler affärer med cybersäkerhet i ditt företag?	1	DISA – datorstödd utbildning	3
Surfa Lugnt	3	Säkert Digitalt	3	Linköping Science Park – Grundläggande cybersäkerhet	1	IMY – informationssäkerhet	3
		Säkra seniorer	2	RISE – cybersäkerhetsutbildningar	2	Informationssäkerhetsmånaden	3
				Science Park Jönköping – cybersäkerhetsdagen	1	MIK Sverige (Nätverk)	3
				Stöldskyddsförenin – Hardukoll	3	Nikka Systems (”Bli säker”)	3
				Säkerhetsdagen	1	SKR – kompetensgemenskaper	2
						Säkerhet på Nätet	3
						Säkerhetskollen	3
						Tänk säkert	3
Medelvärde:	**2,71**	**Medelvärde:**	**2,38**	**Medelvärde:**	**2,09**	**Medelvärde:**	**2,86**

Tabell. B.4: Visar individuella värden samt medelvärdet av räckvidden för initiativen i varje huvudmålgrupp. (låg - hög).

Omfång av material

Barn och unga	(1-3)	Seniorer	(1-3)	Yrkesverksamma	(1-3)	Generell	1-3
Cybersecurity Academy	2	Digiguiden	3	Campus totalförsvar	2	Cybersäkerhet genom ökad kunskap och beteendeförändring	2
Digitala lektioner	3	Motståndskraft mot telefonbedrägerier	2	Cybercampus Sverige	2	Dataföreningen	3
HackShield	2	SeniorNet Sweden	3	Cybernode	1	Digidel	3
Safer Internet Centre	3	SPF Seniorerna	2	Cybernorth	2	Digitala Varningsgruppen	2
Safer Internet Day	3	Studieförbundet Vuxenskolan	2	Framtidens brott	2	Din egen digitala säkerhet	2
Du har rättigheter på nätet	1	Svårlurad	2	Hur skapas fler affärer med cybersäkerhet i ditt företag?	1	DISA – datorstödd utbildning	3
Surfa Lugnt	2	Säkert Digitalt	2	Linköping Science Park – Grundläggande cybersäkerhet	2	IMY – informationssäkerhet	3
		Säkra seniorer	2	RISE – cybersäkerhetsutbildningar	3	Informationssäkerhetsmånaden	2
				Science Park Jönköping – cybersäkerhetsdagen	1	MIK Sverige (Nätverk)	3
				Stöldskyddsförenin – Hardudkoll	2	Nikka Systems (”Bli säker”)	3
				Säkerhetsdagen	1	SKR – kompetensgemenskaper	1
						Säkerhet på Nätet	3
						Säkerhetskollen	2
						Tänk säkert	3
Medelvärde:	**2,29**	**Medelvärde:**	**2,25**	**Medelvärde:**	**1,73**	**Medelvärde:**	**2,5**

Tabell. B.5: Visar individuella värden samt medelvärdet för materialomfång för initiativen inom varje huvudmålgrupp. (låg - hög).

Kunskapsnivå

Barn och unga	(1-3)	Seniorer	(1-3)	Yrkesverksamma	(1-3)	Generell	1-3
Cybersecurity Academy	2,5	Digiguiden	1	Campus totalförsvar	2,5	Cybersäkerhet genom ökad kunskap och beteendeförändring	2
Digitala lektioner	1	Motståndskraft mot telefonbedrägerier	1	Cybercampus Sverige	2,5	Dataföreningen	2,5
HackShield	1	SeniorNet Sweden	1	Cybernode	3	Digidel	1
Safer Internet Centre	1,5	SPF Seniorerna	1	Cybernorth	2	Digitala Varningsgruppen	1,5
Safer Internet Day	1	Studieförbundet Vuxenskolan	1	Framtidens brott	2,5	Din egen digitala säkerhet	1
Du har rättigheter på nätet	1	Svårlurad	1	Hur skapas fler affärer med cybersäkerhet i ditt företag?	2	DISA – datorstödd utbildning	1
Surfa Lugnt	1	Säkert Digitalt	1	Linköping Science Park – Grundläggande cybersäkerhet	1	IMY – informationssäkerhet	1
		Säkra seniorer	1	RISE – cybersäkerhetsutbildningar	2,5	Informationssäkerhetsmånaden	1
				Science Park Jönköping – cybersäkerhetsdagen	2	MIK Sverige (Nätverk)	1
				Stöldskyddsförenin – Hardudkoll	1	Nikka Systems (”Bli säker”)	1,5
				Säkerhetsdagen	2,5	SKR – kompetensgemenskaper	2
						Säkerhet på Nätet	1
						Säkerhetskollen	1
						Tänk säkert	1
Medelvärde:	**1,29**	**Medelvärde:**	**1**	**Medelvärde:**	**2,14**	**Medelvärde:**	**1,32**

Tabell. B.6: Visar individuella värden samt medelvärdet av kunskapsnivån för material i initiativen i varje huvudmålgrupp. (grundläggande - avancerat).

C

Appendix C - Enkät

Fråga	Bakgrundsvariabel	Svarsalternativ
Q2	Åldersgrupp	Yngre än 18 | 18–24 | 25–34 | 35–44 | 45–54 | 55–64 | 65–80 | äldre än 80
Q3	Kön	Man | Kvinna | Annat, nämligen: | Vill ej uppge
Q4	Högsta avslutade utbildning	Ingen avslutad | Grundskola/Motsvarande | Gymnasium/Motsvarande | Eftergymnasial utbildning kortare än 3 år | Eftergymnasial utbildning minst 3 år
Q5	Sysselsättning	Anställd | Egenföretagare | Studerande | Pensionär | Sjukskriven | Arbetssökande | Annat, nämligen:
Q6	Mest använda digitala enhet	Mobiltelefon | Dator | Surfplatta

Tabell. C.1: Bakgrundsvariabler i enkäten och deras svarsalternativ.

Fråga	Kunskapsvariabel	Beskrivning/Svarsalternativ
Q7	Kunskapsbedömning (cybersäkerhet)	Linjär skala 1-5 (1 = mycket låg, 5 = mycket hög)
Q8	Kännedom om folkbildande cybersäkerhetsinitiativ	Ja | Nej
Q8xB	Kända initiativ	Om Q8 = ”Ja”, fritext
Q9	Kännedom om informationskällor	Ja | Nej
Q9xB	Kända informationskällor	Om ”Ja” svarades på Q9, fritext

Tabell. C.2: Kunskapsvariabler i enkäten samt deras beskrivning/svarsalternativ.

Fråga	Beteendevariabel	Svarsalternativ
Q10	Ändrat beteende efter att ha tagit del av information	Ja | Nej | Vet inte | Har inte tagit del av information
Q11	Använda säkerhetsåtgärder	Starka lösenord | Tvåfaktorsautentisering | Antivirusprogram | Uppdaterar mina enheter regelbundet | VPN | Lösenordshanterare | Skärmlås | Backup av filer | Försiktighet med länkar och e-post | Inget av ovanstående/vet ej | Annat, nämligen: fritext

Tabell. C.3: Variabler för frågor 10–11 i enkäten samt beskrivning/svarsalternativ.

Fråga	Attityd- och behovsvariabel	Svarsalternativ
Q12	Bedömning av målgrupper med störst utbildningsbehov	Barn och unga | Vuxna | Äldre | Personer med funktionsvariationer | Personer med bristande kunskaper i svenska | Annan, nämligen: | Alla lika mycket
Q13	Föredragen inlärningsmetod av cybersäkerhet	Genom digitala föreläsningar | Genom fysiska föreläsningar | Genom information som skickas till mig digitalt, exempelvis via e-post | Genom självstudier via en digital plattform, exempelvis Youtube eller annan webbsida | Utförlig skriftlig information, exempelvis böcker | Genom att spela spel | Genom att delta i simuleringar (uppleva säkerhetsincidenter i en kontrollerad miljö) | Som tips vid mina dagliga aktiviteter, exempelvis lösenordstips när jag ska skapa ett konto | Reklam i form av exempelvis affischer eller broschyrer | Genom tips eller stöd från exempelvis vänner, familj eller kollegor | Lyssna på inspelat material, exempelvis en podcast eller ljudbok | Annat, nämligen:

Tabell. C.4: Variabler för frågorna 12–13 i enkäten, avseende deltagarnas attityder och behov, samt tillhörande svarsalternativ.

Referenser

[1] Maria Bada, Angela M Sasse, and Jason RC Nurse. “Cyber security awareness campaigns: Why do they fail to change behaviour?” In: *arXiv preprint arXiv:1901.02672* (2019).

[2] S. Baki and R. M. Verma. “Sixteen Years of Phishing User Studies: What Have We Learned?” In: *IEEE Transactions on Dependable and Secure Computing* 20.2 (2023), pp. 1200–1212. DOI: 10.1109/TDSC.2022.3151103.

[3] D. Baltuttis, T. Teubner, and M. T. P. Adam. “A Typology of Cybersecurity Behavior Among Knowledge Workers”. In: *Computers & Security* 140 (2024), p. 103741. DOI: 10.1016/j.cose.2024.103741.

[4] Begripsam and CKF Dalarna. *Svenskarna med funktionsnedsättning och internet 2023*. 2025. URL: https://www.begripsam.se/forskning/internet/2023-rapporter-och-resultat (visited on 06/29/2026).

[5] D. Branley-Bell et al. “Exploring Age and Gender Differences in ICT Cybersecurity Behaviour”. In: *Human Behavior and Emerging Technologies* 2022.1 (2022), p. 2693080. DOI: 10.1155/2022/2693080.

[6] *Det här är cybersäkerhetslagen*. 2026. URL: https://www.ncsc.se/sv/radgivning-och-stod/cybersakerhetslagen-nis2/det-har-ar-cybersakerhetslagen/ (visited on 06/29/2026).

[7] *Digg – Myndigheten för digital förvaltning*. URL: https://www.digg.se (visited on 06/29/2026).

[8] European Commission. *Digital Economy and Society Index (DESI) 2022*. 2022. URL: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (visited on 06/29/2026).

[9] Europol. *The Evolving Threat Landscape: How Encryption, Proxies and AI are Expanding Cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*. Tech. rep. Luxembourg: Publications Office of the European Union, 2026. DOI: 10.2813/5737847.

[10] Jesper Holgersson, Joakim Kävrestad, and Marcus Nohlberg. “Cybersecurity and digital exclusion of seniors: what do they fear?” In: *International symposium on human aspects of information security and assurance*. Springer. 2021, pp. 12–21.

[11] W. C. H. Hong et al. “The Influence of Social Education Level on Cybersecurity Awareness and Behaviour”. In: *Education and Information Technologies* 28.1 (2023), pp. 439–470. DOI: 10.1007/s10639-022-11121-5.

[12] Kevin Johansson et al. “Improving cybersecurity awareness among SMEs in the manufacturing industry”. In: *SPS2022: Proceedings of the 10th Swedish Production Symposium*. SAGE Publications 1 Oliver’s Yard, 55 City Road, London, EC1Y 1SP. 2022, pp. 209–220.

[13] J. Kävrestad. *Identifiering av behov och uppfattningar kring cybersäkerhetsmedvetenhet hos olika användargrupper (ICANP)*. Mar. 2026. URL: https://hj.diva-portal.org/smash/record.jsf?pid=diva2%3A2044220&dswid=-4607 (visited on 06/29/2026).

[14] J. Kävrestad, R. Pettersson, and M. Nohlberg. *The Language Effect in Phishing Susceptibility*. 2020. URL: https://api.semanticscholar.org/CorpusID:232389608 (visited on 06/29/2026).

[15] J. Kävrestad et al. “Survey of Users’ Willingness to Adopt and Pay for Cybersecurity Training”. In: *Human Aspects of Information Security and Assurance*. Ed. by N. Clarke and S. Furnell. Cham: Springer International Publishing, 2022, pp. 14–23. DOI: 10.1007/978-3-031-12172-2_2.

[16] W. Li et al. “Experimental Investigation of Demographic Factors Related to Phishing Susceptibility”. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. University of Hawai’i at Mānoa, 2020. DOI: 10.24251/HICSS.2020.274.

[17] *Myndigheten för civilt försvar*. URL: https://www.mcf.se/sv/ (visited on 06/29/2026).

[18] J. Nicholson, L. Coventry, and P. Briggs. “If It’s Important It Will Be A Headline: Cybersecurity Information Seeking in Older Adults”. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 2019, pp. 1–11. DOI: 10.1145/3290605.3300579.

[19] *NIS 2-direktivet: säkra nätverks- och informationssystem*. Jan. 2026. URL: https://digital-strategy.ec.europa.eu/sv/policies/nis2-directive (visited on 06/29/2026).

[20] Norton. *115 Cybersecurity Statistics + Trends to Know*. URL: https://us.norton.com/blog/emerging-threats/cybersecurity-statistics (visited on 06/29/2026).

[21] Malcolm Pattinson et al. “Matching training to individual learning styles improves information security awareness”. In: *Information and Computer Security* 28.1 (2019), pp. 1–14. ISSN: 2056-4961. DOI: https://doi.org/10.1108/ICS-01-2019-0022. URL: https://www.sciencedirect.com/science/article/pii/S2056496119000278.

[22] A Reeves, P Delfabbro, and D Calic. “Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue”. In: *SAGE open* 11.1 (2021), p. 21582440211000049.

[23] J. Simonet and S. Teufel. “The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users”. In: *ICT Systems Security and Privacy Protection*. Ed. by G. Dhillon et al. Cham: Springer International Publishing, 2019, pp. 194–208. DOI: 10.1007/978-3-030-22312-0_14.

[24] Statistikmyndigheten SCB. *Antal pågående anställningar efter anställningstid, kön och sektor*. URL: https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__AM__AM0211__AM0211A/PagaendeAnstAnstTid/ (visited on 06/29/2026).

[25] Statistikmyndigheten SCB. *Företagens ekonomi 2023*. URL: https://www.scb.se/hitta-statistik/statistik-efter-amne/naringsverksamhet-och-utrikeshandel/foretagens-produktion-forsaljning-och-ekonomi/foretagens-ekonomi/pong/statistiknyhet/foretagens-ekonomi-2023/ (visited on 06/29/2026).

[26] S. Talib, N. L. Clarke, and S. M. Furnell. “An Analysis of Information Security Awareness within Home and Work Environments”. In: *2010 International Conference on Availability, Reliability and Security*. 2010, pp. 196–203. DOI: 10.1109/ARES.2010.27.

[27] N. A. Tamboly et al. “Rethinking Human-Centric Cybersecurity: A Mixed-Methods Analysis of Incident Severity Determinants”. In: *Computer and Information Science* 19.1 (Feb. 2026), p. 1. DOI: 10.5539/cis.v19n1p1.

[28] A. C. Tricco et al. “PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation”. In: *Annals of Internal Medicine* 169.7 (Oct. 2018), pp. 467–473. DOI: 10.7326/M18-0850.

[29] P. Wang and P. Lutchkus. “Psychological Tactics of Phishing Emails”. In: *Issues in Information Systems* 24.2 (2023), pp. 71–83. DOI: 10.48009/2_iis_2023_107.

[30] M. Whitty et al. “Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords”. In: *Cyberpsychology, Behavior, and Social Networking* 18.1 (2014), pp. 3–7. DOI: 10.1089/cyber.2014.0179.

[31] L. H. Yeo and J. Banfield. “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis”. In: *Perspectives in Health Information Management* 19.2 (Mar. 2022), p. 1i.