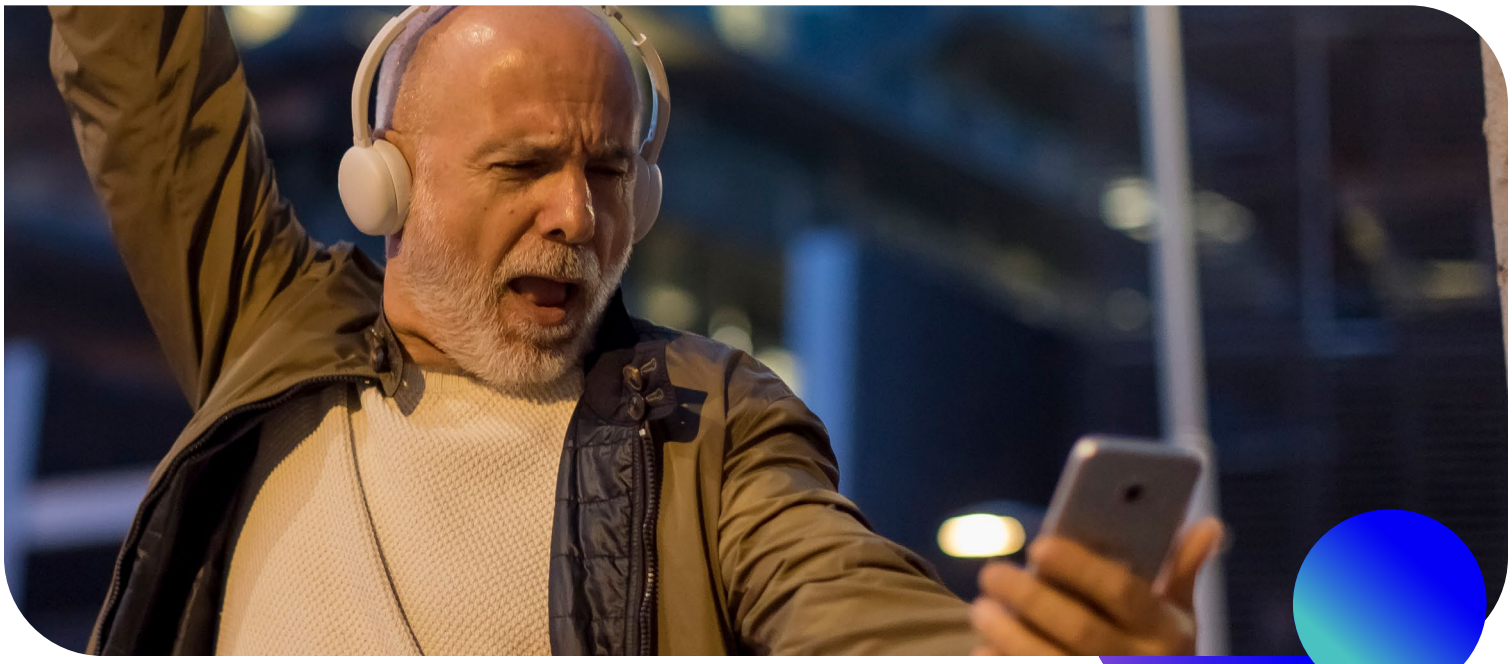
Gen™

DIGITAL FREEDOM IN THE EU

Building a safe digital world.



Gen's recommendations for the next EU mandate

Gen, a global tech leader

Gen is a global cybersecurity leader, with dual headquarters in Prague, Czech Republic and in Tempe, Arizona. The company marks its presence in over 150 countries, catering to nearly 500 million users worldwide. The Gen portfolio includes comprehensive cybersecurity solutions from a family of trusted brands such as Norton, Avast, LifeLock, Avira, AVG, ReputationDefender, and CCleaner.

Digital Freedom as a key principle

Powering Digital Freedom lives at the heart of everything Gen does. This goes beyond the Company's mission to create solutions that enable people to navigate their digital lives safely, privately, and confidently. It's about empowering both the generations of today and future generations to be able to take advantage of the ease technology offers, worry free. That's why Gen approaches everything we do with the customers and communities we serve in mind. We champion the simplification and safeguarding of customer experiences in the ever-evolving digital landscape, reinforcing our role as a leader in digital security and empowerment.

Gen

Leveraging Artificial Intelligence safely to protect people

Recent considerable advances in generative AI and Large Language Models (LLMs) such as ChatGPT and Google Gemini (previously Bard) has attracted global interest and provided a useful assistant for a range of everyday tasks. And as this technology gets more sophisticated, so do the threats that come along with them.

Cybercriminals are leveraging AI at an unacceptable level to:

- Use AI-generated content on social media to disseminate fake news, deceptive advertisements, deepfakes of public figures, or even direct messages that appear to come from trusted contacts.
- Expand their capabilities beyond text generation; they now have text-to-video and other multi-media creation tools. These advancements make it progressively harder to distinguish a true recorded video from a generated one, especially when videos are frequently cut, such as with TV news.
- Develop new malicious LLMs in the future without built-in safeguards, like "WormGPT", designed to support the generation of malicious content and creation of malwares.
- Increase the likelihood of misinformation or unethically sourced data. Generative AI and LLMs are rooted in the quality of the data it is sourcing from. Inaccurate or unethically sourced data not only leads to legal and ethical issues but also jeopardizes AI reliability. This potentially transforms these technologies into vehicles for misinformation and security threats. Essentially, the safety and effectiveness of AI hinges on the integrity of its foundational data.

Generative AI and LLMs present opportunities for the cybersecurity of consumers:

- With informed vigilance, accurate cybersecurity tools, and adherence to safety guidelines, people will be able to navigate the online world even more securely.
- Generative AI and LLMs can bolster cybersecurity and support security research by providing insightful analytics and AI-based assistant tools. For example, LLMs can automate and enhance penetration testing, identifying vulnerabilities and covering more potential weaknesses, which can lead to an overall more resilient system.

Recommendations

- Implement a robust disclosure mechanism that indicates that publications and impactful online content (including web content, blogs, and particularly image, video, and audio) are digitally signed – in a similar way software is signed. This allows the consumer to understand if content is artificially generated or not or whether it was tampered with or not. This signature should be easily identifiable and verifiable by the consumer to ensure transparency and trust in the content. To start, it should be available on all social media platforms.
- Launch EU-wide campaigns to increase public awareness and foster AI literacy addressing the potential benefits and risks associated with AI technologies.
- Promote the development and adoption of AI-based tools and methodologies to enhance cybersecurity measures, including malware and scam detection and response.
- Champion policies and solutions ensuring that consumers can simply determine if the person, organisation or IoT and software they are dealing with is genuine.

Ensure the success of digital identity

The average individual manages over 150 online accounts, with personal data scattered across numerous databases globally.[1] The escalating trend of data breaches amplifies the threat of identity fraud. Gen aims for a future where individuals have full control over their data, ensuring a safe, private, and secure data-sharing experience across digital platforms.

Privacy should not be compromised for access to online services. Gen strives for intuitive, cross-platform solutions, offering tools that empower individuals to manage their data and identity.

The cornerstone of Digital Freedom lies in open standard digital wallets, facilitating seamless transactions and management of trusted digital relationships across popular platforms, free from vendor lock-ins. As a Founding Premier Member of the OpenWallet Foundation (OWF), we are a pioneer in the movement towards open-source, interoperable digital wallets. Partnering with entities like the Linux Foundation, OWF looks to drive global adoption of secure digital wallet solutions, setting industry best practices that uphold choice, security, and privacy.

Recommendations

- Support collaborative efforts like OWF that aim to drive global adoption of open, secure, and interoperable digital wallet solutions.
- Promote an international standard, or “safety score,” for people to see how safe any digital wallet is. A “safety score” will allow the direct comparison of different digital wallets from the perspective of privacy protection, security, certification compliance and legal compatibility. Gen and the OWF are creating such a standard right now.
- Adopt policies that promote and support an open-source environment, fostering collaborative and transparent development in digital identity solutions.
- Ensure the success of eIDAS 2.0 by educating the public on its benefits and the cybersecurity aspects of digital wallets to help drive informed and secure adoption.
- Ensure the user experience of eIDAS wallets is as good or better than the pre-installed wallets.

[1]Digital Trust: Putting Your Information Under Your Control (avast.com)

Reinforce consumers' privacy and control

At Gen, our commitment to privacy is foundational. Our customer-first approach ensures personal data is processed with the utmost respect for privacy, embedding robust privacy measures seamlessly into our products. Gen processes data in a manner aligned with expectations of our customers and strives for maximum transparency. We encourage consumers to safeguard their online presence and use effective privacy strategies. While personalized online experiences offer significant value to consumers, it also presents major societal threats particularly in the context of generative AI. Because extensive data collection is needed for personalisation, this can lead to privacy concerns. Another potential risk is biases in AI algorithms that can lead to unfair or discriminatory outcomes. Furthermore, there is a risk of echo chambers and misinformation, as AI-driven personalisation can narrow the diversity of information people are exposed to, reinforcing pre-existing misbeliefs or spreading false content.

Recommendations

- Reinforce the Digital Services Act mandating all online platforms and service providers promote client-side recommendations, personalisation transparency and make sure that the platforms are open to third-party personalisation control and explainability technology.
- Establish a European standardised label certifying the cybersecurity and privacy compliance of IoT devices, ensuring they adhere to robust data protection and security standards.
- Launch comprehensive data privacy education campaigns to inform and educate people so they are capable of protecting their personal data in the digital realm.
- Advocate for policies that bolster individuals' control over their data, facilitating easy management, retrieval, or deletion of personal data.
- Focus on promoting transparency of processing of personal data and increasing pressure on companies engaging in activities manipulating user behaviour.

Strengthen consumer protection on all digital platforms

Consumers should have the freedom to choose their cybersecurity provider, allowing them access to monitor their full digital experience on desktop, mobile and in the cloud. This choice empowers people to defend against scams and malware, shifting control from providers to the individual, and fostering a more secure digital environment.

Some digital platforms restrict cybersecurity solutions from accessing some key system components. The loss of access to these control points – ones that are necessary for consumers to fully benefit from the solutions offered by their cybersecurity provider – creates not only competition issues but, more importantly, exposes consumers to cybersecurity risks as it limits their use of the cybersecurity products they've chosen.

The debate around consumer digital security also extends to online platforms, including social networks, messaging applications and in the future metaverse. Given that most scams, particularly AI-based ones, are disseminated through these platforms, it is important for third-party cybersecurity providers to have access to the online platforms to increase consumer protection against cybersecurity threats.

Recommendations

- Create an obligation for digital platforms, operating systems and digital service providers to offer options including third-party antivirus and cybersecurity solution providers during the initial setup or installation process of devices. This promotes consumer choice and awareness.
- Digital platforms, operating systems and digital service providers to ensure their products are designed and developed to enable seamless integration and compatibility with a wide array of third-party anti-malware, anti-scam, anti-fraud and other cybersecurity solutions.

Close the cybersecurity skill gap in EU

The recent surge in cybercrime, with Avast blocking 10 billion attacks in 2023 (49% increase year-over-year)[2] and attributing more than 75% of all threat detections on desktops to scams, phishing, and malvertising, starkly demonstrates the urgent need for enhanced cybersecurity skills and awareness. This dire situation underscores the necessity for comprehensive education and a push for cybersecurity competence regardless of factors like age, gender, ethnicity or geography.

In response to this critical need, Gen's active support for Women4Cyber, through a significant annual contribution of €141,000 over three years, marks a commendable step towards addressing the gender disparity in the cybersecurity field. This initiative aligns with Gen's broader social impact goals and its ESG strategy, which focuses on Cyber Safety education and training, diversity and inclusion, environmental stewardship, and data privacy.

Recommendations

- Launch comprehensive cyber literacy programs to educate the public on basic and evolving cybersecurity principles, the risks associated with cybercrime, and the steps individuals can take to protect themselves online.
- Establish Key Performance Indicators (KPIs) on women's participation in the cybersecurity sector as part of the Digital Decade agenda to promote gender diversity and inclusion.
- Foster public-private partnerships to develop and deliver cybersecurity training programs, leveraging the expertise and resources from both sectors to improve cyber literacy and skills.
- Reinforce the Cybersecurity Skill Academy to turn it into a centralized online platform providing accessible cybersecurity resources, training modules, and awareness campaigns to educate the public and organizations on prevailing cyber threats and best practices.
- Offer incentives to organizations that invest in cybersecurity training for their employees, encouraging a culture of continuous learning and awareness.

[2] Avast Q3/2023 Threat Report - Avast Threat Labs

Further and more detailed reports by Gen threat labs and experts:

Gen: “Insights into AI-based cyberspace.” August 2023. Available at: https://cmsb.nortonlifelock.com/sites/default/files/2023-09/LLM%20malware%20090523.pdf
Gen: “Cybersecurity Predictions for 2024. Navigating the evolving landscape.” December 2023. Available at: https://www.gendigital.com/blog/news/innovation/cybersecurity-predictions-2024
Gen: “Hierarchical Multi-Instance Learning for Transactional Data. Using HMIL architecture to process complex data.” December 2023. Available at: https://www.gendigital.com/blog/news/innovation/hmil-transactional-data

Gen is a global company with a family of trusted consumer brands.