REWIRE
CYBERSECURITY SKILLS ALLIANCE

Co-funded by the Erasmus+ Programme of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R.5.4.5 Policy Recommendations

Improving Public Awareness in Cybersecurity

Title	Improving public awareness in cybersecurity
Document description	The policy brief investigates the present status of cybersecurity awareness within the European Union, identifying challenges and gaps in current endeavors. It contains actionable recommendations to improve societal-level cybersecurity awareness.
Nature	Public
Task	T.5.4 Policy recommendations – 5th Policy Brief within R5.4.1
Status	Final
WP	WP5
Lead Partner	EVTA
Partners Involved	MRU, EKT,KTH, ApiroPlus, EUC, ReadLab, TUC, URL, LRGA, NRDCS, BME, EUC, UL, ReadLab
Date	29/04/2024

CONTENTS

1. EXECUTIVE SUMMARY

Governments, companies, and individuals express significant concerns about cybersecurity due to the growing reliance on digital technologies for daily activities. Banking, healthcare, education, and various services are now heavily dependent on digital platforms, exposing vulnerabilities to cyber threats. Robust defences are essential but insufficient against the dynamic cyber threat landscape. The human element, considered the weakest link, strongly influences overall security (Singer & Friedman, 2014; ENISA, 2023). The REWIRE Pestle Analysis (Ricci et al, 2022) emphasises the crucial need for public education on cyber threats and heightened society-level cybersecurity awareness. Despite the thriving cybersecurity sector in the European Union (EU), adequate public awareness lags, with 48% of citizens feeling uninformed about cyber risks and few victims reporting crimes to the police (European Commission, 2020a).

Drawing insights from a thorough literature review, this brief examines the current state of cybersecurity awareness across the European Union, identifying challenges and gaps in existing efforts. The document delves into the diverse impact of escalating cyber threats on individuals, highlighting the influence of socio-demographic factors, national economic resources, and socio-cultural contexts. It addresses vulnerabilities to cyberattacks and the level of awareness regarding cyber threats. Emphasising a multifaceted approach, the brief explores diverse methods for effectively delivering cybersecurity awareness initiatives. It provides an overview of the existing European policy framework and its constraints, as well as a summary of cybersecurity awareness initiatives aimed at informing individuals about cyber risks and thus promoting best practices for online security. Actionable recommendations underscore the need for a concerted effort to enhance societal-level cybersecurity awareness. This involves collaborative engagement with stakeholders across legal, organisational, technical, and educational domains. Specific measures include conducting comprehensive studies on cybersecurity-related behaviour across different demographic groups, ensuring ample funding for targeted awareness campaigns, and integrating cybersecurity awareness into non-technical educational and training programs. By providing insights and practical steps, the policy brief seeks to inspire collaborative endeavours among stakeholders, fostering a proactive role in advancing cybersecurity awareness and education.

Highlights

- In the European Union, public awareness of cybersecurity lags, with 48% of citizens feeling uninformed about cyber risks, leading to underreporting of crimes
- Cybersecurity awareness-raising measures at both EU and national levels are currently lacking adequate targeting, effective publicity, and inclusivity towards diverse population segments
- Some demographics, including seniors, children, and people with disabilities, are particularly vulnerable to heightened cybersecurity risks, requiring focused awareness interventions
- Broadening public awareness and understanding to minimize human vulnerabilities is key for effective cybersecurity at both governmental and organizational levels
- There is a need to ensure continuous funding for specialized cyber awareness programs, integrate cybersecurity awareness into all levels of non-technical training and education, and foster cross-border collaboration among stakeholders for best practices in cybersecurity awareness
- Enhancing public awareness in cybersecurity is vital for the reliable operation of European societies and economies within an open and secure cyberspace

2. INTRODUCTION

The field of Information Technology has undergone significant expansion over the past decade, contributing to a widespread global growth in Internet usage among individuals and various sectors, including academia, government, and industry (Aloul, 2012; Jalali et al.2019; Lee et al.,2017). Fuelled by technology integration, this transformation has reshaped daily life across various domains. As society increasingly depends on cyberspace and daily life becomes intricately connected with smart devices, the risks posed by cyberattacks and cyberwarfare become more pronounced.

The COVID-19 pandemic further normalised remote work, e-commerce, and online socialisation. The shift from traditional infrastructure to the web, along with increased interconnectivity, and the emergence of technologies like artificial intelligence have led to a rise in cyberattacks that are more sophisticated, complex, and impactful, as cautioned by the European Union Agency for Cybersecurity (ENISA) in its 2021 Threat Landscape report. The accelerated digital transformation has resulted in a notable increase in cyberattacks targeting businesses, governments and individuals. In late 2022 and early 2023, cyberattacks escalated in variety and quantity, with 726 incidents and 111,218,696 data breaches reported in Europe by ENISA (CIRAS Incident Reporting, 2023) and IT Governance Europe (Kosling, 2023).

Citizens worldwide face an escalating surge of cyber threats and crimes, significantly affecting their lives. Growing cyber threats, including identity theft, financial fraud, and privacy breaches, heighten individuals' vulnerability online, undermining security and risking privacy, financial stability, and well-being. As technology progresses, it is increasingly vital to prioritise heightened awareness and strong cybersecurity measures to protect individuals from evolving cyber threats. The growing number of attacks targeting unsuspecting individuals underscores the crucial role of human factors in information security management. To mitigate risks stemming from the lack of human preparedness, prioritising cybersecurity awareness is essential.

Despite being a critical challenge for governments, public cybersecurity awareness remains inadequate (ENISA, 2021b). Although the significance of cybersecurity is widely acknowledged, the behaviour of citizens does not consistently reflect a high level of awareness on the matter. As per the European Union's Cybersecurity Strategy (2020a), a substantial proportion of EU citizens, approximately 40%, have faced security-related issues. Moreover, 60% feel incapable of safeguarding against cybercrime. Over the last three years, one-third have received fraudulent emails or phone calls seeking personal information, yet 83% have never reported a cybercrime (EU's Cybersecurity Strategy for the Digital Decade, 2020, p.2). Moreover, Eurobarometer surveys reveal disparities in knowledge and concerns among EU Member States, emphasizing the necessity for targeted cyber awareness-raising measures. Despite significant advancements in EU cybersecurity policy, there is a crucial need to address awareness gaps among citizens. The existing emphasis on legislation and

frameworks primarily targeting Member States and organisations overlooks the vital aspect of empowering individuals. Rectifying this omission is essential to strengthen the EU's cybersecurity stance and foster a more resilient and knowledgeable digital society. The existing literature highlights several challenges in promoting society-level cybersecurity awareness throughout the EU. These challenges include resource constraints, a lack of scientific evidence on effective awareness methods, uneven participation of Member States with disparities in knowledge and implementation abilities, inadequate and poorly publicised awareness-raising measures for diverse populations, insufficient skills, and the absence of comprehensive national educational programs in cybersecurity across Europe. The limited representation of cybersecurity in non-technical educational programs and a scarcity of research on how individuals engage with cybersecurity practices further contribute to compromised cyber awareness and safety.

Addressing this gap in public awareness is imperative for building a resilient and secure digital environment. Efforts should be directed towards comprehensive education campaigns emphasising the practical implications of cybersecurity for individuals and society. This policy brief calls for collaborative engagement among relevant stakeholders to enhance the overall cybersecurity posture and create a more vigilant and informed public. It underscores the importance of continuous investment in personalised and readily available cyber awareness initiatives. Also, it calls for the implementation of extensive interdisciplinary cybersecurity training programs and encourages transnational collaboration among Member States and pertinent stakeholders. This collaboration aims to facilitate the exchange of best practices, resources, and expertise in the realm of cybersecurity awareness.

3. THE GROWING MENACE: CYBER THREATS AND THEIR IMPACT ON INDIVIDUALS AND SOCIETY

The impact of cyberspace on society is undeniable. It has provided a platform for instantaneous communication, commerce and interaction between individuals and organizations across the globe. The free flow of information is impacting the lives of all Europeans. For many people, access to the Internet has become a basic necessity for working, studying and exercising freedom of expression, political freedom and social interaction. As cyberspace has grown in prominence, unfortunately, so has the number and variety of cyberattacks (Verizon, 2018). These attacks vary from hacking, social engineering, and denial-of-service (DoS) to ransomware and spyware infections, impacting individuals and the crucial national infrastructure of any country.

The increasing number and sophistication of cyberattacks and cybercrime across Europe are expected to grow, fuelled by the projected connection of 41 billion devices to the Internet of Things by 2025 (European Council, n.d.). Ransomware poses a significant cyber threat in the EU, involving the monthly theft of over 10 terabytes of data. The primary method for initiating cyberattacks is currently identified as phishing (European Council, n.d.). Moreover, the ENISA Threat Landscape report of 2023 reveals that ransomware, malware, and social engineering stand out as prime threats, each exploiting human vulnerabilities at various levels to be realized. Additionally, according to ENISA's "Foresight Cybersecurity Threats for 2030" report (Mattioli & Malatras, 2024), skill shortages and human error exploited in legacy systems rank second and third, respectively, in the revised top-ten threats list, based on impact and likelihood score. Cybercriminals target individuals with the same intensity as large organisations and companies. While corporate leaders can afford dedicated cybersecurity teams, the average person lacks such resources, emphasising the need for heightened personal cybersecurity awareness and accessible tools to protect against persistent cybersecurity threats.

Cyberattacks have multifaceted effects on individuals and society, involving reputational consequences, financial losses, physical repercussions, and societal and psychological impacts (ENISA Threat Landscape, 2023 & Bada & Nurse, 2019). These attacks can result in economic loss, where cybercriminals exploit various methods to access and misuse financial information, leading to unauthorised transactions that can be challenging to recover. Identity theft is a prevalent outcome, with stolen personal details causing fraudulent activities and legal complications. Victims not only face tangible losses but also endure emotional trauma, feeling violated, embarrassed and anxious (Bada & Nurse, 2019). The consequences extend to reputational damage, as cybercriminals may tarnish an individual's online image, affecting credibility and trust, which can be particularly detrimental in professional settings, potentially resulting in job loss or difficulty securing employment.

Reflecting on the social impact of the cyberattacks, the WannaCry attack significantly impacted the UK, affecting critical infrastructure like the National Health Service, leading to cancelled operations, delayed scans and treatments, and redirected ambulances (BBC, 2017). Furthermore, the reviewed literature (Gomez & Shandler, 2022) indicates that cyberattacks have been pivotal in eroding trust in social institutions. These attacks typically have a subtler impact by weakening citizens' trust and amplifying existing concerns about the trustworthiness of the underlying technology. Research by Shandler and Gomez in 2023 reveals that the ransomware attack on a Düsseldorf hospital markedly reduced public confidence, particularly within segments of the population directly affected by the incident. Additionally, recent data (Matzkin et al., 2023; Jardine et al., 2024) has emphasized the substantial societal implications of cybersecurity, particularly in relation to political outcomes. These studies indicate that cyberattacks have the potential to influence voters' perspectives and actions, fostering more militaristic political stances, encouraging an increase in violence, and intensifying public demands for strict security measures that may impinge on privacy (Leal and Musgrave, 2023; Snider et al., 2021).

Certain segments of the population, such as senior citizens and children, face elevated vulnerability and heightened risks in the realm of cyberattacks (Blackwood-Brown et al., 2019 & Global Cybersecurity Forum). This susceptibility may be influenced by factors such as varying levels of digital literacy, socioeconomic disparities, or specific demographic characteristics. The worldwide survey conducted by the Global Cybersecurity Forum revealed that 72% of children globally have encountered various online cyber threats (Panhans et al., 2022). The findings highlight the rising dangers faced by children, including online bullying, unauthorised use of personal data, ideological manipulation, harassment, commercial profiling, and security threats. These risks can significantly impact the health and well-being of children. Similarly, individuals within civil society, dissidents, and human rights advocates encounter a growing cyber threat. As per the ENISA Threat Landscape report (2023), governments often exploit spyware surveillance technologies to monitor and target these groups, pursuing goals that deviate from democratic principles.

Recent literature (Renaud & Coles-Kemp, 2022) indicates that people with disabilities constitute a unique demographic group that is more prone to cyberattacks. This vulnerability primarily stems from inaccessible security and privacy features and a deficiency in accessible guidance on cyber awareness. Recognising and addressing socio-demographic vulnerabilities is crucial for implementing targeted cybersecurity measures to safeguard these individuals from potential threats. As online threats and cyberattacks persist, the community must gain a comprehensive understanding of these vulnerabilities.

As noted in this section, the rising cyber threats present a significant challenge to individuals and society, leading to financial losses, disruptions in critical infrastructure, privacy breaches, and compromised personal information. Effectively addressing this issue necessitates a collaborative effort involving governments, private sectors, and individuals. Proactive measures, such as robust cybersecurity frameworks, heightened awareness, and

international cooperation, are essential to mitigate risks and protect the digital well-being of individuals and the resilience of our interconnected society.

4. THE STATE OF CYBERSECURITY AWARENESS: INSIGHTS AND GAPS AMONG THE GENERAL PUBLIC

Cybersecurity awareness and skills are essential to navigating the digital landscape. To identify and effectively mitigate the impacts of cyberattacks, individuals must be equipped with the knowledge and capabilities to safeguard themselves online. This proactive approach not only enhances personal security but also contributes to minimising the substantial losses incurred due to cyber threats. As defined by ENISA and EGA report on Raising Awareness of Cybersecurity (2021b), cybersecurity awareness refers to the degree of appreciation, understanding, or knowledge individuals possess regarding various cybersecurity aspects. This includes recognising cyber risks and threats and understanding appropriate protective measures. The goal is to enable individuals to identify IT security concerns and respond appropriately, fostering a proactive approach to online behaviour and self-protection against potential risks and threats (Hansche, 2008). Despite being a significant challenge for governments, there is still insufficient public awareness of cybersecurity, as the ENISA report (2021b) indicates. Existing research (Bada & Nurse, 2019) highlights a lack of knowledge among the general population in crucial cybersecurity domains, including using security packages, securing devices, and comprehending online threats. This overall deficiency in public understanding contributes to inadequate protection activities.

The EU consistently assesses Europeans' attitudes toward cybersecurity through regular surveys, such as the Special Eurobarometer, to gauge citizens' awareness, experiences, and perceptions of cybersecurity. The findings from the Special Eurobarometer 499 (European Commission, 2020b), which explores Europeans' attitudes towards cybersecurity, reveal significant disparities in respondents' knowledge about the risks of cybercrime across Member States. In Denmark, 80% of respondents felt well-informed, whereas in Romania, only 32% shared this sentiment. Almost half of the respondents (47%) expressed a lack of confidence in their awareness of cybercrime risks, and 17% indicated being completely uninformed. Additionally, socio-demographic factors play a role, as men and younger individuals were more likely to feel well-informed compared to women and those aged 55 and older (European Commission, 2020b). The varying levels of perceived knowledge about cybercrime risk across Member States indicate a need for targeted awareness campaigns and education initiatives and the importance of improving cybersecurity literacy across the surveyed population.

Despite variations, widespread concerns emerged among respondents about various cybercrimes, with over two-thirds expressing apprehension about bank card or online

banking fraud (67%) and malicious software or identity theft (66%). Concern levels were lower for hacking of online accounts (61%), fraudulent emails or calls (59%), and cyberattacks affecting online services (57%). Geographical differences were also evident in cybersecurity concerns among EU Member States, with respondents in Sweden, the Netherlands, and Denmark consistently showing lower levels of concern. In comparison, those in Bulgaria and Ireland consistently expressed higher levels of worry. Noteworthy, these variations underscore significant differences in awareness and apprehension related to cybersecurity issues across EU Member States.

Survey participants were also queried about their involvement in reporting cybercrimes or illegal online conduct. The results reveal that a substantial majority (83%) have not reported any cybercrime or online illicit behaviour, with 17% having done so. The fact that fewer than 20% of respondents have reported such incidents suggests a potential gap in their awareness or willingness to take action against cyber threats.

The Eurobarometer 480 on Europeans' attitudes toward Internet security (European Commission, 2019a) explored the impact of concerns about online privacy and security on user behaviour. Findings reveal significant concerns among Internet users regarding the misuse of personal data and the security of online payments. Approximately 47% of respondents took measures like installing or changing antivirus software, avoiding unknown email sources (45%), and reducing the disclosure of personal information on websites (37%). However, notable percentages have not taken more drastic actions, such as lowering online purchases, cancelling transactions, or opting out of online banking.

Based on the Eurobarometer 390 (European Commission, 2014) findings and utilising the latent class analysis method, Lee and Kim's (2020) research on Latent Groups of Cybersecurity Preparedness in Europe discloses that merely 15.1% of surveyed respondents fall within the highest category of cybersecurity preparedness. Conversely, the remaining 85% of the sample is distributed across two distinct subgroups: uninformed users with the lowest levels of online security awareness and disciplined users with moderate cybersecurity preparedness. The findings highlight the need for targeted awareness campaigns and education initiatives to address the disparities in cybersecurity awareness among the general population.

Individual-level sociodemographic factors and country-level economic/institutional resources shape cybersecurity preparedness because individuals are situated within social and cultural contexts (Kim & Lee, 2020). Several studies (Öğütçü et al., 2016; Sultan, 2019 ; Anwar et al., 2017; European Commission, 2020b;) demonstrate that individual cybersecurity awareness is influenced by sociodemographic factors such as age, gender, and socioeconomic status. Senior citizens generally exhibit restricted cybersecurity awareness and skills (Morrison et al., 2020). However, distinctions within this age group become evident based on various factors such as gender, duration of using computers, years of Internet use, experience with internet-enabled mobile devices; years spent working in a corporate or formal setting, time since retirement, and educational attainment (Blackwood-Brown et al., 2019).

Furthermore, higher socioeconomic status is linked to increased cybersecurity preparedness. Well-educated individuals, often in white-collar jobs, are more likely to use computers and the Internet in their workplace compared to blue-collar workers, leading to greater awareness of cybersecurity issues due to their engagement in various online activities and cybersecurity training (Öğütçü et al., 2016). Similarly, the Centre for Long-term Cybersecurity Research findings reveal that individuals with lower income and those from underserved communities are less likely to be aware of whether they have fallen victim to a cyberattack. Additionally, they exhibit a lower awareness of cybersecurity risks and an incomplete understanding of cybersecurity concepts (Sultan, 2019).

Recent research (Zwilling et al., 2020; Piesarskas et al, 2022) highlights a positive link between integrating cybersecurity education into formal academic curricula and enhancing overall cyber awareness. It emphasises the vital role of including security courses in non-technical programs at all educational levels to fortify individuals against potential cyber threats, stressing the need for a comprehensive and inclusive approach to cybersecurity education.

Conversely, scholars hold conflicting perspectives on the influence of gender on cybersecurity awareness. While one set of studies (Ifinedo 2014; Zwilling et al., 2020) suggests that men exhibit higher preparedness for cybersecurity, research by Lee and Kim (2020) highlights persistent stereotypes about women's cybersecurity awareness. Their work on Cybersecurity Preparedness in Europe challenges the notion that women inherently possess lower cybersecurity preparedness than men. Furthermore, the persistent gender digital divide and the higher likelihood of women being targeted by cybercrime offenders (Virtanen, 2017) may contribute to the disparity rather than inherent differences in preparedness.

The level of economic development and institutional resources at the country level and the Global Cybersecurity Index (GCI) significantly influence cybersecurity awareness at the individual level. Nations with higher GDP per capita generally exhibit greater cybersecurity preparedness (Kim & Lee, 2020). These countries are likely more equipped to establish secure environments through legal, technical, and educational initiatives. Similarly, in countries with a higher GCI, individuals are more likely to exhibit advanced levels of cybersecurity preparedness, as these nations prioritise developing institutional resources and relevant laws to create cybersecurity-resilient environments.

In conclusion, the state of cyber awareness among the general public reveals significant gaps. Despite the increasing importance of navigating the digital landscape with cybersecurity skills, the findings indicate a lack of awareness and preparedness. Eurobarometer surveys highlight discrepancies in knowledge and concerns across EU Member States, underscoring the need for focused awareness campaigns. Most respondents haven't reported cybercrimes, suggesting potential gaps in willingness to address threats actively. Sociodemographic factors, institutional resources, and a country's economic development significantly impact cyber awareness. Bridging these gaps necessitates multifaceted efforts, including targeted

awareness campaigns, education initiatives, and policy interventions for a more cyber-resilient society.

5. HUMAN-CENTRIC CYBERSECURITY: METHODS FOR ENHANCING AWARENESS

The general public and employees utilizing cyberspace are key contributors capable of actively participating in developing defensive measures against cyberattacks. Nevertheless, the primary obstacles to establishing effective defense mechanisms may stem from a lack of awareness, behavioral actions, and attitudes (Zwilling et al., 2020). Despite the installation of protective tools on computers and infrastructure, research indicates that these measures do not eliminate cybersecurity breaches (Schultz, 2005; Zwilling et al., 2020). The persistent vulnerability in the cybersecurity chain stems from human error (Anwar et al., 2017). A noted before, the vulnerabilities arising from human behavior represent a considerable information security risk, resulting in substantial economic losses for individuals and corporations alike (Workman, 2007; Zwilling et al., 2020).

The importance of human factors in information security management is often overlooked despite their critical role. People's failure to take precautions against information security threats has been largely ignored, as highlighted by Workman in 2007. Minimizing human vulnerabilities is crucial for enhancing cybersecurity. Both governments and organizations must ensure that individuals are not only aware of potential threats but also understand the necessary actions in case of an issue. By broadening the awareness of cybersecurity risks among the general public, states can mitigate the extent of cybersecurity risks associated with human vulnerabilities.

The methods employed for delivering information security play a pivotal role in elevating the overall levels of cyber awareness (Abawajy, 2012). Numerous models for delivering cybersecurity awareness exist, including newsletters, web-based cybersecurity training, game-based approaches, and simulation-based methods. Abawajy's (2012) research on the efficacy and impact of diverse information security awareness delivery methods among end-users indicates that integrated delivery models are more effective than individual methods in cybersecurity awareness delivery. Cybersecurity awareness training is a powerful means of empowering people with knowledge on specific topics. However, as risk landscapes evolve, the methods for delivering cybersecurity awareness should adapt accordingly. Success in awareness hinges on maintaining the relevance and consistency of messages while also diversifying the delivery mechanisms to sustain interest among the diverse audience. This implies that while a one-size-fits-all cybersecurity awareness strategy might be convenient for governments and organizations, it will fail to realize information security objectives (Abawajy, 2012).

The prioritization of user-centric designs in developing cybersecurity awareness places a strong emphasis on enhancing users' engagement in implementing preventive measures against cyber threats and attacks (McKenna et al., 2015). Likewise, the content of cybersecurity awareness resources should be tailored to the needs and contexts of different audiences to enhance their effectiveness (Ahmed, 2023). In the dynamic landscape of cybersecurity, where cybercriminals continuously evolve their techniques and strategies, it becomes imperative for cybersecurity education and awareness initiatives to regularly refresh their content and adapt their approaches to remain pertinent. Furthermore, studies suggest that creating resources that simplify intricate cybersecurity concepts can contribute to making this topic more understandable for the general public (Ahmed, 2023). Adaptability, accessibility, situational relevance, and user-centric designs are key factors for success in the dynamic landscape of cybersecurity, emphasising the need for ongoing efforts to empower individuals with knowledge and preventive measures against evolving cyber threats. In conclusion, acknowledging individuals' pivotal role in cybersecurity is crucial, given the persistent challenge of human error. Enhancing cybersecurity requires addressing human vulnerabilities through effective awareness and education initiatives, tailored to diverse audiences and evolving threat landscapes.

6. PUBLIC CYBERSECURITY AWARENESS IN THE EU POLICY FRAMEWORK

Governments play a significant role in making sure citizens feel safe. However, not all countries are on the same level of awareness and readiness for cyberattacks. In the EU, some countries, like Estonia, France, and Norway, are doing well in the cybersecurity domain. In contrast, there is an apparent discrepancy when comparing other countries, especially in Southern and Eastern Europe (Kertysova et al., 2018). According to Kertysova et al. (2018), this creates two challenges: first, it's hard for countries to work together because their security and privacy rules differ. Second, countries that need to prepare for new cyber threats weaken the European cybersecurity system and are more prone to being attacked.

Studies have shown that the EU has increasingly prioritised cybersecurity since the early 2000s, issuing numerous regulations and directives for its Member States aimed at various aspects of prevention. These include safeguarding personal data, protecting critical infrastructure, ensuring secure online transactions, and establishing common 5G network security standards. The first comprehensive EU cybersecurity strategy was introduced in 2013, emphasising the need for legislation to address gaps in national capabilities, cross-border coordination during incidents, and private sector involvement (Enescu, 2020). Since 2014, the European Commission has been assessing Member States' digital development and progress through the Digital Economy and Society Index (DESI) reports. DESI evaluates digital skills, including information processing, Internet use, communication, cooperation skills, and

proficiency in using digital services. It also considers skills related to problem-solving cybersecurity, including the user's ability to safeguard their devices' information processing and to protect their privacy. This suggests recognizing the need for a well-informed and cyber-aware general public as an integral component of a digitally resilient society.

Subsequently, in 2020, the EU Cybersecurity Strategy was introduced to enhance Europe's resilience against cyber threats and enable citizens and businesses to benefit from secure digital services and tools. The strategy reveals a concerning trend in public cybersecurity awareness, where a significant portion of EU citizens (approximately 40%) have encountered security-related issues. More notably, three out of five individuals feel a lack of capability in protecting themselves from cybercrime. The data also suggests a gap in reporting, as despite one-third experiencing fraudulent activities, a substantial 83% have never reported a cybercrime. The strategy also emphasizes building collective capabilities to respond to major cyberattacks and collaborating globally for international security in cyberspace.

Significant legislative strides in EU cybersecurity were made with the revision of the NIS2 Directive in 2023 and the amendment of the EU Cybersecurity Act of 2019 in the same year. The NIS2 directive's objective is to elevate the EU's cybersecurity posture, fostering resilience within EU organizations. The directive tasks ENISA with assisting Member States in implementing it within their national legislation. However, the 21-month period provided for transposing the directive implies that adaptation timelines will vary across Member States. This variation, coupled with the rapid pace of cybersecurity developments, may result in divergent levels of citizen awareness and preparedness across the EU.

Moreover, the EU Cybersecurity Act establishes a framework for certification schemes, ensuring heightened cybersecurity for ICT products and services to mitigate market fragmentation (Fuster & Jasmontaite, 2020). It also emphasizes the pivotal role of ENISA in enhancing cybersecurity awareness and education through fostering coordination among Member States, sharing best practices, and establishing national education points of contact (EU Cybersecurity Act, 2019).

While these developments mark substantial progress, the primary focus on the private sector often overlooks the vulnerable individuals who are most at risk. In the context of citizen engagement amidst interconnected technologies, the EU's Cybersecurity Act aims to address growing concerns about digital security. Introducing a certification framework seeks to instill consumer confidence in the security of interconnected services. Despite this positive step, it was stressed by the Deputy Director General of the European Consumer Organization, Ursula Pachi, that a regulatory gap persists, especially in mandating manufacturers and retail service providers to secure their products (EURACTIV, 2019). This gap exposes citizens to potential cyber threats, emphasizing the pressing need for more robust regulations and enforcement mmechanisms to safeguard against evolving digital risks.

Furthermore, within the existing European policy and legal framework, cybersecurity is predominantly considered a concern exclusively for states and organisations. According to Papakonstantinou (2022), the current regulatory instruments are tailored for Member States and significant organisations in the EU. For individuals, cybersecurity is essentially perceived as a service indirectly delivered to them. In other words, cybersecurity is presented as a responsibility solely for specific actors, framed as an administrative and bureaucratic duty to be executed through the implementation of mechanisms and procedures rather than an ongoing concern for everyone.

Moreover, generic references to cybersecurity awareness within the general public are evident in the EU's DigComp 2.2 framework, updated in 2022, featuring a dedicated safety competence area. This area encompasses the protection of devices and digital content, safeguarding personal data and privacy in cyberspace, promoting well-being, and fostering awareness of digital technologies for social inclusion. In summary, while the EU has made significant strides in cybersecurity policy, there remains a critical need to bridge awareness gaps among its citizens. The current focus on legislation and frameworks primarily directed at states and organisations overlooks the imperative to empower individuals. Addressing this oversight is essential to fortify the EU's cybersecurity posture and create a more resilient and informed digital society.

7. A SNAPSHOT OF CYBERSECURITY AWARENESS INITIATIVES ACROSS EUROPE

The EU is actively involved in promoting cybersecurity awareness among the general public through various programmes and initiatives. These efforts aim to educate individuals about cybersecurity risks, disseminate best practices for staying safe online, and underscore the importance of protecting personal and sensitive information. By promoting awareness and education, the EU endeavours to empower individuals to navigate the digital landscape securely, fostering a more resilient and informed citizenry in the face of evolving cybersecurity challenges.

Since 2011, the European Commission has launched a notable initiative—the European Cybersecurity Month (ECSM) campaign organised by ENISA with an annually changing theme. Each October, this initiative is dedicated to promoting cybersecurity awareness among EU citizens and organisations. Through education and the dissemination of online security information and best practices, the campaign underscores the simple steps that can be adopted to safeguard data, be it financial, personal, or professional.

The European Cybersecurity Organization (ECSO), in collaboration with the European Commission in executing the public-private partnership on cybersecurity, offers a monthly platform through the ECSO Cybersecurity Awareness calendar. This platform allows European

cybersecurity stakeholders to showcase their expertise, spotlight their organisation's initiatives related to a specific theme each month, and actively participate in the collective goal of enhancing cybersecurity awareness among the general public throughout the continent. Furthermore, ECSO conducts workshops that focus on creating cyber awareness campaigns, fostering collaboration among a diverse array of stakeholders with varying perspectives on awareness initiatives.

Safer Internet Day (SID) has evolved into a global event promoting responsible online use, especially among youth and children. Originating in 2004 under the EU-funded Safe Borders project, SID, now celebrated in around 200 countries, is a crucial initiative supported by the European Commission to raise awareness about online safety and empower individuals worldwide to protect themselves online (Safer Internet Day Org, n.d.). Additionally, the European Commission's Digital Skills and Jobs Coalition, a multi-stakeholder partnership aimed at addressing the digital skills gap in Europe, concentrates on promoting the development of cybersecurity skills through various training initiatives. The goal is to equip individuals with the essential skills to navigate the digital world safely and securely (European Commission, 2022). The coalition aims to enhance public awareness of handling digital challenges by targeting cybersecurity skills.

At the national level, most Member States conduct an annual cybersecurity public awareness campaign with a designated theme each year. In 2023, the Centre for Cybersecurity in Belgium (CCB) partnered with the Cyber Security Coalition (CSC) to launch a significant awareness campaign titled "Phishing, it's in the details". The campaign emphasises the importance of scrutinising URLs before clicking. Various communication materials and channels, such as posters, online leaflets, videos, social media posts, and television and cinema spots, were utilised to engage a broad audience. Additionally, the On Safe on Web website in Belgium serves as a centralised platform gathering links to commonly used websites like Facebook and Amazon, directing users to pages where they can set up two-factor authentication, thereby enhancing online security measures. Before the COVID-19 pandemic, a federal awareness-raising truck traversed the country, mainly targeting small towns to engage with citizens. These interactions revealed alarming levels of cybersecurity ignorance among some segments of the population, highlighting the crucial need for education and awareness initiatives (CCB, 2024).

In 2022, Estonia implemented two significant preventive campaigns aimed at enhancing the cyber hygiene of its residents due to a notably lower awareness level than the average, and the use of the best practices of cyber security decreases with age. The summer initiative specifically focused on Russian-speaking residents, while the broader call encouraged all Estonians to adopt a more IT-conscious approach (Cyber Security in Estonia, 2023).

In France, since 2017, the ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) has developed an online cybersecurity awareness course named SecNumAcadémie, tailored for the general public and non-specialist users. The primary aim

is to enhance the cyber awareness of these individuals, empowering them to actively contribute to their own security and that of their organizations. Comprising four modules covering cybersecurity fundamentals, authentication principles, internet security, and ubiquitous security, this MOOC enables users to grasp essential concepts of information systems security (ISS) applicable both in professional and personal settings. To date, the course has attracted 250,000 learners and issued over 45,000 certificates of achievement.

Greece spearheads numerous cybersecurity awareness campaigns at the national level, aligning with EU initiatives and bolstered by the Greek Safer Internet Centre (SIC). These efforts encompass a diverse array of events and resources tailored for students and the general public, such as treasure hunt games, seminars, infographics, videos, and presentations. These activities are orchestrated at a national level in conjunction with the EU Cybersecurity Month. Additionally, various national cybersecurity endeavors are championed by both official Greek governmental specialized institutions and authorities, including the Hellenic Police Cyber Crime division, National Intelligence Agency, or Hellenic Data Protection Authority. Furthermore, non-profit organizations play a pivotal role in raising cybersecurity awareness among students and the general populace. For instance, the Cyber Security International Institute (CSIi) improves public understanding of the digital realm and cybersecurity through educational programs, events, news sharing, consultations, and the establishment of three digital academies: Parent, Student, and Travel Editions.

In Luxembourg, BEE SECURE initiated a 2023 campaign to educate the public about cybersecurity essentials in response to the rising incidents of online fraud, including phishing, sextortion, and personal account hacking. The campaign, named 'Keep your space safe,' received support from various entities, such as municipalities, high schools, youth centers, childcare services, general practitioners, police offices, and telecommunications operators who actively distributed the "Secure your smartphone" leaflet in their boutiques and stores. In conjunction with the annual Cyber Security Month campaign, Spain arranges events to foster public awareness and a cybersecurity culture. The topics covered are vast, including IT security, cyber-attacks, consciousness, digital transformation, and guidance on identifying technological risks.

In Lithuania, the National Cyber Security Centre introduced a new free remote Cyber Hygiene training platform in 2023. The training covers nine topics, offering essential guidelines for secure digital practices and awareness of common cyber threats. Participants learn how to create and use passwords securely, protect their mobile devices, and safely work from home. The course also educates on phishing, SMS phishing (smishing), telephone fraud (voice phishing or vishing), and ransomware (National Cyber Security Centre, 2024).

In Spain, the INCIBE Strategic Plan 2021-2025 led by the National Institute of Cybersecurity of Spain (INCIBE), drives the country's digital transformation under the España Digital 2026 program. One of its pillars is strengthening cybersecurity for citizens, SMEs, and businesses with an investment of 98 million euro allocated for information, awareness, and training in

cybersecurity. This initiative encompasses various channels committed to cybersecurity awareness(for businesses, citizens, and minors), including the CONFIA program focusing on awareness, cybersecurity training, cooperation for consolidating a cybersecurity culture, and development of tailored technology solutions. Additionally, the response services of the Cybersecurity Helpline and incident response mechanisms via INCIBE-CERT are strengthened. Since 2014, the free Cybercamp initiative has promoted cybersecurity and digital trust, engaging citizens and entities through events like #cybercampULPGC, also involving educational institutions in the process. INCIBE also runs the Cybercooperators Program, fostering collaboration among cybersecurity experts and offering talks and workshops across all age groups. Moreover, in 2023, INCIBE initiated an awareness campaign on identity theft, providing resources to educate users about online risks and threats facilitated by social engineering techniques, such as phishing, vishing, and smishing.

In Cyprus, the Digital Security Agency of Cyprus (DSA), launched a campaign during the 2023 European Cyber Security Month (ECSM) focused on phishing, ransomware, and other cybersecurity threats to raise public awareness. Additionally, the National Competence Center of Cyprus (NCC-CY) introduced a Cyber-Hygiene Framework for small and medium enterprises (SMEs) to enhance their resilience against cyber threats. Furthermore, the ASPIS III campaign, now in its third year, continues to educate the general public about electronic fraud, ransomware, smishing, vishing, and phishing.

The Latvian Cybersecurity Strategy 2023- 2026 awareness-raising objectives focus on developing cybersecurity awareness for different segments of society, including children and youth, seniors, and government employees, to bolster their knowledge and understanding of cyber hygiene. The private sector has shown a growing commitment to enhancing cyber awareness among its workforce and establishing a more secure cyber environment. Deloitte (2023) reports that businesses of various sizes now employ multifaceted cyber awareness training models and tools, incorporating cyber awareness into the organizational culture. Organizations frequently implement comprehensive programs, including customized awareness sessions, quizzes, gamification, and simulation training, as part of their regular initiatives.

Overall, these initiatives offer valuable insights and materials covering various cybersecurity subjects, encompassing knowledge about cyber threats, adopting secure online practices, safeguarding personal information, and addressing cyber incidents. Notably, the assessment of the ESCM 2022 revealed a notable uptick in self-reported cybersecurity behaviors within the specified demographic (individuals aged 45-65) who accessed the campaign information. The data indicates a significant increase in various cybersecurity behavior types, including those related to email, password management, software updates, and network usage, following the campaign (Kalenti & Biro, 2023). Nevertheless, while providing valuable insights into the increased cybersecurity behaviors within the target group of individuals aged 45-65, the campaign impact study falls short in acknowledging the inherent diversity within this demographic. Treating this age group as a homogenous category overlooks the nuanced

variations in cybersecurity behaviors and awareness influenced by other socio-demographic factors such as socioeconomic status, disability or educational background.

Overall, the diverse array of cybersecurity awareness initiatives across Europe reflects a collective commitment to fostering a more secure digital environment. These multifaceted efforts, from EU-level campaigns to national and private sector initiatives, highlight the significance of continuous education and awareness to empower individuals in securely navigating the digital landscape. While there have been notable successes, constant evaluation and refinement are necessary to address evolving cybersecurity challenges and ensure inclusivity in awareness campaigns, considering the nuanced variations in cybersecurity behaviors influenced by various socio-demographic factors. Also, it is crucial to emphasize the necessity for evaluating the effectiveness of current cyber awareness initiatives. Continuous national, regional, and EU assessments, along with traditional methods like ex-ante and ex-post evaluations, are essential for this purpose. Without proper assessment, identifying and sharing best practices becomes challenging. By conducting thorough evaluations, we can ensure impactful cyber awareness efforts, enhancing cybersecurity across communities and sectors.

8. CHALLENGES AND GAPS IN CYBERSECURITY AWARENESS EFFORTS

While the cybersecurity awareness initiatives outlined by the EU Member States showcase progress, some notable challenges and gaps warrant attention. Despite the presence of thorough cybersecurity strategies, variations in implementation and efficacy may exist among different Member States. The European Court of Auditors (2019) briefing paper underscores that the Commission recognizes the cybersecurity strategy's effectiveness as only "partially effective" in enhancing awareness among citizens and businesses. This limitation is attributed to the magnitude of the undertaking, resource constraints, uneven involvement of Member States, and a dearth of scientific evidence on the most effective methods to raise and assess awareness (ECA, 2019, p.35).

Insufficient resources present a persistent challenge to achieving a comprehensive, whole-society approach to cybersecurity awareness. Limited funding constrains outreach efforts, hindering the implementation of an inclusive program that can effectively engage diverse demographic groups. Overcoming this resource constraint is crucial to ensuring the success of cybersecurity initiatives in reaching and benefiting a broad spectrum of individuals and communities. While the European Union has recognized the significance of cybersecurity, as evident in its prioritization through various funding initiatives like Horizon Europe, Erasmus+, Digital Europe Programs, and the Connected Europe Facility, the current support appears insufficient to enhance cyber awareness and resilience significantly. For instance, some European countries, like Estonia, face challenges obtaining resources for conducting polls,

highlighting a potential barrier to conducting comprehensive research and data gathering for targeted campaigns (Carrapico & Barrinha, 2017). In other words, guaranteeing sufficient and consistent national funding for society-level cybersecurity awareness initiatives remains challenging for some Member States.

Notably, a study commissioned by the European Economic and Social Committee (Kertysova et al., 2018) underscores a substantial gap between the increasing digitization of society and the allocation of resources dedicated to cybersecurity. The study highlights that both individual Member States and private enterprises lack adequate support for cybersecurity awareness, revealing a concerning trend where the rapid adoption of digital technologies is not met with a proportional commitment to fortifying defenses against potential cyber threats. Addressing this resource disparity is crucial to strengthening overall cybersecurity resilience within the EU.

Additionally, disparities persist among European countries in terms of their knowledge, awareness, and ability to implement strategies, programs, and capabilities in the realm of cybersecurity (Kertysova et al., 2018). While Estonia, France, Norway, and the United Kingdom serve as examples, Southern and Eastern European countries, particularly Slovenia and Slovakia, generally trail behind. The absence of essential capabilities in certain Member States exposes the European cybersecurity framework to fragmentation and susceptibility to potential attacks (Kertysova et al., 2018). Gaps in the overall defense mechanisms of specific Member States may lead to insufficient protection of individual's personal data and sensitive information. This, in turn, can result in a lower level of awareness among the general population about the importance of cybersecurity measures and the potential threats they face as the overall cybersecurity posture of the region is weakened.

Shifting people's attitudes is a gradual process. Identifying all target groups is crucial to prevent anyone from being overlooked. There seems to be a need for more targeted efforts towards vulnerable populations, such as the elderly, people with disabilities and individuals with lower education and socioeconomic status. While some countries like Croatia acknowledge the challenge and attempt to reach these groups through specific campaigns, more tailored approaches may be necessary to effectively engage and educate these demographics across the Union (Lee & Kim, 2020).

Despite the growing concern about cybersecurity, an emerging yet somewhat limited body of research investigates how individuals perceive and participate in cybersecurity practices (Kertysova et al., 2018). Further research is necessary to fully understand the challenge of cybersecurity awareness at the societal level, particularly in the European context. This involves examining cyberattacks' impact on individuals, their online security behaviors and strategies, and the accessibility of cybersecurity awareness information provided by public authorities. Conducting research in these areas could enhance our understanding of where citizens may have lower levels of cybersecurity literacy. This information would also be

valuable in developing tailored training programs and raising awareness among users about the likelihood and consequences of cyber threats.

Another challenge in enhancing cybersecurity awareness among the general population is to ensure that awareness-raising measures undertaken at both EU and national levels are not only well-targeted and effectively publicized but also inclusive, reaching diverse segments of the population (European Court of Auditors, 2019, p.35). A key consideration is to align these measures with the evolving threat landscape, adapting strategies to address emerging risks. Care must be taken to avoid unintended consequences like "security fatigue'. Research suggests that individuals may experience security fatigue, becoming weary of security measures perceived as hindrances to their primary activities (Bada et al., 2015). This fatigue can pose risks to the well-being of organizations and society at large.

In many instances, security awareness campaigns require significant effort and skills from the public, but the effectiveness of these measures in altering behavior is often unclear. Issues include the lack of alignment between solutions and risks, the absence of measurement for progress and value, incorrect assumptions about people and their motivations, and the establishment of unrealistic expectations (Bada et al., 2015). The effectiveness of cybersecurity awareness efforts is contingent on solid evidence of actual human behavior and the presence of user motivation to adopt the knowledge offered by the campaign and engage in cyber-safe practices.

The study conducted by Bada et al. (2015) emphasizes key factors for improving the effectiveness of cybersecurity awareness campaigns. It highlights the need for professionally organized campaigns, discourages fear tactics, emphasizes targeted and actionable cybersecurity education, stresses the importance of ongoing training and feedback during behavioral change, and underscores the significance of considering diverse cultural contexts in cybersecurity awareness efforts. Moreover, effective cybersecurity awareness campaigns require the expertise of public communication and marketing professionals to appropriately frame messages (de Bruijn & Janssen, 2017). Message framing involves communicating complex societal issues clearly and robustly in an easily understandable way.

Insufficient skills and competencies contribute to a lack of cybersecurity awareness in the general public. When individuals lack a fundamental understanding of cybersecurity principles, they may struggle to identify and address potential threats, increasing vulnerability to cyberattacks. The absence of comprehensive national educational programs in cybersecurity across Europe, the limited representation of cybersecurity in non-technical educational programs, and the lack of skills and training contribute to compromised cyber safety (Kertysova et al., 2018; Piesarskas et al, 2022). This could hinder Internet users from protecting themselves effectively against cyberattacks. Educating and raising public awareness through programs is crucial for empowering the public to navigate the digital landscape securely. As the ENISA report (2021b) highlights, a fundamental requirement for safeguarding digital systems against cyber incidents is possessing basic competencies and an

understanding of cyber threats, vulnerabilities, and effective countermeasures. Moreover, strengthening capabilities in education, research, and awareness initiatives at the national and European levels is essential for fostering cyber resilience among the general public.

Finally, addressing the challenges and gaps in cybersecurity awareness efforts within the European Union demands coordinated, sustained efforts from diverse stakeholders. Achieving comprehensive public cybersecurity awareness and resilience necessitates overcoming resource constraints, tailoring initiatives for diverse demographics, adapting strategies to the evolving threat landscape, and fostering collaboration among public authorities, industry, academia, and civil society organizations. The EU can only bridge existing gaps and fortify its overall cybersecurity posture through such collective endeavors.

9. POLICY RECOMMENDATIONS

This section presents a series of targeted recommendations aimed at key stakeholders to enhance cybersecurity awareness among the general population and address existing challenges and gaps in cyber awareness across the EU. These recommendations target key stakeholders involved in this multifaceted endeavor, encompassing governmental bodies, educational institutions, industry associations and civil society entities. By tailoring guidance to each stakeholder group's distinct roles and responsibilities, these recommendations aim to foster a collaborative approach to cybersecurity awareness.

Acknowledging the crucial role of an educated public in upholding European cybersecurity, this emphasis is placed on the need for sustained investment in tailored and easily accessible cyber awareness programs, implementation of comprehensive cross-disciplinary cybersecurity training programs, and promotion of transnational collaboration among Member States and relevant stakeholders to facilitate the exchange of best practices, resources, and expertise in cybersecurity awareness. Collectively, these recommendations aim to create a robust and adaptive cybersecurity awareness ecosystem, ultimately empowering individuals to navigate the digital landscape securely and fortifying the overall cyber resilience of the European population.

9.1. For Public Authorities & Policymakers

- Establish a comprehensive national cybersecurity awareness strategy with defined objectives, timelines, and performance indicators overseen by a dedicated government department or task force. Consider consolidating awareness-raising efforts within a single institution; however, as ENISA report on Raising-Awareness of Cybersecurity (2021b) indicates, there are also some successful exceptions where tasks are horizontally distributed.

- Integrate cybersecurity awareness goals into broader national policies related to education, digital literacy, and public safety. Create synergies with existing initiatives to maximize impact and outreach.
- Implement targeted cybersecurity awareness campaigns at local, regional and national levels to bridge the existing gaps and cultivate a culture of cybersecurity responsibility among European citizens. Employ diverse communication channels (e.g., TV, radio, social media, and community outreach) to ensure accessibility and resonance across diverse demographics. Evaluate and adapt campaigns continuously to address evolving cyber threats effectively.
- Incorporate socio-demographic considerations (e.g., gender, age, disability) in designing and implementing cybersecurity awareness measures to safeguard individuals facing elevated vulnerability and heightened risks in cybersecurity attacks. Ongoing education and empowerment efforts, tailored to diverse socio-demographic groups, are essential for bolstering cybersecurity resilience in our digital era.
- Conduct comprehensive national and EU-wide studies to assess cybersecurity behavior across all demographic groups. Utilize public surveys to gain crucial insights, informing targeted awareness initiatives that address the unique needs of different constituencies. Also, aggregated data from law enforcement agencies on cyber incidents can be utilized to identify trends and understand the impact on societal groups, determining optimal risk mitigation measures and enabling targeted awareness campaigns (ENISA, 2021b).
- Allocate sufficient and consistent funding to support national and local cybersecurity awareness campaigns. Provide national and EU grants to educational institutions, non-profit organizations, and community groups engaged in cyber awareness and education initiatives.
- Revise the existing European cybersecurity policy framework to shift from a predominantly state and organization-centric approach to a more inclusive model that empowers individuals. Introduce policies that promote a collaborative and shared responsibility for cybersecurity, recognizing individuals as active participants rather than passive recipients of cybersecurity services.
- Foster collaboration between government agencies, private sector organizations, academia and non-profit entities to jointly develop and implement cyber awareness programs. This partnership can harness the strengths of each sector to create comprehensive initiatives that respond to the unique needs of diverse cohorts, such as remote communities, linguistically diverse individuals, children, seniors, and people with disabilities.
- Encourage cooperation among EU Member States to exchange best practices, resources, and expertise in cybersecurity awareness. Facilitate the establishment of transnational cyber communities that unite various stakeholders, enabling the collective pooling of knowledge and sharing of experiences to improve cybersecurity awareness among the general public.

- Create a centralized online resource hub at the EU level, offering easily accessible cybersecurity guidelines, best practices, and resources curated explicitly for individuals with varying levels of cybersecurity awareness.
- Prioritize user-centric designs in cybersecurity awareness initiatives, tailor content and awareness-raising measures to diverse audiences, and regularly update resources to remain pertinent in the evolving cyber landscape. Emphasize adaptability, accessibility, and simplicity in conveying intricate cybersecurity concepts for improved user understanding and engagement.
- Establish helplines and support services at national and European levels where citizens can seek advice and assistance regarding cybersecurity issues. Ensure these services are accessible and provide timely guidance on reporting cyber incidents.
- Establish an EU Cybersecurity Awareness Award to acknowledge and reward outstanding contributions to cybersecurity awareness. Encourage organizations and individuals to innovate and excel in promoting a secure online environment.

9.2. For Educational Institutions

- Integrate comprehensive cybersecurity education into school and university curricula, adopting a lifelong learning approach. Develop tailored learning materials that are accessible as well as cross-cutting cybersecurity training programs, including dedicated cybersecurity awareness courses, workshops, or modules, to equip learners of all ages with essential cybersecurity knowledge, skills, best practices, and risk awareness.
- Provide ongoing training for educators to stay abreast of cybersecurity threats and solutions. Equipping teachers with updated knowledge allows them to convey essential information to students effectively.
- Integrate cybersecurity awareness and fundamental principles into non-technical training and educational programs at all levels and types of education. A basic understanding of cyber threats, areas of vulnerability, and effective preventive measures is essential to safeguard digital systems from cyber incidents. This mainstream approach can empower individuals with the knowledge and skills to protect themselves from cyberattacks.
- Conduct hands-on workshops and simulations (e.g., cyber escape games, capture-the-flags, cyber hackathons) that simulate real-world cyber threats. Practical exercises help individuals develop practical skills and understand the consequences of security lapses.
- Promote responsible online behavior, emphasizing cautious sharing of personal information, recognizing phishing attempts, preventing online banking fraud, identity theft, and understanding the consequences of cyberbullying.

- Foster collaborations with cybersecurity industry professionals to bring real-world insights and experiences into the classroom. Encourage internships, guest lectures, and mentorship programs to bridge the gap between academic learning and practical application.
- Establish a confidential reporting system for students, teachers, and staff to report suspicious online activities or potential cybersecurity threats. Encouraging reporting can contribute to early detection and mitigation of cyber incidents.

9.3. For Private Sector & Industry Associations

- Implement mandatory cybersecurity training programs for employees at all levels to improve the organization's cyber hygiene practices. Ensure that these programs cover topics such as phishing awareness, password management, and safe online practices at work and home.
- Offer incentives for cybersecurity certifications, such as performance bonuses or recognition, to employees who obtain cybersecurity certifications. Encourage ongoing professional development in cybersecurity through financial and non-financial incentives.
- Undertake customer-facing awareness initiatives by integrating cybersecurity awareness messages into customer communications, product packaging, and online platforms. Educate customers on secure practices, potential risks, and the importance of keeping their devices and accounts safe**.**
- Allocate resources to support local and national cybersecurity awareness initiatives and fund studies that explore effective methods of educating the public on emerging cyber threats.
- Encourage industry members to volunteer their expertise in schools and community centers for cybersecurity awareness sessions.
- Enforce cybersecurity training for private sector employees, with a specific focus on supply chain cybersecurity management. Train on core principles, threat awareness, and data protection. Establish protocols to assess and manage supply chain cybersecurity risks. Prioritize supply chain cybersecurity to bolster overall resilience and safeguard the public from cyber threats.

9.4. For Civil Society Entities

- Organize community-based workshops and training sessions to educate individuals on cyber awareness best practices. Tailor the content to address specific concerns of diverse groups within the community.

- Host community awareness events and forums to engage the community in discussions on cybersecurity. Address local issues, share success stories, and encourage a sense of collective responsibility for online safety.
- Support the formation of grassroots cybersecurity advocacy groups within communities. Empower citizens to actively promote cybersecurity awareness and share best practices within their social circles.
- Advocate and provide inputs for policies that aim to address the existing cybersecurity awareness gap and promote awareness of the risks associated with inadequate cybersecurity practices and the potential impact on individuals and society.
- Partner with local schools and VET providers to supplement their cybersecurity education efforts. Provide resources, speakers, and support for extracurricular cybersecurity clubs or activities.

10. CONCLUSIONS

The existing gap in cybersecurity awareness within the general population of Europe is a cause for concern, with a significant number of citizens expressing a lack of knowledge and reluctance to report cybercrimes to law enforcement. This policy brief highlights the disparities in societal-level cybersecurity awareness across EU Member States. The variations in individual cybersecurity awareness, influenced by sociodemographic factors and institutional resources, particularly impact vulnerable demographic groups such as senior citizens and children. The consequences of cybersecurity attacks extend beyond immediate risks, causing reputational damage that affects individuals' credibility and trust. As our world becomes increasingly digital, society-level awareness and education on cybersecurity are no longer optional but necessary. The dynamic nature of the cybersecurity environment requires adaptable strategies to keep the public well-informed and prepared for emerging threats.

Joint initiatives and cybersecurity literacy training programs should be developed to tackle existing challenges, emphasizing stakeholder collaboration effectively. Building robust, sustainable, and collaborative partnerships among relevant stakeholders is essential to address system-level cybersecurity concerns comprehensively. Integrating cybersecurity practices into daily routines, similar to established habits like handwashing, is crucial to enhancing cyber awareness, especially among those struggling with online protection concepts. Ensuring an open, safe, and secure cyberspace is vital for the reliable operation of European societies and economies. Allocating resources to programs and research to improve cybersecurity hygiene is not only a wise investment but also holds the potential for extensive social and economic benefits. The collective effort to enhance public awareness and education on cybersecurity requires active participation from all segments of society. Through collaborative practices, we can empower everyone with the knowledge and skills needed to navigate the digital world securely, thereby contributing to the overall cybersecurity resilience of our communities.

REFERENCES & FURTHER READING

Abawajy, J. (2014). User Preference of Cyber Security Awareness Delivery Methods. *Behavior & Information Technology*, *33*(3), 237-248.

Ahmed, A., SSCP. (2023, July 11). Enhancing Public Awareness and Education in Cybersecurity: *A Canadian Perspective*. https://doi.org/10.31219/osf.io/xgzy8

Aizsardzības ministrija. (n.d.). The Cybersecurity Strategy of Latvia 2023-2026. Retrieved from https://www.mod.gov.lv/mod/files/document

Aloul FA. The Need for Effective Information Security Awareness. *J Adv Inf Technol*. 2012;3(3):176–83. doi:10.4304/jait.3.3.176-183

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, *69*, 437-443.

Bada, M., Sasse, A., Nurse, J.(2015). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behavior? *International Conference on Cyber Security for Sustainable Society*.

Bada, M., Nurse, J. (2019). The Social and Psychological Impact of Cyber-Attacks in Emerging Cyber Threats and Cognitive Vulnerabilities, pp.73-92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

BBC News. (2017, May 15). Doctors' Emotional Resilience 'at Risk' From Tough Working Conditions. Retrieved from https://www.bbc.com/news/health-39899646

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems*, *61*(3), 195-206.

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber) Security Actor?. JCMS: Journal Of Common Market Studies, 55(6), 1254-1272.

Chronicle.lu. (2023, November 7). Bee Secure Launches New Cybersecurity Awareness Campaign. Retrieved from https://chronicle.lu/category/ict/47356-bee-secure-launches-new-cybersecurity-awareness-campaign

Dalal, R. (2023, February 22). Elevating Cyber Awareness Within Organizations. Retrieved from https://www.deloitte.com/global/en/services/risk-advisory/blogs/elevating-cyber-awareness-within-organizations.html

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, *34*(1), 1-7.

DNS Belgium. (n.d.). Cybersecurity Campaign Against Phishing. Retrieved from https://www.dnsbelgium.be/en/news/cybersecurity-campaign-against-phishing

Cypriot Digital Security Authority. (2023). *Cyber-Hygiene Framework for Small and Medium Enterprises (SMEs)*. National Cybersecurity Centre (NCC-CY). Retrieved from https://ncc.cy/images/ENGLISH_HYGIENE.pdf

Cybersecurity National Coordination Centre Cyprus.(n.d.). *Commissioner of Communications Message.* Retrieved from https://ncc.cy/en/ncc

Enescu, S. (2020). A Comparative Study on European Cyber Security Strategies. *Redefining Community in Intercultural Context*, *9*(1), 277-282.

EURACTIV. (2019, December 13). Cybersecurity: What does it mean to EU citizens?. YouTube. https://www.youtube.com/watch?v=WqHGKniUCmM&t=178s&ab_channel=Euractiv

European Commission. (2014). *Special Eurobarometer 390: Cyber security*. Retrieved from https://data.europa.eu/data/datasets/s1058_77_2_ebs390?locale=en

European Commission. (2019a). *Special Eurobarometer 480: Europeans' Attitudes towards Internet Security.* Retrieved from https://data.europa.eu/data/datasets/s2207_90_2_480_eng?locale=en

European Commission. (2019b). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance*). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Commission. (2020a). *Joint Communication to the European Parliament and the Council-EU's Cybersecurity Strategy for the Digital Decade*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2020b). Special Eurobarometer 499: *Europeans' Attitudes towards Cyber Security (cybercrime*). Retrieved from https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en

European Commission. (2022). *Digital Skills Coalition*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-skills-coalition

European Commission. (2023). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555

European Commission. (2023). *The Digital Economy and Society Index (DESI)*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/desi

European Commission. (2024). *Safer Internet Day*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/safer-internet-day

European Council. (2023). *Cyber threats in the EU* [Infographic]. Retrieved from https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

European Court of Auditors. (2019). *Challenges to Effective EU Cybersecurity Policy- Briefing Paper*. European Court of Auditors.

European Cyber Security Organization. (n.d.). *Building the Future of European Cyber Security Awareness Campaigns*. Outcome paper from ECSO workshop. Retrieved from https://ecs-org.eu/ecso-uploads/2022/10/5fad5305488be.pdf

European Cyber Security Organisation. (n.d.). *Cybersecurity Awareness Calendar*. Retrieved from https://ecs-org.eu/activities/cybersecurity-awareness-calendar/

European Cyber Security Month.(n.d). *National Campaign Coordinator Greece*. Retrieved from https://cybersecuritymonth.eu/countries/greece

European Union Agency for Cybersecurity (ENISA). (n.d.). *European Cybersecurity Month*. Retrieved from https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month

European Union Agency for Cybersecurity (ENISA). (n.d.). *CIRAS Incident Reporting*. Retrieved from https://ciras.enisa.europa.eu/

European Union Agency for Cybersecurity.(2021a). *Threat Landscape 2021- April 2020 to mid-July 2021* . Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Union Agency for Cybersecurity. (2021b). *Raising awareness of cybersecurity*. Retrieved from https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023: July 2022 to June 2023*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity Regulation in The European Union: The Digital, the Critical and Fundamental Rights. The Ethics of Cybersecurity, 97-115.

French Republic. (n.d.). *SecNumAcadémie*. Retrieved from https://secnumacademie.gouv.fr/

Gomez, M. A., & Shandler, R. (2022). Cyber Conflict and the Erosion of Trust. Retrieved from https://www.cfr.org/blog/cyber-conflict-and-erosion-trust

Hansche, S. 2008. Designing a Security Awareness Program: Part I. Information System Security 10(1), 14–22

Jalali MS, Siegel M, Madnick S. Decision-Making and Biases in Cybersecurity Capability Development: Evidence From A Simulation Game Experiment. J Strategic Inf Syst. 2019;28(1):66–82. doi:10.1016/j.jsis.2018.09.003

Jardine, E., Porter, N., & Shandler, R. (2024). Cyberattacks and Public Opinion–The Effect of Uncertainty in Guiding Preferences. *Journal of Peace Research*, 00223433231218178.

Kalenti, M., Biro, P. (2023). European Cybersecurity Month 2022 Campaign Report. *European Union Agency for Cybersecurity*. Retrieved from https://www.enisa.europa.eu/publications/european-cybersecurity-month-2022-campaign-report

Kertysova, K., Frinking, E., Dool, K. V. D., Maričić, A., & Bhattacharyya, K. (2018). Cybersecurity: Ensuring Awareness and Resilience of The Private Sector Across Europe in the Face of Mounting Cyber Risks. Study of The Hague Centre for Strategic Studies for The European Economic and Social Committee (EESC).

Kosling, K. (2023, December 15). Data Breaches and Cyber Attacks in Europe in November 2023. Retrieved from https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-europe-in-november-2023-111218696

Leal, M. M., & Musgrave, P. (2023). Hitting Back or Holding Back in Cyberspace: Experimental Evidence Regarding Americans' Responses to Cyberattacks. *Conflict Management and Peace Science*, *40*(1), 42-64.
Lee, KG., Chong, CW., Ramayah T. (2017) Website Characteristics and Web Users' Satisfaction in a Higher Learning Institution. *Int J Manage Educ*. 2017;11(3):266–83. doi:10.1504/IJMIE.2017.084926

Lee, C. S., & Kim, J. H. (2020). Latent Groups of Cybersecurity Preparedness in Europe: Sociodemographic Factors and Country-Level Contexts. *Computers & Security*, *97*, 101995.

Lithuanian National Cyber Security Centre.(n.d.). *Cyber Security Incident Analysis and Reports*. Retrieved from https://www.nksc.lt/en/

Mattioli, R., Malatras, A.(2024). Foresight Cybersecurity Threats For 2030 – Update. *European Union Agency for Cybersecurity*.https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary

Matzkin, S., Shandler, R., & Canetti, D. (2023). The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment. *The British Journal of Politics and International Relations*, 13691481231210383.

McKenna, S., Staheli, D., & Meyer, M. (2015, October). Unlocking User-Centered Design Methods for Building Cyber Security Visualizations. In *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)* (pp. 1-8). IEEE.

Morrison, B.A., Coventry, L., Briggs, P. 2020. Technological Change in the Retirement Transition and the Implications For Cybersecurity Vulnerability in Older Adults. *Frontiers in Psychology,* doi: 10.3389/fpsyg.2020.00623

National Institute of Cybersecurity of Spain. (n.d.). *What is CyberCamp?*. Retrieved from https://www.incibe.es/eventos/cybercamp/sobre/cybercamp

National Institute of Cybersecurity of Spain. (n.d.). *Confía*. Retrieved from https://www.incibe.es/ed2026/confia

National Institute of Cybersecurity of Spain. (n.d.). *The Cybercooperantes Program*. Retrieved from https://www.incibe.es/incibe/cibercooperantes

Öğütçü, G., Testik, Ö.M., Chouseinoglou, O. 2016. Analysis of Personal Information Security Behavior and Awareness. *Computers & Security*, 56, 83–93.

Panhans, D., Hoteit, L., Yousuf, S., Breward, T., AlFaadhel, A. M., & AlShaalan, B. H. (2022, September 21). Why Children Are Unsafe in Cyberspace. Retrieved from https://www.bcg.com/publications/2022/why-children-are-unsafe-in-cyberspace

Papakonstantinou, V. (2022). European Cybersecurity in Context: A Policy-Oriented Comparative Analysis. *Available at SSRN 4211604*.

Piesarskas, E., Alksnys.,D, Valutytė, R., Ricci, S., Jerabek, J., Dán, G., Stupka,V., Danidou.Y., James Blake, P., Zafeiriades, D., Kosmadakis, D., Zharkalliu ,K., Karras, A., Georga, F., Delgado, A., Sánchez, J., Judickaitė, D., Pakutinskas, P. (2022). R2.3.1. Cybersecurity Skills Strategy. REWIRE - Cybersecurity Skills Alliance- A New Vision for Europe. https://rewireproject.eu/wp-content/uploads/2022/05/R2.3.1-Cybersecurity-Skills-Strategy_FINAL-v1-compressed.pdf

Renaud, K., & Coles-Kemp, L. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. *SN computer science*, *3*(5), 346. https://doi.org/10.1007/s42979-022-01239-1

Republic of Estonia Information System Authority.(2023). *Cyber Security in Estonia 2023*. Retrieved from https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf

Ricci, S., Jerabek, J., Dán, G., Lendak, I., Varga, V., Piesarskas, E., Pakutinskas, P., Alksnys, D.(2022). *R.2.1.1. PESTLE Analysis Results*. REWIRE - Cybersecurity Skills Alliance A New Vision for Europe.

Shandler, R., & Gomez, M. (2023). The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government. *Journal of Information Technology & Politics*, 20:4, 359-374, DOI: 10.1080/19331681.2022.2112796

Schultz, E. (2005). The Human factor in Security. *Computers & Security*, *6*(24), 425-426

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. oup usa. https://doi.org/10.1093/wentk/9780199918096.003.0001

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies. *Journal of Cybersecurity*, *7*(1), tyab019.

Spanish Government. (n.d.).*Strengthening Cybersecurity for Citizens, SMEs, and Professionals.* Retrieved from https://espanadigital.gob.es/medida/fortalecimiento-de-la-ciberseguridad-de-la-ciudadania-pymes-y-profesionales

Spanish Government. (2021). *Plan Estratégico INCIBE 2021-2025 De miles a millones*. Retrieved from https://www.incibe.es/sites/default/files/paginas/que-hacemos/plan_estrategico_INCIBE_2021-2025_y_resultados_conseguidos_2021-2022.pdf

Spanish National Security Department. (2019, October 1). *European Cybersecurity Month Spain*. Retrieved from https://www.dsn.gob.es/ca/actualidad/eventos-seguridad-nacional/european-cybersecurity-month-spain

Sultan, A. H. M. A. D. (2019). Improving Cybersecurity Awareness in Underserved Populations. *Center for Long Term Cybersecurity, UC Berkely. https://cltc. berkeley. edu/wpcontent/uploads/2019/04/CLTC_Underserved_Populations. pdf.*

University of Las Palmas de Gran Canaria.(2022). *INCIBE and ULPGC Organize an Awareness and Training Program on Cybersecurity*. Retrieved from https://www.ulpgc.es/noticia/2022/12/05/incibe-y-ulpgc-organizan-programa-concienciacion-y-formacion-ciberseguridad

Verizon. (2018.). *Data Breach Investigations Report*. Retrieved from https://www22.verizon.com/wholesale/contenthub/data_breach_investigation_report.htm

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323-338.

Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With New Examples of Knowledge, Skills and Attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(6), 315-331.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82-97.