Co-funded by the European Union

RESEARCH AND ANALYSIS

Cybersecurity, Artificial Intelligence and Digital Skills among Adults (30+)
A quantitative and evidence-based study of risks and deficits (2023–2025)

1. Scope and methodological approach

This analysis synthesizes empirical indicators and persistent trends for the period 2023–2025, based on:
official European statistics on digital skills and strategic targets through 2030;
aggregated EU-level data on cyber incidents and threats published by ENISA;
global forensic analyses of security breaches (Verizon Data Breach Investigations Report – DBIR);
economic assessments of breach costs and emerging risks related to artificial intelligence and so-called shadow AI (IBM Cost of a Data Breach Reports).

The purpose of the analysis is not descriptive, but explanatory and argumentative – to:
quantify the scale of the problem;
identify causal mechanisms;
substantiate the need for targeted training interventions for adults (30+).

2. Digital skills as a structural precondition for risk

Comparative analysis: the EU, Bulgaria and Italy

2.1. European Union – a systemic deficit amid widespread digital use

In 2023, 55.6% of the EU population (aged 16–74) had at least basic digital skills, which means that around 44% of European citizens lack the minimum set of competences required for safe participation in the digital environment.

These skills include:
managing a digital identity;
basic cyber hygiene;
secure use of online services;
recognising manipulative content and scams.

Within the Digital Decade 2030 framework, the EU has set a target for 80% of adults to have at least basic digital skills. The gap between the current situation and this target clearly shows that the deficit is not marginal but structural, with a direct impact on cybersecurity, trust in institutions, and societal resilience.

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.2. Bulgaria – systemic deficit, high vulnerability and limited digital autonomy

2.2.1. Basic digital skills

According to the Digital Decade Country Reports, only about 35.5% of the adult population in Bulgaria has at least basic digital skills. This is among the lowest levels in the EU and is far below the EU average (~55.6%).

In practice, this means that nearly two thirds of adult Bulgarian citizens:
do not have sustained skills for safe online behaviour;
use digital services without fully understanding the risks;
respond intuitively rather than in an informed way when digital incidents occur.

2.2.2. Internal inequalities and age differences

The data for Bulgaria shows a clearly pronounced age- and education-related digital divide:
lower skills among people above 45–50 years of age;
significant differences between urban and less connected regions;
a strong correlation between educational attainment and digital literacy.

2.2.3. Use of e-services and real-life practice

Despite the growing use of e-banking, e-government and social platforms, many Bulgarian users rely on these services instrumentally, without:
awareness of security settings;
stable habits for protecting personal data;
understanding the consequences of digital mistakes.

2.2.4. Advanced skills and artificial intelligence

The use of AI by citizens and small organisations often happens without understanding what data is being shared, without critical evaluation of automated outputs, and without a clear grasp of secondary risks.

2.3. Italy – below the EU average and a strong internal digital divide

2.3.1. Basic digital skills

45.8% of Italy's population (aged 16–74) has at least basic digital skills – a value below the EU average, meaning that more than half of Italian citizens are vulnerable in the digital environment.

2.3.2. Age and social inequalities

Among people over 65, only 17.7% have at least basic digital skills. There are also strong regional differences, as well as a dependency on educational attainment.

2.3.3. Limited internet and service use
Around 16.3% of Italians have never used the internet, which is an indicator of digital exclusion and increased vulnerability at first contact with online services.

2.3.4. Advanced skills and artificial intelligence
Only about 8% of enterprises use AI, while the share of ICT specialists (~4.1%) remains below the EU average – an indicator of slow adaptation to advanced technologies.

3. Cyber threats in the EU: an empirical picture of risk

ENISA data for 2023–2024 shows persistently high levels of cyber incidents, with leading threat categories including:
ransomware and extortion;
social engineering;
attacks against service availability (DDoS);
data compromise;
supply-chain attacks.

By sector, a significant share of incidents affect:
public administration – 19%;
transport – 11%;
the financial sector – 9%.

These sectors are directly connected to citizens' everyday lives and make the risk "invisible but constant".

4. The human factor as the dominant cause of breaches

4.1. Data from the Verizon DBIR 2024

According to the Verizon DBIR 2024, the human factor is involved in 68% of all breaches. This includes:
social engineering;
errors in handling information;
compromised credentials;
poor decisions under time pressure and emotional stress.

4.2. Ransomware and double extortion
Ransomware/extortion scenarios appear in around 32% of breaches, often involving not only encryption but also theft and extortion using personal data.

5. Social engineering and financial losses

In 2023:
over 22,000 BEC (Business Email Compromise) cases;
over USD 2.9 billion in financial losses.

These patterns also replicate in individual contexts (fake invoices, “boss” emails, payment and delivery scams).

6. The economic cost of breaches and the role of AI

6.1. Cost of breaches
IBM 2024: USD 4.88 million average global cost
IBM 2025: USD 4.4 million, with a slight decline but still a structurally high level

6.2. AI oversight gap
IBM 2025 reports:
63% of organisations without AI governance policies
97% without adequate access control in AI-related incidents

These deficits are directly applicable to the civic context as well.

7. Synthesis of quantitative findings

EU: ~55.6% with at least basic digital skills
Bulgaria: ~35.5%
Italy: ~45.8%
Human factor: 68% of breaches
BEC losses: >USD 2.9 billion
AI governance deficit: 63%

8. Conclusion

Data for 2023–2025 indicates that the digital skills deficit among adults is systemic, the human factor is dominant in breaches, and artificial intelligence adds a new layer of complexity and risk.
Training for adults in cybersecurity, AI and digital skills should be viewed as a strategic intervention for societal resilience, rather than as an additional educational activity.

Strengthening the digital resilience of adults (30+)
A policy-analytical review of cybersecurity, artificial intelligence and digital skills in the European context

Executive summary

The rapid digitalisation of public services, labour markets and social interactions is fundamentally transforming European societies. The available empirical evidence, however, shows that a significant share of the adult population lacks the digital skills required for safe, autonomous and informed participation in this process. This policy-oriented analysis examines EU and international data for 2023–2025, focusing on cybersecurity, the human factor and the penetration of artificial intelligence, with special attention to adults over 30. The analysis argues that the mismatch between digital dependence and actual digital competence constitutes a systemic societal risk, requiring targeted public interventions at both European and national level.

Defining the problem: digital dependence without digital resilience

Across the European Union, digital technologies have become the primary interface between citizens and key public systems – banking, public administration, healthcare, education and employment. For adults over 30, participation in the digital environment is no longer a matter of choice, but a structural necessity. Nevertheless, European Commission data shows that only around 55–56% of the EU population has at least basic digital skills. In Bulgaria this share is approximately 35.5%, and in Italy around 45.8%.

This creates a condition that can be defined as “digital dependence without digital resilience” – a situation in which citizens are compelled to use digital systems they do not sufficiently understand and over which they have limited control. From a public policy perspective, this condition generates not only individual risks, but also systemic consequences for trust in institutions, the security of public services, and social cohesion.

Digital skills as a systemic risk factor

In political discourse, digital skills are often discussed through the lens of employability and competitiveness. The analysis of current data, however, shows that they should also be understood as a key factor for public security. The lack of basic digital skills limits citizens’ ability to recognise manipulation, assess risks and manage their own digital identity.

The comparative analysis between the EU, Bulgaria and Italy reveals that low levels of digital literacy are accompanied by pronounced internal inequalities by age, education and region. In Italy, the share of people with basic digital skills drops sharply among those over 65, and a significant portion of citizens have never used the internet. In Bulgaria, the skills deficit is combined with limited access to structured lifelong learning opportunities. This places many adults in a state of functional vulnerability – they use digital services daily, but lack the capacity for critical assessment and informed decision-making.

The human factor as a key element of cyber risk

Data on cyber threats in the EU shows that risk is not limited to technological infrastructure; it is deeply linked to human behaviour. Analyses by ENISA and Verizon DBIR demonstrate that the human factor is involved in approximately 68% of all recorded security breaches. Social engineering, phishing attacks, compromised credentials and errors in handling information prove more significant than sophisticated technical exploits.

From a public policy standpoint, this means that cybersecurity investments cannot be effective if they do not include systematic work on citizens' behaviours, habits and cognitive patterns. The fact that the most affected sectors are public administration, transport and financial services underlines that this is a risk with direct implications for daily life and citizens' trust.

Economic and social consequences of a lack of intervention

Economic analyses show that the cost of cyber incidents remains structurally high. The average global cost of a data breach is estimated between USD 4.4 and 4.88 million. While these figures primarily concern organisations, the indirect consequences for citizens are significant – leakage of personal data, service disruptions, financial fraud and erosion of trust in institutions.

Social engineering and related scams cause annual losses on the order of billions of dollars globally. These attacks exploit trust, authority and urgency – factors particularly relevant for adults over 30 who carry professional and family responsibilities. This turns the lack of digital resilience into an economic and social problem with broad public impact.

Artificial intelligence as a new layer of vulnerability and opportunity

The spread of artificial intelligence in citizens' and organisations' everyday practices adds a new degree of complexity to digital risk. International analyses highlight an "AI governance gap", whereby a significant share of users employ AI tools without clear rules, without access controls and without understanding the implications of data processing.

For adult users, this often results in inadvertent sharing of sensitive information, uncritical acceptance of automated outputs and increased dependence on opaque algorithmic systems. From a policy perspective, this requires integrating AI literacy into broader strategies for digital resilience, rather than treating it as a niche or purely technical topic.

Policy implications and directions for public interventions

The analysis shows that adults' digital skills should be reconsidered as an issue of societal resilience, comparable to public health or civil protection. This calls for shifting the focus

from limited training in technical skills to building digital autonomy, risk awareness and informed decision-making.

Within EU programmes and national strategies, this implies prioritising adults over 30 as a key target group, integrating cybersecurity, data protection and AI literacy into lifelong learning, and supporting approaches oriented toward human behaviour rather than technology alone.

Relevance for European Union programmes

Programmes such as Erasmus+, CERV, Digital Europe and ESF+ provide an appropriate framework for developing and testing policies and models for strengthening adults' digital resilience. Such interventions contribute directly to the objectives of the Digital Decade 2030 and to strengthening the EU's social and institutional resilience amid accelerated digitalisation.

Conclusion

This analysis shows that the combination of low digital skills, a dominant human factor in cyber incidents and the rapid spread of artificial intelligence constitutes a systemic challenge for European societies. Adults over 30 are at the centre of this challenge, as they combine high digital dependence with uneven access to structured learning opportunities. Addressing this problem through targeted public policies and programmes is not an auxiliary measure, but a strategic investment in security, trust and the democratic functioning of a digital Europe.

STRUCTURED GUIDELINES

for public and programme interventions in the field of
cybersecurity, artificial intelligence and the digital resilience of adults (30+)

I. Normative and conceptual framework

1. Digital Resilience Principle

Digital resilience should be defined as:
the individual's ability to use digital technologies in an informed, autonomous and safe manner, including in the presence of risk, uncertainty or manipulative pressure.

Policies and programmes should not be limited to raising skills; they should aim at:
sustained behaviour;
critical decision-making;
adaptability to new technologies (including AI).

2. Human-Centred Security Principle
Based on empirical data showing the dominant role of the human factor in cyber incidents, public interventions should assume that:
the human is not the "weak link", but the primary bearer of security;
behaviour, cognitive patterns and social context are key variables.

II. Guidelines for strategic targeting

3. Prioritising adults (30+) as a strategic group
Policies should explicitly recognise adults over 30 as:
a group with high digital dependence;
bearers of social, economic and family responsibilities;
insufficiently covered by existing digital policies (which are often focused on youth or ICT specialists).

4. Segmenting the audience by risk, not by age
Within the 30+ group, segmentation is recommended based on:
type of digital activity (administrative, financial, professional);
level of autonomy in using technologies;
exposure to risks (financial, data, identity).

This enables more precise targeting of interventions and resources.

III. Guidelines for the substantive focus of interventions

5. A shift from "skills" to "decision-making"
The content of interventions should focus on:
the logic of digital risk;
recognising manipulative scenarios;
decision-making under pressure and uncertainty.

Technical knowledge is secondary to:
cognitive awareness;
social context;
behavioural patterns.

6. Integrating cybersecurity as an everyday practice
Cybersecurity should be presented not as a specialised domain, but as:
part of everyday digital habits;
an element of personal and professional responsibility;

an extension of offline safety practices.

7. Artificial intelligence: focus on use, not on the technology
AI-related interventions should concentrate on:
understanding how and when AI tools are used;
what data should not be entered;
how to check and validate AI-generated outputs.

The goal is to reduce the AI oversight gap among citizens and small organisations.

IV. Methodological guidelines for implementation

8. Behaviour-oriented design of interventions
The use of the following is recommended:
case-based scenarios;
analysis of real-life situations;
simulations of decisions under risk.

The focus should be on:
“how do I react”;
“what do I check”;
“how do I slow down the decision”.

9. Interdisciplinary approach
Effective interventions combine:
cybersecurity;
cognitive psychology;
AI ethics;
social and economic aspects of digitalisation.

This increases the durability of the effect over time.

V. Guidelines for institutional integration

10. Embedding in lifelong learning policies
These guidelines should be integrated into:
national lifelong learning strategies;
active labour market programmes;
civic education and participation.

11. Support for local and civil society structures
NGOs, municipalities and education centres are key intermediaries for reaching adults.
Policies should:
support their capacity;
encourage locally adapted models;
enable experimentation and piloting.

VI. Guidelines for monitoring and evaluation

12. Measuring behavioural change, not only knowledge
Success indicators should include:
changes in decision-making;
reduced propensity for risky behaviour;
increased autonomy in digital situations.

13. Long-term sustainability of impact
Programmes should be:
upgradeable;
adaptive to new technologies and threats;
supported by institutional continuity.

The evidence-based guidelines show that adults' digital resilience is a cross-cutting theme, integrating security, education, social policy and digital transformation. Public interventions that ignore the human factor and the behavioural dimensions of risk are structurally ineffective. Conversely, interventions that place the adult citizen at the centre have the potential to increase the resilience not only of the individual, but also of institutions and society as a whole.

LOGICAL FRAMEWORK (INTERVENTION LOGIC)
for interventions in the field of cybersecurity, artificial intelligence and the digital resilience of adults (30+)

1. Overall context and problem situation
The digitalisation of public services, the economy and social interactions creates a structural dependence of citizens on digital systems. At the same time, a significant share of the adult population in the EU lacks at least basic digital skills, while the human factor is the leading cause of cyber incidents. The penetration of artificial intelligence further complicates the environment, increasing the risk of automated errors, manipulation and inadvertent data leakage.

The problem is not a lack of technology, but a lack of digital resilience, understood as the capacity for informed, autonomous and safe behaviour under conditions of risk and uncertainty.

2. Overall objective
To increase the digital resilience of adults (30+) as a factor for:
public security;
trust in public institutions;
social and economic stability in a digital environment.

3. Specific objective
To develop sustained behavioural and cognitive capacities among adults (30+) for:
recognising and managing digital risks;
safe use of digital services and AI;
informed decision-making in the online environment.

4. Expected results
Improved ability to recognise social engineering, scams and manipulation.
Improved management of digital identity and personal data.
Reduced propensity for impulsive decisions under digital pressure.
Increased awareness of risks when using AI.
Established basic culture of digital autonomy.

5. Key activities
Developing behaviour-oriented training interventions.
Analysing and using real-life cases from everyday contexts.
Training of trainers (ToT) based on a human-centred approach.
Piloting and adapting to the local context.
Monitoring and evaluating behavioural change.

6. Indicators of success
Demonstrated change in decisions in simulated risk scenarios.
Reduction of errors in recognising scams.
Increased level of self-reliance in managing digital situations.
Qualitative feedback on confidence and autonomy.

7. Assumptions and risks
Willingness of institutions to treat digital skills as a matter of public security.
Access to adult groups through intermediaries (NGOs, municipalities).
Risk of underestimating the behavioural component – requires systematic communication.

ToT (TRAINING OF TRAINERS) POLICY MODEL
for building capacity for digital resilience

1. Purpose of the ToT model
To build a sustainable network of trainers who:
understand digital risk as a social and behavioural phenomenon;
can work with adult audiences;
apply human-centred and evidence-based methods.

2. Trainer profile
The trainer is not necessarily an ICT expert, but rather:
a facilitator of critical thinking;
a mediator between technology and everyday life;
able to analyse behavioural reactions.

3. Key competences
understanding of cyber risks and social engineering;
basic AI literacy and ethical aspects;
knowledge of cognitive biases;
facilitation skills and experience working with adults.

4. Methodological principles
learning through cases, not through instructions;
analysis of real scenarios;
working with group dynamics;
encouraging autonomy, not fear.

5. Institutional framework
The ToT model should be:
integrated into national and European programmes;
supported by public institutions;
used as a standard for scaling interventions.

6. Sustainability and upgrading
periodic updates of the content;
a community of practice among trainers;
linkages to policies and current threats.

BIBLIOGRAPHY
(international sources, scholarly standard – APA 7)

1. European policies, digital skills and statistics

European Commission. (2023).
Digital Decade: Policy Programme 2030 – State of the Digital Decade Report 2023.
Publications Office of the European Union.
https://digital-strategy.ec.europa.eu/en/policies/digital-decade

European Commission. (2024).
Digital Decade Country Report: Bulgaria.
Publications Office of the European Union.
https://digital-strategy.ec.europa.eu/en/library/digital-decade-country-reports

European Commission. (2024).
Digital Decade Country Report: Italy.
Publications Office of the European Union.
https://digital-strategy.ec.europa.eu/en/library/digital-decade-country-reports

European Commission. (2023).
Digital Skills and Jobs – Key indicators.
https://digital-skills-jobs.europa.eu/en

Eurostat. (2023).
Digital skills statistics.
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_skills

2. Cybersecurity and threats (ENISA)

European Union Agency for Cybersecurity (ENISA). (2023).
ENISA Threat Landscape 2023.
Publications Office of the European Union.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Agency for Cybersecurity (ENISA). (2024).
ENISA Threat Landscape 2024.
Publications Office of the European Union.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

European Union Agency for Cybersecurity (ENISA). (2023).
Threat Landscape for Distributed Denial of Service Attacks.

https://www.enisa.europa.eu/publications/threat-landscape-for-ddos-attacks

3. Breaches, human factor and social engineering

Verizon. (2024).
2024 Data Breach Investigations Report (DBIR).
Verizon Enterprise Solutions.
https://www.verizon.com/business/resources/reports/dbir/

Federal Bureau of Investigation (FBI). (2023).
Internet Crime Report 2023.
FBI – Internet Crime Complaint Center (IC3).
https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Hadnagy, C. (2018).
Social Engineering: The Science of Human Hacking (2nd ed.).
Wiley Publishing.
ISBN: 978-1119433385

4. Economic impact of breaches and risk management

IBM Security & Ponemon Institute. (2024).
Cost of a Data Breach Report 2024.
IBM Corporation.
https://www.ibm.com/reports/data-breach

IBM Security & Ponemon Institute. (2025).
Cost of a Data Breach Report 2025.
IBM Corporation.
https://www.ibm.com/reports/data-breach

5. Artificial intelligence, automated decisions and risk

OECD. (2019).
Artificial Intelligence in Society.
OECD Publishing.
https://doi.org/10.1787/eedfee77-en

OECD. (2023).
AI, Data and Privacy: Empirical evidence and policy implications.
OECD Digital Economy Papers.
https://www.oecd.org/digital/

European Commission. (2024).
Artificial Intelligence Act (AI Act): Proposal and policy framework.
https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Floridi, L., et al. (2018).
AI4People—An Ethical Framework for a Good AI Society.
Minds and Machines, 28(4), 689–707.
https://doi.org/10.1007/s11023-018-9482-5

6. Cognitive psychology, decisions under risk and behaviour

Kahneman, D. (2011).
Thinking, Fast and Slow.
Farrar, Straus and Giroux.
ISBN: 978-0374275631

Tversky, A., & Kahneman, D. (1974).
Judgment under Uncertainty: Heuristics and Biases.
Science, 185(4157), 1124–1131.
https://doi.org/10.1126/science.185.4157.1124

Gigerenzer, G. (2008).
Gut Feelings: The Intelligence of the Unconscious.
Penguin Books.
ISBN: 978-0143113392

7. Digital literacy, adults and education

van Dijk, J. (2020).
The Digital Divide.
Polity Press.
ISBN: 978-1509534831

UNESCO. (2018).
Digital Literacy Global Framework.
UNESCO Institute for Statistics.
https://uis.unesco.org/

OECD. (2021).
Skills for a Digital World.
OECD Publishing.
https://www.oecd.org/education/

8. Supplementary sources (Italy and national analyses)

Fondazione Repubblica Digitale. (2024).
Report on the State of the Digital Decade – Italy.
https://www.fondorepubblicadigitale.it/

Secondo Welfare. (2023).
Jobs and digital skills: The situation in Italy.
https://www.secondowelfare.it/

Reuters. (2025).
Just 8% of Italian enterprises are using AI, study finds.
https://www.reuters.com/