



MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA

Förtroendet för den digitala säkerheten **håller på att vända i en mer positiv riktning**

– för första gången i barometerns historia

Barometern för digital säkerhet 2026

Innehållsförteckning

Sammanfattning.....	3
Genomförande och användning av undersökningen.....	8
Förtroendet för den digitala världen stärks.....	9
Digitala tjänster och enheter ökade förtroendet.....	10
Fundamentet består av myndigheter, finansbranschen och inhemskhet.....	11
Användningen av artificiell intelligens ökar snabbare än förtroendet.....	12
Digitala tjänster används i stor utsträckning och deras betydelse har identifierat.....	13
Den egna uppfattningen om säkerhetsfärdigheter motsvarar inte verkligheten.....	14
Oron över bedrägerier ökar, men resiliensen förbättras.....	15
Finländarna tror att de känner igen bedrägerier.....	16
Nätbrottslighet bekämpas genom samarbete och vaksamhet.....	18
Framgångsrika bedrägerier har fortfarande betydande konsekvenser.....	19
Information om digitala bedrägerier förmedlas sällan till dem som kan agera.....	20
Kommunikation och tydliga verksamhetsmodeller är de viktigaste skyddsmetoderna.....	21
Den digitala säkerheten håller på att vända till det bättre.....	22
12 centrala indikatorer att följa upp.....	23
Tio anvisningar för digitala användare – så här undviker du digitala bedrägerier och så här ska du göra om du blir lurad.....	24
12 rekommendationer för organisationer och föreningar.....	26

Barometern för digital säkerhet är en årlig undersökning om digital säkerhet som genomförs av Myndigheten för digitalisering och befolkningsdata.

Undersökningen har publicerats årligen sedan 2020.

Målgruppen för undersökningen är myndiga personer som är bosatta i Finland.

Totalt 1 250 personer svarade på undersökningen 2026, som genomfördes i juli 2026.

MER INFORMATION

Kimmo Rousku

VAHTI-generalsekreterare, ledande specialsakkunnig
 fornamn.efternamn@dvv.fi eller digiturva@dvv.fi
 Tfn 0295 536 000 (växel)



Sammanfattning

Barometern för digital säkerhet 2026 visar att det har skett en betydande vändning i den digitala säkerheten ur medborgarnas synvinkel. För första gången i barometerns historia utvecklas flera centrala indikatorer samtidigt i en positiv riktning:

- den långvariga minskningen av förtroendet har avstannat,
- trygghetskänslan har stärkts och
- medborgarna vidtar allt oftare konkreta skyddsåtgärder.

Förändringen beror inte på att hoten skulle ha försvunnit, utan på att finländarnas förmåga att agera trots hoten har förbättrats.

Förtroendet för de digitala tjänsternas och enheternas säkerhet har börjat öka. Förtroendeindexet förbättrades under året med sju poäng till –20 och ligger redan nära nivån år 2023. Andelen personer som upplevde att deras förtroende hade försvagats sjönk från 38 procent till 29 procent.

Förändringen är störst i de äldsta åldersgrupperna där förtroendet för de digitala tjänsternas och enheternas säkerhet har förbättrats mest: bland 65–74-åringarna steg indexet med 22 poäng och bland 75–99-åringarna med 18 poäng.

Av respondenterna anser 86 procent att deras vardag i den digitala miljön är trygg, vilket är fyra procentenheter mer än året innan.

Inhemskt ursprung är ett trumfkort

Välkändhet och inhemskt ursprung ökar förtroendet för den digitala världen. 70 procent anser att Finlands digitala verksamhetsmiljö är säker och 54 procent bedömer att cybersäkerheten och den digitala säkerheten förverkligas bättre här än i de flesta EU-länder.

87 procent litar på myndigheter och aktörer inom finansbranschen i fråga om behandlingen av deras uppgifter. Skillnaden mellan inhemskt och utländskt ursprung är skarp: 70 procent litar på inhemska webbutiker och 20 procent på utländska webbutiker.

I Finland är också förtroendet för det innehåll som myndigheterna producerar starkt: 88 procent av respondenterna litar på myndigheternas innehåll. Denna siffra har hållits på samma nivå sedan 2023. Av finländarna litar 66 procent på inhemska nyhetsmedier och 50 procent på utländska nyhetsmedier.

Förtroendet är koncentrerat till aktörer vars ansvar är tydligt och vilka upplevs som en del av det finländska samhället.



*I Finland råder ett starkt
förtroende för myndig-
heternas information.*

Förtroendet för artificiell intelligens släpar efter

Artificiell intelligens blir vanligare snabbare än förtroendet för AI byggs upp. Andelen som använder artificiell intelligens minst varje månad har ökat från 20 procent till 47 procent på två år och andelen som använder artificiell intelligens dagligen har ökat från 4 procent till 16 procent. Användningen är inte längre fokuserad till unga.

Förtroendet för AI-tjänster ligger långt efter: endast 23 procent litar starkt på informationssäkerheten för AI-tjänster eller det innehåll de producerar. AI-läskunnighet håller på att bli en central färdighet inom digital säkerhet.

Finländarna bedömer sin egen kompetens inom digital säkerhet som bättre än deras beteende ger anledning till.

89 procent av finländarna bedömde att deras färdigheter inom digital säkerhet var bra. Trots det skulle 12 procent logga in i nätbanken under ett telefonsamtal på begäran av en person som presenterar sig som representant för banken, 6 procent skulle klicka på en inloggningslänk som skickats i en banks eller myndighets namn och 22 procent hade under året reagerat på något som visade sig vara ett bedrägeriförsök.

Utvecklingen går dock i rätt riktning: åtskilliga kompetensmätare förbättrades med 6–8 procentenheter och 48 procent har förbättrat säkerheten för sina betalningsmedel.



AI-läskunnighet håller på att bli en central färdighet inom digital säkerhet.

Bedrägerier vanliga, inverkan minskar

Bedrägerier är vanliga i Finland, men deras inverkan håller på att minska. 81 procent av finländarna har utsatts för digitala bedrägerier eller bedrägeriförsök, var femte möter dem minst en gång i veckan. Samtidigt sjönk medelvärdet för jämförbara hotindikatorer från 34 procent till 30 procent under året.

Nedgången syns i alla centrala kanaler, men är allra störst när det gäller textmeddelanden. Detta beror bland annat på att nätbrottslingarnas verksamhet i Finland har kunnat begränsas med tekniska medel genom ett omfattande samarbete mellan myndigheterna och näringslivet.

Finansbranschen, teleoperatörerna och myndigheterna har utvecklat lösningar som till exempel kan förhindra åtkomst till bedrägerisidor inrättade av brottslingar samt försvåra förfalskning och utnyttjande av avsändaridentifikationer för textmeddelanden vid bedrägerier.

Även om oron för bedrägerier har ökat, upplevs bedrägerierna påverka den egna vardagen och förtroendet för den digitala världen i något mindre utsträckning än tidigare. Detta tyder på att finländarnas digitala kristållighet håller på att stärkas.

Priset för framgångsrika bedrägerier förblir ändå högt. Tio procent berättar att de har förlorat pengar under året – 9 procent av dem att de förlorat över tusen euro. Detta innebär cirka 450 000 personer och uppskattade årliga förluster i storlekssklassen 128 miljoner euro enbart för privatpersoner. Dessutom bedömde 30 procent att bedrägerier orsakar betydande ekonomiska bekymmer. Skadorna som organisationerna åsamkas läggs till detta.

Utöver de ekonomiska förlusterna gör bedrägerierna människorna mer försiktiga och minskar förtroendet för digitala tjänster.



10 % berättar att de har förlorat pengar under det senaste året – av dem förlorade 9 % mer än 1 000 euro.

Viljan att anmäla måste öka

Enligt barometerns resultat har finländarna mest att förbättra när det gäller att anmäla digitala bedrägerier.

43 procent av dem som identifierat ett bedrägeri berättar inte för någon; 17 procent underrättar tjänsteleverantören, 12 procent informerar banken och 7 procent polisen. Även i de fall som ledde till brott låter 42 procent bli att göra en brottsanmälan. Det finns dock ingen anledning att skämmas om man blir utsatt för ett digitalt bedrägeri, eftersom även de främsta experterna inom området blir lurade och förlorar pengar.

Underlåtelsen att anmäla försämrar myndigheternas, bankernas och operatörernas lägesbild av digitala bedrägerier och fördröjer bekämpningen av dem.

Finlands styrka är inte ett lågt antal bedrägerier utan växande kapacitet att agera trots bedrägerier.

Medborgarnas kompetens inom digital säkerhet har förbättrats och det är viktigt att fortsätta utveckla den. Säkerheten kan dock inte grunda sig på att varje enskild användare ska identifiera allt mer trovärdiga och tekniskt avancerade bedrägerier. Nästa steg i utvecklingen är att ytterligare stärka säkerheten i tjänsternas strukturer, processer och tekniska skydd. Det ska vara lätt för användaren att säkerställa att kontakten är äkta, anmäla misstänkt verksamhet och få skydd även när han eller hon inte själv identifierar bedrägeriet.

Samtidigt behövs ett smidigare samarbete och en tydligare ansvarsfördelning mellan myndigheterna, finansbranschen, teleoperatörer, digitala plattformar och tjänsteleverantörer. Målet är en miljö där en säker verksamhet är lättast för användaren och det primära alternativet.



Säkerheten måste fungera också när en människa misstar sig.

Genomförande och användning av undersökningen

Undersökningen Barometern för digital säkerhet som genomförs av Myndigheten för digitalisering och befolkningsdata utreder vuxna finländares kompetens inom cybersäkerhet och digital säkerhet, deras attityder och deras erfarenheter av säkerheten i den digitala verksamhetsmiljön.

Målet är att skapa en helhetsbild av hur finländarna använder digitala tjänster, hur de upplever sin egen kompetens och säkerhet samt hur de förhåller sig till aktuella fenomen och hot i den digitala världen.

Barometern för digital säkerhet har genomförts sedan 2020. Undersökningens koncept förnyades hösten 2022, då forskningsbyrån Vastakaiku Oy valdes till genomförare av undersökningen. Undersökningsmaterialet samlas in med hjälp av M3-panelen som administreras av Bilendi Oy.

Denna rapport behandlar resultaten från Barometern för digital säkerhet 2026. Resultaten jämförs delvis med tidigare resultat från Barometern för digital säkerhet 2023–2025.

Undersökningens målgrupp är myndiga personer som bor i Finland. Enkäten 2026 besvarades av 1 250 personer i juli 2026. Resultaten är viktade

så att materialet utgör ett nationellt representativt urval enligt kön, ålder och bostadsområde. Felmarginalen i undersökningen 2026 är cirka $\pm 3,0$ procentenheter på en förtroendenivå på 95 procent.

Med hjälp av undersökningen kan man bland annat granska hur viktig den digitala världen är i finländarnas vardag och hur aktivt olika digitala tjänster och enheter används. Barometern producerar också information om medborgarnas användning av artificiell intelligens och förtroendet för den samt om hur finländarna bedömer situationen beträffande cybersäkerhet och digital säkerhet i Finland.

I undersökningen granskas dessutom finländarnas egen bedömning av sin kompetens inom digital säkerhet, deras känsla av säkerhet i vardagen och de digitala hot de stöter på. Samtidigt utreds hur mycket finländarna litar på olika aktörer och digitala tjänster när det gäller en säker behandling av personuppgifter och andra viktiga uppgifter.

År 2026 har man också lagt till nya frågor i undersökningen som kan användas för att jämföra till exempel hur Finland placerar sig internationellt.

I slutet av rapporten listar vi åtta anvisningar för användare av digitala tjänster om hur man kan

undvika digitala bedrägerier och hur man ska agera om man blir lurad. Dessutom listar vi rekommendationer för organisationer och föreningar för att öka säkerheten i hanteringen av digitala ärenden.

Resultaten från Barometern för digital säkerhet utnyttjas av Myndigheten för digitalisering och befolkningsdata för att utveckla cybersäkerheten och den digitala säkerheten, i verksamheten i ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI) samt i myndighetens egna projekt och tjänster.

Barometerns longitudinella material gör det också möjligt att år efter år följa förändringar i attityder, kompetens, beteende och förtroende i anslutning till digital säkerhet.

Mer information om VAHTI-verksamheten
dvv.fi/sv/vahti-natverket

Vi upprätthåller och utvecklar också guiden "Mina personuppgifter har stulits eller läckt ut" för medborgare:
www.suomi.fi/guider/informationsslacka

Förtroendet för den digitala världen stärks

Den viktigaste behållningen av Barometern för digital säkerhet 2026 är att det har skett en positiv förändring. För första gången i barometerns historia har flera viktiga indikatorer samtidigt vänt i en bättre riktning. Förtroendet för den digitala värld-

den försämrats inte längre på samma sätt som under tidigare år, utan trygghetskänslan har stärkts och finländarna har allt oftare vidtagit konkreta åtgärder för att förbättra sin egen säkerhet.

Förtroendet har vänt i en bättre riktning, men det finns fortfarande mycket att utveckla.

Skadorna som åsamkas av digitala bedrägerier kan vara betydande och påverka den bedragnas ekonomi negativt.

Organisationer bör utveckla och öva sina processer för att hantera digitala bedrägerier.



Digitala tjänster och enheter ökade förtroendet

Den tydligaste förändringen syns i förtroendet för säkerheten hos digitala tjänster och enheter.

Förtroendeindexet förbättrades med sju poäng från 2025 till 2026: från -27 till -20. Indexet består av skillnaden mellan dem som upplever att deras förtroende har stärkts och dem som upplever att förtroendet har försvagats.

Andelen personer som upplevde att deras förtroende hade försvagats sjönk från 38 procent till 29 procent. 62 procent uppger att deras förtroende har förblivit oförändrat och 9 procent att förtroendet har stärkts.

Resultatet för 2026 ligger redan mycket nära 2023 års nivå, då indexet var -19.

Respondenterna motiverar stärkandet av förtroendet med utvecklingen av skyddsmetoder, identifiering, övervakning och förhindrande av bedrägerier, ökad kommunikation om digital säkerhet samt bankers, operatörers och myndigheters åtgärder. Respondenterna anser också att den egna kompetensen och försiktigheten har ökat.

Förtroendet försvagas å sin sida av det ökade antalet bedrägerier och deras trovärdighet, de allt mer utvecklade bedrägerierna som möjliggörs av artificiell intelligens samt upplevelsen av att ansvaret för säkerheten till stor del faller på användaren själv.

	Förtroendeindex	Förändring jämfört med föregående år
2023	-19	
2024	-26	-7
2025	-27	-1
2026	-20	+7

Mellan 2023 och 2024 försämrades förtroendet kraftigt. Detta kan delvis förklaras av ett dataintrång riktat mot Helsingfors stads sektor för fostran och utbildning som fick stor publicitet våren 2024. Barometermaterialet visar dock inte i sig något orsakssamband mellan en enskild händelse och en förändring i förtroendet.

Stor förändring i de äldsta åldersgrupperna

Förtroendet för säkerheten hos digitala tjänster och enheter har ökat särskilt bland 25–34-åringar och personer över 64 år. Under året steg till exempel förtroendeindexet för 65–74-åringar från -42 till -20, dvs. med 22 poäng, och för 75–99-åringar från -49 till -31, dvs. med 18 poäng.

86 procent av finländarna anser att deras dagliga verksamhet i den digitala verksamhetsmiljön är ganska eller mycket säker. Detta är fyra procentenheter mer än ett år tidigare. 10 procent upplever sin verksamhet som osäker.

Bland 18–24-åringarna ökade säkerhetskänslan med åtta procentenheter under året och bland 75–99-åringarna med nio procentenheter.

Fundamentet består av myndigheter, finansbranschen och inhemskhet

År 2026 togs nya frågor med i barometern. Svaren på dessa frågor stärker bilden av Finland som ett säkert digitalt samhälle.

70 procent av respondenterna anser att Finlands digitala verksamhetsmiljö är säker och endast 3 procent är helt av annan åsikt. Dessutom bedömde 54 procent att cybersäkerheten och den digitala säkerheten i Finland genomförs bättre än i de flesta andra EU-länder. 17 procent är av annan åsikt om påståendet, men nästan en tredjedel kan inte ta ställning till det. Detta vittnar delvis om hur utmanande frågan är.

Förtroendet för samhällets centrala institutioner är särskilt starkt.

Av finländarna litar 87 procent på aktörer inom finansbranschen och myndigheterna när det gäller säker behandling av personuppgifter och andra viktiga uppgifter. Båda dessa resultat har hållits på samma höga nivå som året innan. 81 procent av respondenterna litar på sin arbetsgivare.

Finländarna litar på inhemska webbutiker och innehåll

Även inhemskt ursprung verkar öka förtroendet. Som en ny fråga undersökte vi förtroendet för Suomi.fi-tjänsten. Av respondenterna litar 82 procent mycket på Suomi.fi-tjänsten. 70 procent litar på inhemska webbutiker och endast 20 procent på utländska webbutiker.

Förtroendet för webbutikerna har dock minskat: i fråga om inhemska webbutiker från 75 procent till 70 procent och i fråga om utländska från 23 procent till 20 procent. Orsaken är sannolikt falska webbutiker och andra bedrägerier i anslutning till betalning.

Det är anmärkningsvärt att andelen som har förlorat pengar i falska webbutiker samtidigt har minskat från 10 procent till 7 procent. Förtroendet har alltså försämrats trots att de faktiska förlusterna har minskat.

Betydelsen av inhemskt ursprung syns också när det gäller innehåll. 88 procent av finländarna litar mycket på innehåll som myndigheterna producerar, exakt lika många som året innan. 66 procent litar på välkända inhemska nyhetsmedier, medan motsvarande andel i fråga om välkända utländska nyhetsmedier är 50 procent.

Som helhet är förtroendet för den digitala världen alltså inte jämnt fördelat. Förtroendet är starkast när aktören är välkänd, dess ansvar är tydligt och den upplevs som en del av det finländska samhället.

Användningen av artificiell intelligens ökar snabbare än förtroendet

En av de mest markanta förändringarna i barometern gäller användningen av AI-tjänster.

När man för första gången frågade om artificiell intelligens 2024 använde 20 procent av finländarna artificiell intelligens minst en gång i månaden. År 2025 var andelen 31 procent och 2026 var den redan 47 procent. Den regelbundna användningen av AI-tjänster har alltså mer än fördubblats på två år.

Andelen som använder artificiell intelligens dagligen eller nästan dagligen har ökat från 4 procent till 16 procent på två år.

Samtidigt har andelen personer som inte alls använder artificiell intelligens minskat från 55 procent till 27 procent. Ökningen begränsas inte längre till unga. 66 procent av 18–24-åringarna, 59 procent av 25–49-åringarna, 43 procent av 50–64-åringarna, 31 procent av 65–74-åringarna och redan 26 procent av 75–99-åringarna använder artificiell intelligens varje månad eller oftare. De största förändringarna under året framträder bland 35–49-åringar och 65–74-åringar.

AI-innehåll är mer tillförlitligt än sociala medier

Förtroendet för artificiell intelligens ökar dock betydligt långsammare än användningen. Endast 23

procent litar mycket på att AI-tjänster behandlar personuppgifter och andra viktiga uppgifter på ett säkert sätt. Ett år tidigare var andelen 20 procent. Likaså litar endast 23 procent av finländarna mycket på det innehåll som artificiell intelligens producerar.

I nuläget litar finländarna dock mer på det innehåll som artificiell intelligens producerar än på innehållet i sociala medier, vilket 21 procent av respondenterna litar mycket på. Förtroendet för innehållet som produceras av artificiell intelligens ökade med två procentenheter under året, medan förtroendet för innehållet i sociala medier minskade med fyra procentenheter.

Bilden från 2026 är tudelad: utnyttjandet av artificiell intelligens blir snabbt normalt, men förtroendet för AI ökar inte i samma takt. Detta gör AI-läskunnighet och säker användning av AI till en av de viktigaste digitala säkerhetsfärdigheterna under de närmaste åren.

Den regelbundna användningen av artificiell intelligens har mer än fördubblats på två år.



Digitala tjänster används i stor utsträckning och deras betydelse har identifierats

Digitala tjänster har blivit en etablerad del av finländarnas vardag, eftersom 77 procent anser att digitala tjänster och applikationer är viktiga. Resultatet har i praktiken hållits på samma nivå redan i fem år. År 2026 är betydelse störst för personer under 35 år: 88–93 procent anser att tjänsterna är viktiga.

Användningen av digitala tjänster är också omfattande. 72 procent av finländarna använder digitala tjänster mycket under dagen, och bland personer under 50 år är andelen till och med 81–91 procent. Även i den äldsta gruppen, 75–99-åringar, använder hälften digitala tjänster mycket.

Finländarnas genomsnittliga skärmtid på fritiden är 21 timmar i veckan. Det är ungefär en timme mer än ett år tidigare. Personer under 35 år sam-

lar på sig en skärmtid på 27–30 timmar i veckan. 75–99-åringarna tillbringar minst tid vid skärmen, men även för dem är antalet 14 timmar, dvs. i genomsnitt två timmar per dag.

De identifierar också själva skärmtiden som ett problem. 45 procent anser att deras egen skärmtid på fritiden är för omfattande eller alltför omfattande. Av personerna under 50 år är 58–63 procent av denna åsikt.

Digitaliseringen är inte längre en separat verksamhetsmiljö utan en betydande del av det normala livet. Samtidigt blir också den digitala säkerheten allt tydligare en del av säkerheten i vardagen.

45 % anser att de använder för mycket tid framför skärmen.

Den egna uppfattningen om säkerhetsfärdigheter motsvarar inte verkligheten

Hela 89 procent av finländarna ger sig själva ett bra eller mycket bra vitsord när det gäller säker användning av digitala tjänster och enheter. Resultatet är högt, även om det har sjunkit med två procentenheter efter tre nästan identiska år.

I den äldsta åldersgruppen upplever 76 procent att deras kompetens är god, medan hela 95 procent av 35–49-åringarna är av denna åsikt.

Den egna uppfattningen om kompetensen strider dock delvis mot det faktiska beteendet.

12 procent av respondenterna skulle logga in i nätbanken under ett telefonsamtal om uppringaren presenterade sig som representant för en bank eller myndighet. 6 procent av respondenterna skulle klicka på en länk i ett e-postmeddelande eller textmeddelande som skickats i en banks eller myndighets namn och 8 procent svarar på samtal från okända utländska nummer.

Så mycket som 22 procent uppger att de under det senaste året klickat på en länk, öppnat en bilaga eller svarat på ett samtal som visade sig vara ett bedrägeriförsök.

Här framträder en av barometerns mest intressanta motstridigheter: vi betraktar oss själva som

säkrare digitala användare än vårt beteende låter förstå.

Beredskapen för bedrägeriförsök har förbättrats

Samtidigt syns emellertid också tydliga positiva förändringar i kompetensen. Allt fler vet vad de ska göra om de misstänker nätbedrägeri, kan kontrollera att en webbplats eller webbutik är säker och använder olika lösenord i olika tjänster. Dessa färdigheter har förbättrats med 6–8 procentenheter på ett år.

Mängden utbildning och information om stark autentisering har minskat exceptionellt kraftigt sedan 2025: –10 %. Detta kan delvis bero på att myndighetsposten har blivit i första hand digital. Till följd av förändringen har antalet användare av Suomi.fi-meddelanden ökat med över 2,4 miljoner sedan våren 2025. Suomi.fi-meddelanden, liksom allt fler andra digitala tjänster, kräver stark autentisering.

Även användningen av konkreta skyddsåtgärder har ökat. 48 procent av finländarna har förbättrat säkerheten i anslutning till användningen av sina betalkort och konton under det senaste året. Det är sex procentenheter mer än 2025. Ökningen är störst bland 75–99-åringar, 18–24-åringar och 50–64-åringar.

Vi betraktar oss själva som säkrare digitala användare än vårt beteende låter förstå.

Oron över bedrägerier ökar, men resiliensen förbättras

Finländarna är klart mer oroad över digitala bedrägerier än tidigare. 69 procent är ganska eller mycket oroad. Detta är hela tio procentenheter mer än ett år tidigare. Även missbruk av personuppgifter oroar 75 procent av finländarna.

En central orsak till en så betydande ökning är sannolikt att temat har diskuterats mer än tidigare i olika medier. Även egna och närståendes, släktingars, vänners och bekantas erfarenheter påverkar ökningen.

Den ökade oron syns dock inte som en negativ utveckling i alla indikatorer. 19 procent av respondenterna säger att digitala bedrägerier har påverkat deras egen vardag mycket. Detta är fyra procentenheter mindre än i fjol.

Hälften av respondenterna anser att bedrägerier har påverkat förtroendet för det digitala samhället mycket, men även här har andelen minskat med tre procentenheter jämfört med året innan.

Också samhällets beredskap bedöms vara något bättre än tidigare. 44 procent av finländarna anser att Finlands beredskap att förhindra och bekämpa digitala bedrägerier är god. Detta är tre procentenheter mer än i fjol. Majoriteten, dvs. 56 procent,

anser ändå att Finlands beredskap fortfarande är dålig.

Samtidigt är 91 procent av respondenterna beredda att anstränga sig för att trygga sin egen säkerhet på nätet. Siffran har förbättrats med två procentenheter på ett år.

Den digitala säkerheten betraktas dock inte i lika hög grad som tidigare som individens uppgift. Andelen som anser att den digitala säkerheten i första hand är individens ansvar har minskat från 75 procent till 71 procent.

Resultatet kan tyda på att det håller på att uppstå en ny balans i tänkandet: människor är beredda att ta ansvar för sin egen säkerhet, men den digitala säkerheten uppfattas inte längre enbart som individens uppgift.

91 procent är beredda att anstränga sig för att trygga sin säkerhet.

Finländarna tror att de känner igen bedrägerier

Finländarnas tillit till sin egen förmåga att identifiera bedrägerier är hög i en internationell jämförelse. 86 procent bedömde att de är ganska eller mycket säkra på att de känner igen ett digitalt bedrägeri.

I Global Anti Scam Alliances (GASA) Europajämförelse 2026* var motsvarande andel 71 procent, dvs. Finland ligger 11 procentenheter högre.

En stark tillit till den egna förmågan att känna igen bedrägerier innebär dock inte att man inte skulle exponeras för digitala bedrägerier. 81 procent av finländarna har råkat ut för digitala bedrägerier eller bedrägeriförsök under de senaste 12 månaderna, medan det europeiska jämförelsetalet är 75 procent.

Var femte finländare berättar att de stöter på bedrägerier minst varje vecka och 5 procent till och med dagligen eller nästan dagligen.

Den höga förekomsten av digitala bedrägerier i Finland kan delvis förklaras av den höga digitaliseringsgraden i vårt samhälle: vi har en heltäckande och välfungerande digital infrastruktur, elektroniska tjänster och betalningssystem används i stor utsträckning och nästan alla använder någon smart enhet. Dessutom är befolkningens språkkunskaper goda. Dessa faktorer gör Finland till ett attraktivt mål även för internationell nätbrottslighet.

Under AI-eran fungerar språket inte längre som skydd

Samtidigt kan idén om Finland som ett slags "Mumindal" i den digitala världen ha bibehållits, ett tryggt samhälle i Nordens innersta delar som skyddas av det geografiska läget och det internationellt sällsynta finska språket. Det finns allt färre grunder för denna trygghetskänsla.

Nätbrottsligheten är global och geografin ger inget betydande skydd mot den. Den snabba utvecklingen av artificiell intelligens påverkar också det skydd som språket erbjuder: det är lättare än tidigare att producera högklassiga finskspråkiga bedrägerimeddelanden, diskussioner, tal och videor.

Artificiell intelligens gör det möjligt att producera allt trovärdigare djupa förfalskningar av ljud, bild och video. Detta gör det svårare att skilja mellan genuint innehåll och syntetiskt innehåll som har producerats eller manipulerats med AI.

EU:s AI-förordning, som började tillämpas den 2 augusti 2026, medförde nya skyldigheter, bland annat krav på att informera om användningen av AI och att märka deepfakes och annat innehåll som genererats eller manipulerats med hjälp av AI.

*Global Anti Scam Alliance (GASA): State of Scams in Europe 2026



Bluff- och nätfiskemeddelanden tas emot mer sällan än tidigare.

Åtskilliga hot uppvisar en nedåtgående trend

En annan av de största positiva signalerna 2026 är utvecklingen av de realiserade hoten. Det totala medelvärdet för jämförbara hotindikatorer sjönk från 34 procent till 30 procent under året.

E-post är fortfarande den vanligaste bluffkanalen: 71 procent av respondenterna har fått bluff- eller nätfiskemeddelanden. 48 procent har råkat ut för sms-bedrägerier, 47 procent för bedrägerisamtal, 42 procent för bedrägeriförsök i sociala medier och 33 procent för bedrägerier via snabbmeddelandeapplikationer.

Åtskilliga vanliga bedrägeriformer har minskat i antal. Andelen som fått bluff- och nätfiske-meddelanden per e-post sjönk från 78 procent till 71 procent, andelen som fått sådana via SMS från 62 procent till 48 procent och andelen som fått bedrägerisamtal från 54 procent till 47 procent. När det gäller snabbmeddelandeapplikationer sjönk andelen från 42 procent till 33 procent.

I fråga om SMS-bedrägerier är förändringen alltså hela -14 procentenheter och i fråga om snabbmeddelandebedrägerier -9 procentenheter.

Störningar och avbrott i digitala tjänster påverkar människors möjligheter att sköta sina ärenden di-

gitalt. Av de svarande uppger 36 procent att de har varit förhindrade att sköta sina ärenden på grund av störningar. Andelen har ökat med tre procentenheter jämfört med 2025.

Andelen personer som förlorat pengar till falska webbutiker minskade från 10 procent till 7 procent, andelen som förlorat pengar till följd av utpressning eller digitalt bedrägeri från 7 procent till 6 procent och andelen som förlorat pengar på grund av identitetsstöld från 6 procent till 5 procent.

Finlands styrka är alltså inte att bedrägerierna är få. Styrkan verkar snarare ligga i att medborgarna känner igen bedrägerier relativt bra och lär sig att hantera dem.



I Finland förekommer många bedrägerier, men deras antal har minskat och de identifieras bättre.

Nätbrottslighet bekämpas genom samarbete och vaksamhet

I Finland har man under det senaste året tagit i bruk flera nya tekniska metoder för att bekämpa digitala bedrägerier.

Spärrlista begränsar åtkomsten till skadliga adresser

Ett sätt att bekämpa digitala bedrägerier är en så kallad spärrlista som genomförs i samarbete mellan finansbranschen, teleoperatörer och myndigheter och som snabbt kan begränsa åtkomsten till skadliga webbadresser som nätbrottslingar använder.

När en ny bedrägeriwebbplats eller en annan skadlig adress identifieras och anmäls till tjänsten kan den i bästa fall spärras inom några minuter och vanligtvis inom några timmar.

Spärrlistan är ett effektivt verktyg, men för att den ska fungera krävs det att skadliga webbadresser upptäcks och anmäls snabbt. Det är alltså fortfarande viktigt att anmäla nya bluffsidor och skadliga länkar.

Avsändaridentifikationer för textmeddelanden ska godkännas på förhand

Finland gjorde SMS-bedrägerier betydligt svårare i maj 2026, när de nya skyldigheterna för identifikation av avsändare trädde i kraft (Traficoms förnyade föreskrift 28 L/2025 M om interoperabilitet av kommunikationsnät och kommunikationstjänster).

Finländska telefonnummer och avsändaridentifikationer i namnform som organisationer använder i sina textmeddelanden ska godkännas på förhand. Kravet gäller förutom SMS-meddelanden även MMS- och RCS-meddelanden. Tack vare tillståndskravet förhindras i regel förfalskning av avsändaridentifikationen för en bank, myndighet eller annan känd organisation i Finland.

Meddelanden som skickats utan tillstånd visas för mottagaren med identifikationen "Okänd" och från och med 2.11.2026 med koden "Skräppost", eller så spärras de helt.

De tekniska lösningarna eliminerar inte sms-bedrägerier helt. Nätbrottslingar kan fortfarande skicka bluffmeddelanden från egna eller andra nummer de använder och styra mottagarna till exempel till skadliga webbsidor.

Därför behövs vid sidan av tekniska skyddsåtgärder även att användarna är vaksamma och har förmåga att känna igen bedrägeriförsök.

Framgångsrika bedrägerier har fortfarande betydande konsekvenser

Av dem som utsatts för ett bedrägeri har 8 procent överlåtit någon form av skyddad information som en följd av bedrägeriet. Oftast är det fråga om personuppgifter eller bank- och betalkortsuppgifter, vilka har överlåtits av 4 procent av dem som utsatts för bedrägerier.

I praktiken får brottslingen i samband med samma händelse vanligtvis också tillgång till andra personuppgifter, beroende på vilken kanal som har använts för det digitala bedrägeriet.

10 procent av finländarna uppger att de under de senaste 12 månaderna har förlorat pengar som en följd av digitalt bedrägeri, utpressning eller inköp i falska webbbutiker.

Särskilt oroväckande är att ungefär var sjätte av dem (16 %) har förlorat pengar mer än en gång. Av dem som förlorade pengar förlorade 69 procent 1–100 euro, 19 procent 101–500 euro, 3 procent 501–1 000 euro och 9 procent över 1 000 euro.

Om det enligt Statistikcentralens uppskattning finns cirka 4,5 miljoner aktiva digitala användare i Finland och 10 procent av dem har förlorat pengar till följd av digitala bedrägerier, är det fråga om cirka 450 000 finländare.

När försiktiga genomsnittliga eurobelopp används för förlusternas storlek kan det totala beloppet av de ekonomiska förlusterna uppskattas till cirka 128 miljoner euro per år. Uppskattningen är till sin storleksklass i linje med till exempel de årliga uppgifter som polisen och Finanssiala ry publicerar.

Det är viktigt att notera att uppskattningen endast gäller förluster för privatpersoner. Utöver dessa orsakas ekonomiska skador bland annat av digitala bedrägerier mot företag och andra organisationer, betalningsrörelsebedrägerier och utpressning samt betal- och kreditkortsbedrägerier.

Den totala beloppet av de direkta ekonomiska förluster orsakade av digital brottslighet i Finland är således betydligt större, men det är svårt att göra en tillförlitlig uppskattning av beloppet. Därför är det särskilt viktigt att anmäla brott, särskilt i situationer där brottet leder till att pengar går förlorade.

I fall där en brottsling fått tillgång till en persons bankkonto, kreditkort eller andra identitetsuppgifter, fick bedragaren pengarna via en kontoöverföring i drygt en tredjedel (34 %) av de digitala bedrägerierna. I cirka en fjärdedel av fallen (22 %) överfördes pengarna med betal- eller kreditkort och i 15 procent av fallen överfördes pengarna via så kallade snabbbetalningstjänster.

Det lönar sig att observera att till exempel presentkort och värdesedlar som skaffas i butiker har använts i fem procent och kryptovaluta i endast tre procent av bedrägerierna.

Finland skiljer sig på flera sätt avsevärt från resultaten i GASA Europe-undersökningen. I Europa är det betydligt vanligare än i Finland att bedragare får pengar via presentkort eller värdebevis, genom en digital plånbok (t.ex. PayPal, Apple Pay eller Google Pay), via kryptovaluta eller kryptotjänster eller i kontanter. Resultatet visar att betalningstrafiken i Finland är koncentrerad till tjänster som tillhandahålls av traditionella aktörer inom finanssektorn och att användningen av kontanter är begränsad.

Information om digitala bedrägerier förmedlas sällan till dem som kan agera

Ett av resultaten för 2026 blir i särskilt hög grad ett utvecklingsobjekt: för få bedrägerier anmäls.

43 procent av dem som utsatts för bedrägerier eller bedrägeriförsök berättade inte för någon. 34 procent berättade för en familjemedlem eller en vän, medan 17 procent anmälde fallet till leverantören av tjänsten eller plattformen, 12 procent till banken eller någon annan finanstjänst och endast 7 procent till polisen.

Situationen förändras väsentligt när den drabbade förlorar pengar i samband med bedrägeriet. Då uppger 37 procent att de anmäler fallet till banken eller betaltjänstleverantören och 30 procent till polisen. Ändå är det 13 procent av dem som förlorat pengar som inte berättar för någon om det inträffade. Även i detta avseende skiljer sig Finland positivt från övriga Europa: i Europa anmäls sådana här händelser mer sällan än i Finland.

Bristen på anmälningar syns ännu tydligare när det gäller begångna brott. Sex procent av fallen där en person utsatts för ett blufförsök ledde till ett brott, till exempel bedrägeri eller förlust av pengar eller personuppgifter. Av dessa offer gjorde 58 procent en brottsanmälan, med 42 procent inte anmälde.

Detta är ett problem på systemnivå. Om bedrägerierna inte anmäls får myndigheterna, bankerna, teleoperatörerna och serviceplattformarna ingen bra lägesbild av antalet bedrägerier, metoderna och utvecklingen. Samtidigt blir det också svårare att identifiera brottslig verksamhet, gripa gärningsmännen och förhindra deras agerande.

Att göra det enkelt, lättbegripligt och till nytta att anmäla borde lyftas fram som ett av följande utvecklingsobjekt inom digital säkerhet.

När ett bedrägeriförsök upptäcks i tid är de centrala signalerna i allmänhet mänskliga. En avsändare som verkar opålitlig väcker misstankar hos 56 procent, en misstänkt länk eller webbplats hos 54 procent och ett motstridigt eller ologiskt Suomi.fi-meddelande hos 51 procent. Ett erbjudande som verkar för bra för att vara sant identifieras som en varningssignal i 43 procent av fallen.

Det måste vara enkelt, lättbegripligt och till nytta att anmäla bedrägerier.

Kommunikation och tydliga verksamhetsmodeller är de viktigaste skyddsmetoderna

Barometerns viktigaste kvalitativa observation gäller varför bedrägerier lyckas eller misslyckas.

Av dem som förlorat pengar berättar 34 procent att bedrägeriet lyckades för att situationen verkade trovärdig och äkta. 23 procent litade på avsändaren eller den som tog kontakt och 22 procent trodde att betalningen var säker. Brådska och ett erbjudande som verkade alltför bra påverkade 20 procent av de svarande, medan bedragarens framträdande som en pålitlig organisation påverkade 19 procent.

Åldern påverkar var man får information. Bankernas, betaltjänsternas och myndigheternas kommunikation framhävs särskilt bland respondenter över 64 år. Sociala medier är däremot viktigare för unga respondenter och de sociala mediernas betydelse minskar stadigt med åldern.

Resultaten visar också vad som i praktiken hjälper medborgarna. Bankernas och betaltjänsternas kommunikation är den viktigaste enskilda faktorn som stöder igenkänning eller undvikande av bedrägerier. Denna faktor uppgavs av 47 procent av respondenterna. Näst viktigast var nyhetsmediernas kommunikation (43 procent), myndigheternas kommunikation och webbplatser (42 procent) samt egen erfarenhet av bedrägerier (41 procent).

Det informeras mycket omfattande om dessa frågor i Finland, och Finlands siffror ligger i många avseenden betydligt högre än genomsnittet i Europa.

Bedrägerier har allvarliga följder även när pengar eller personuppgifter inte går förlorade.

49 procent av dem som utsatts för ett bedrägeri har blivit försiktigare användare av digitala tjänster och 30 procent litar mindre på digitala tjänster än förut. 15 procent varnar andra i större utsträckning, 14 procent är rädda för att på nytt bli föremål för bedrägeri och 8 procent berättar att bedrägerierna har orsakat stress eller ångest.

Konsekvenserna för dem som förlorat pengar kan vara betydligt allvarigare: 15 procent har haft svårigheter att betala nödvändiga utgifter, 12 procent har varit tvungna att minska sin normala konsumtion, 10 procent har behövt ekonomiskt stöd av sina närstående och 6 procent har varit tvungna att ta lån eller skuldsätta sig.

En av Finlands styrkor är den mycket omfattande informationen till medborgarna och samarbetet mellan olika aktörer.

Knappt en tredjedel har mindre förtroende för digitala tjänster och onlinemiljöer än tidigare.

Den digitala säkerheten håller på att vända till det bättre

En positiv utveckling kan skönjas inom den digitala säkerheten, men i praktiken byggs säkerheten upp i människans vardag. Barometern för digital säkerhet 2026 ger inte en bild av ett riskfritt digitalt Finland, tvärtom: fyra av fem finländare stöter på bedrägeriförsök, var femte minst varje vecka, och oron för digitala bedrägerier har ökat kraftigt.

Den avgörande skillnaden 2026 jämfört med tidigare år är dock att ökningen av hoten inte längre automatiskt innebär att förtroendet försvagas.

- Förtroendeindexet har svängt i en bättre riktning.
- Trygghetskänslan har ökat.
- Åtskilliga bedrägeriformer påträffas i mindre utsträckning än förut.
- Medborgarna vidtar konkreta skyddsåtgärder i högre grad än tidigare.
- Man är beredd att anstränga sig mer för den digitala säkerheten.
- Man litar i hög grad på myndigheterna, finansbranschen och de centrala finländska digitala tjänsterna.

Artificiell intelligens förändrar verksamhetsmiljön i en aldrig tidigare skådad takt. Användningen av AI ökar mycket snabbare än förtroendet för AI. Artificiell intelligens stärker samtidigt medborgarnas möjligheter att skydda sig och möjliggör allt mer trovärdiga bedrägerier och andra nätbrott.

Säkerheten ska byggas in i tjänsterna

Ett centralt budskap i barometern är att det digitala samhället i Finland 2026 visar de första tecknen på ökad digital kriställighet. Förtroendet försämrats inte längre och trygghetskänslan har ökat, även om hoten inte har försvunnit och förtroendet ännu inte har återställts.

Nästa steg är inte bara bättre teknik eller mer upplysta medborgare, utan en säkerhet som byggs in i tjänsterna: ett enkelt sätt att säkerställa att en kontakt är äkta, låg tröskel för att anmäla problem och en tydlig ansvarsfördelning mellan banker, myndigheter, operatörer och plattformar.

Medborgarens kompetens är en del av helheten, inte ett substitut för den.



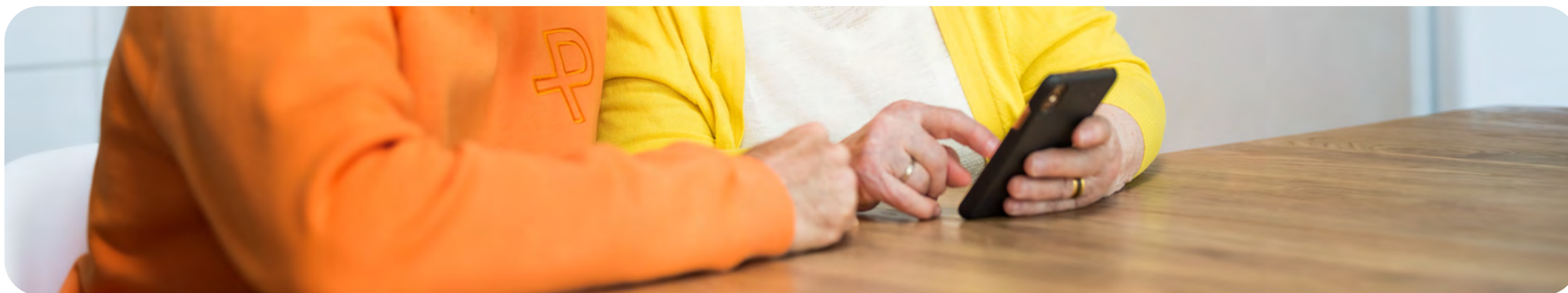
12 centrala indikatorer att följa upp

Indikator	2026	Förändring
Förtroendeindex (förstärkts – försvagats)	-20	+7 poäng
Upplever den digitala miljön i vardagen som säker	86 %	+4 %-enh.
Litar på innehåll som produceras av AI-tjänster	23 %	+2 enh.
Använder AI-tjänster minst en gång i månaden	47 %	+16 %-enh.
Bedömer att hen kan använda digitala tjänster på ett säkert sätt	89 %	-2 %-enh.
Digitala bedrägerier oroar ganska mycket eller mycket	69 %	+10 %-enh.
Realisering av hot, totalt medelvärde	30 %	-4 %-enh.
Har stött på digitala bedrägeriförsök	81 %	*
Har förlorat pengar på grund av digitalt bedrägeri	10 %	*
Anser att Finlands digitala verksamhetsmiljö är säker	70 %	*
Gjorde en polisanmälan om ett digitalt bedrägeri, bedrägeri eller annat brott	58 %	*
Berättade inte för någon om bedrägeriet	43 %	*

* ny fråga

Tio anvisningar för digitala användare

– så här undviker du digitala bedrägerier och så här ska du göra om du blir lurad



1. Stanna alltid upp när du blir uppmanad att agera snabbt

Brådska, skrämsel och påtryckningar är vanliga metoder som används av digitala bedragare. Om någon kräver att du ska agera genast, betala snabbt eller hålla något hemligt, stanna upp och fundera innan du gör något.

2. Lita inte enbart på namnet, numret eller utseendet

Ett samtal, ett meddelande eller en webbsida kan se ut att komma från en bank, myndighet, ett företag eller till och med en bekant person. Kontrollera själv kontakten via en annan kanal genom att använda ett nummer, en applikation eller en webbplats som du känner till sedan tidigare. Eller ring en vän!

3. Identifiera dig inte eller betala inte enligt någon annans anvisningar

Logga inte in i banken, godkänn inte en identifiering eller gör inte en Suomi.fi-betalning på basis av ett överraskande samtal eller meddelande. Öppna alltid själv bankens eller en annan tjänsts applikation eller webbsida. Om du använder webbläsare, skriv själv in webbadressen i webbläsarens adressfält. Gå aldrig till tjänsten via en länk du fått eller resultaten i en sökmotor.

Brottslingen kan i allmänhet inte orsaka betydande skada om han eller hon inte får tag på dina användarnamn, kan identifiera sig i tjänsterna för din räkning eller lyckas kapa din identitet.

4. Kontrollera innan du klickar, köper eller betalar

Granska avsändaren, webbsidans adress, betalningsmottagaren och om det finns något ologiskt i meddelandet. Om ett erbjudande verkar för bra för att vara sant eller om det på annat sätt väcker misstankar, fortsätt inte innan du har kontrollerat saken.

5. Skydda ditt konto och din enhet i förväg

Använd olika lösenord i olika tjänster och aktivera multifaktorautentisering alltid när det är möjligt. Uppdatera enheter och applikationer samt utnyttja de betalnings-, kort- och användargränser som banken erbjuder. Ett litet besvär i förväg kan förhindra en stor skada.

6. Om du misstänker bedrägeri, avbryt situationen omedelbart

Fortsätt inte diskussionen, klicka inte på nya länkar och skicka inte mer information. Stäng samtalet eller kommunikationen och ta i lugn och ro reda på vad som har hänt. Bedrägeriet kan ännu stoppas även om du redan har hunnit göra något, till exempel lämna ut dina uppgifter.

7. Om du gav information eller pengar, agera snabbt

Kontakta omedelbart banken eller betaltjänsten om du har betalat, överlåtit bank- eller kortuppgifter eller godkänt en misstänkt transaktion. Stäng vid behov korten och användarnamnen samt byt ut de lösenord som äventyrats.

Ju snabbare du agerar, desto bättre är möjligheterna att begränsa skadorna.

8. Anmäl händelsen – bli inte ensam

Spara meddelanden, telefonnummer, webbadresser, kvitton och annan information med anknytning till händelsen. Anmäl händelsen till banken, tjänsteleverantören och polisen samt vid behov till andra myndigheter.



9. Skydda din integritet – håll koll på ditt digitala fotavtryck

Innan du publicerar, fundera över vilka uppgifter du delar om dig själv, dina närstående eller din vardag på nätet. Undvik att publicera onödiga personuppgifter, fotografier, lokaliseringssuppgifter, resplaner och annan känslig information. Kontrollera också regelbundet applikationernas och tjänsternas sekretessinställningar samt vilka uppgifter om dig som finns offentligt på nätet.

Man behöver inte skämmas för att bli lurad: genom att anmäla hjälper du till att förhindra att andra blir föremål för samma bedrägeri. Även en liten digital ledtråd kan bidra till att fånga brottslingar!

10. Använd AI för att identifiera digitala bedrägerier

Du kan till exempel fråga AI: "Verkar den här webbplatsen vara ett digitalt bedrägeri?" Klistra in eller skriv webbadressen som du vill kontrollera efter frågan.

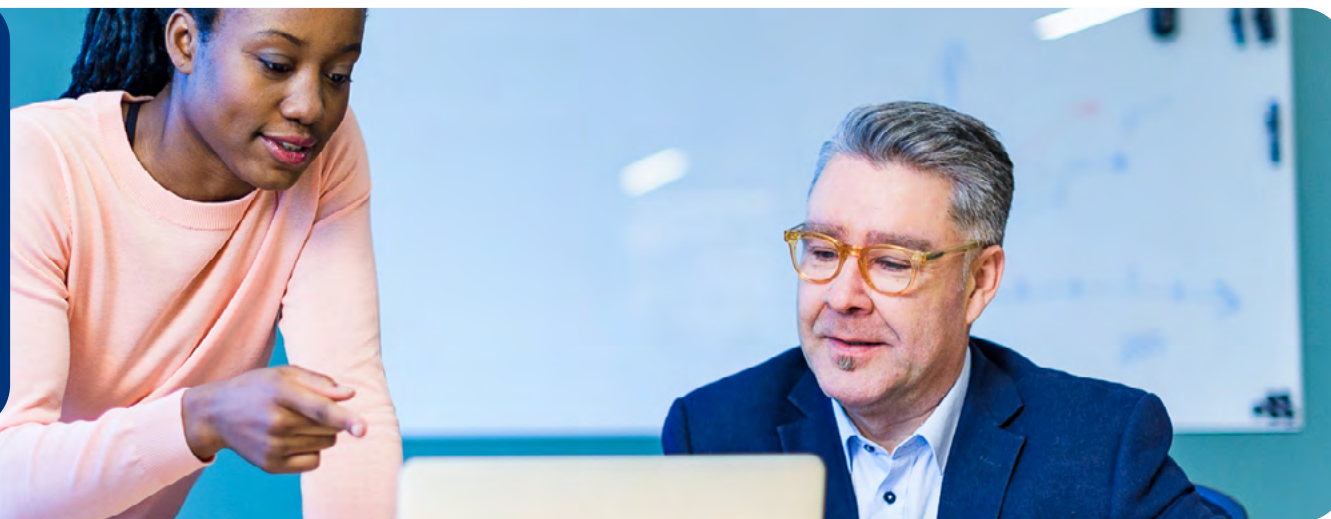
Du kan också ta en skärmbild eller ett foto av ett meddelande och be AI bedöma om det finns tecken på bedrägeri.

Kom ihåg: AI kan ha fel. Även om AI bedömer att en webbplats eller ett meddelande är säkert bör du alltid kontrollera adressen, avsändaren och andra varningssignaler innan du loggar in, betalar eller lämnar ut personuppgifter. AI är ett bra extra par ögon, inte den slutgiltiga sanningen.

12 rekommendationer för organisationer och föreningar

Den vändning av förtroendet som framträder i barometern för digital säkerhet 2026 kan göras till en bestående riktning om

- säkerheten är synlig för användaren,
- det görs enkelt att agera säkert och
- organisationerna åtar sig en aktivare roll i förebyggandet av digitala bedrägerier.



1. Gör det möjligt att anmäla digitala bedrägerier på ett och samma ställe och granska din egen process

Bygg upp en tydlig anmälnings- och serviceväg för kunden i situationer där kunden misstänker att hen har blivit utsatt för digitalt bedrägeri. Organisationen ska kunna inleda sina egna skyddsåtgärder samt vid behov hänvisa klienten till exempelvis polisens, Cybersäkerhetscentrets, dataombudsmannens byrås, bankens eller någon annan behörig aktörs tjänster.

Testa samtidigt att den egna personalen känner till processen och kan agera snabbt.

2. Öva på digitala hot i situationer som känns genuina

Låt inte utbildningen bestå av enbart anvisningar och webbkurser. Ordna övningar till exempel om bluffsamtal, nätfiske, kontoöverföringar, expressbetalningar, förfrågningar som grundar sig på brådska samt bedragare som utger sig för att vara en bank, myndighet, direktör eller annan betrodd aktör.

Lär i synnerhet organisationen att stoppa situationen, kontrollera kontakten via en annan kanal samt anmäla snabbt. Testa samtidigt om organisationens egna anmälningskanaler fungerar i praktiken.

3. Korrigera brist på utbildning inom stark autentisering

Stark autentisering i sig hindrar inte bedrägerier om användaren övertalas att godkänna en händelse som inletts av en brottsling. Lär användarna att alltid kontrollera vad de håller på att godkänna och i vilken tjänst identifieringen sker.

Understryk särskilt att man inte automatiskt ska identifiera sig med bankkoder eller mobilcertifikat på basis av överraskande samtal, meddelanden eller andra kontakter. Ge anvisningar om att avbryta situationen och öppna rätt tjänst via en bekant adress eller applikation.



4. Satsa på grundläggande färdigheter i säker användning av artificiell intelligens

Lär personalen vilka uppgifter som får matas in i tjänsterna för artificiell intelligens och vilka som inte får matas in. Ordna övningar i behandling av personuppgifter och sekretessbelagda uppgifter, granskning av svar som producerats av artificiell intelligens, källkritik samt identifiering av bedrägerier med hjälp av artificiell intelligens, såsom trovärdiga meddelanden, bilder, ljud och videor.

Instruera personalen att i sina arbetsuppgifter använda AI-tjänster som godkänts av organisationen och administreras på ett datasäkert sätt, men uppmuntra dem att lära sig mer om dessa även på fritiden.

5. Utnyttja pålitliga kommunikationskanaler i kommunikationen

Digitala bedrägerier kan inte bekämpas endast genom den kommunikation som en enskild organisation bedriver. Bankernas, myndigheternas, teleoperatörernas, nyhetsmediernas, arbetsplatsernas, läroanstalternas, organisationernas och närståendes meddelanden kan komplettera och stärka varandra.

Rikta meddelandena till olika användargrupper och till de kanaler där de uträttar ärenden. Upprepa centrala verksamhetsmodeller tillräckligt ofta och reagera snabbt på nya bedrägerifenomen.

6. Mät kompetensen utifrån beteendet, och inte bara utifrån självbedömning

Bedöm inte kompetensen inom digital säkerhet enbart genom att fråga hur bra människor själva anser att deras färdigheter är. Komplettera frågorna med situationsbaserade uppgifter, simuleringar och övningar.

Kontrollera till exempel om användarna kan avbryta en misstänkt situation, verifiera avsändaren eller kontakten via en annan kanal, kontrollera en betalningsbegäran och anmäla en misstänkt händelse. Mät framför allt den säkra verksamheten i praktiken.

7. Stöd den som blivit föremål för ett bedrägeri utan att skuldbelägga

Erbjud snabbt hjälp med att stoppa betalningar, skydda användarnamn och personuppgifter, göra en brottsanmälan samt vid behov hitta ekonomisk rådgivning och skuldrådgivning samt psykiskt stöd. Lyssna lugnt och undvik frågor som kan öka skammen eller skuldkänslorna.

Bedrägerierna har medvetet byggts upp för att utnyttja brådska, rädsla, förtroende och auktoriteter. Fokusera på sådant som ännu kan förhindras, skyddas, returneras och anmälas. Tacka för att den drabbade berättar – en snabb anmälan kan förhindra att andra blir föremål för samma bedrägeri.

8. Bygg in bekämpningen av bedrägerier i tjänsterna

Låt inte säkerheten vila enbart på användarens uppmärksamhet och förmåga att identifiera bedrägerier. Utnyttja identifiering av avvikande inloggningar, betalningar och beteende, riskbaserad tilläggsbegränsning samt ändamålsenliga begränsningar och fördröjningar i tjänsterna.

Planera användargränssnitten så att exceptionell eller riskfylld verksamhet väcker användarens uppmärksamhet före godkännandet. Det säkra alternativet ska också vara det enklaste alternativet för användaren.

Försök att använda AI-tjänster som stärker säkerheten på ett kontinuerligt sätt, dygnet runt.

9. Gör det enkelt att kontrollera att organisationens kontakter är äkta

Erbjud kunden ett enkelt sätt att kontrollera att meddelanden, samtal eller andra kontakter verkligen kommer från din organisation. Välj

välkända servicekanaler, interna meddelanden i applikationer och tydliga återuppringsförfaranden.

Undvik tillvägagångssätt som vänjer användarna vid att logga in i tjänster via länkar i överraskande meddelanden. Berätta också tydligt vad din organisation aldrig ber kunden göra per telefon, textmeddelande eller e-post.

10. Skydda särskilt betalningar och andra åtgärder som är svåra att återkalla

Identifiera i dina tjänster situationer där följderna av ett bedrägeri snabbt kan bli betydande: kontoöverföringar, tillägg av ny betalningsmottagare, ändringar av kontonummer, beviljande av användarrättigheter, utlämnande av personuppgifter och godkännande av stark autentisering.

Använd beroende på risken oberoende verifiering, godkännande som görs av två personer, betalningsgränser, tilläggsbegränsning eller kort fördröjning. Målet är att skapa en sista möjlighet att stoppa bedrägeriet före en oåterkallelig åtgärd.

11. Bekämpa aktivt bedrägerier som utförs i din egen organisations namn

Följ upp hur din organisations namn, domännamn, logotyper, telefonnummer och an-

ställdas namn används på webben. Ombesörj tekniskt skydd av e-posten, såsom SPF-, DKIM- och DMARC-definitioner.

Följ liknande domännamn, falska profiler och bluffsidor och skapa en verksamhetsmodell för snabb anmälan och nedtagning av dem. Berätta också snabbt för kunderna om en bedrägerikampanj pågår i din organisations namn.

12. Dela snabbt information om bedrägerier över organisationsgränserna

Ett upptäckt bedrägeri kan ingå i en kampanj som samtidigt riktar sig till tusentals personer och flera organisationer. Skapa en verksamhetsmodell för snabb förmedling av skadliga domännamn, URL-adresser, telefonnummer, kontonummer, betalningsmottagare och andra identifikationsuppgifter till dem som behöver dem.

Samarbeta med myndigheter, banker, teleoperatörer, teknologiföretag och andra parter. Målet är att förkorta kedjan från observation till anmälan, spärning och vid behov nedkörning av system.

Vi rekommenderar organisationer att:

- delta i den avgiftsfria årliga Taisto-övningen i cyber- och digital säkerhet:
dvv.fi/taisto
- bekanta sig med guiden "Uppgifter har stulits eller läckt ut från min organisation":
www.suomi.fi/guider/informationsslacka



**MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA**