Gen™

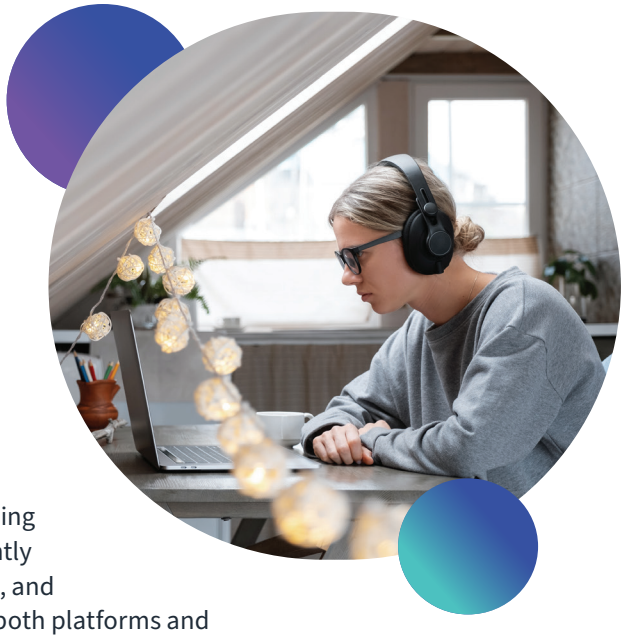
2025

Gen Digital Position Paper:

Combatting Online Scams in the EU

A Call for Enhanced Cyber Safety Collaboration

norton™ Avast™ LifeLock™ by norton MoneyLion®



Executive Summary

Online scams have surged to epidemic levels worldwide and in the EU. The Global Anti-Scam Alliance (GASA) reports that consumers lost close to €1 trillion to scams globally in the past year. At the same time, nearly half of EU consumers encountered online scams, resulting in severe financial losses and has inflicted severe financial damage across the Union. It's getting worse in 2025 with estimated losses of €10 billion in Germany, €7.6 billion in France, and more than €1 billion in Denmark. Social media platforms are primary channels for sophisticated scams, including impersonations, fraudulent job offers, and investment schemes. AI significantly enhances these scams through convincing deepfake videos, synthetic voices, and personalised phishing attempts, complicating detection and prevention for both platforms and consumers. This creates a critical need for a dedicated, preventive layer of cybersecurity that operates across platforms to protect users. As a global leader in consumer cybersafety, our data provides a unique, real-time view into how these cross-platform scams operate.

Major criminal groups, such as CryptoCore, have extensively employed AI technologies, resulting in substantial losses, including over $10.8 million from cryptocurrency scams in just six months. Such scams are further exploited by criminals for large-scale money laundering, disproportionately affecting digitally vulnerable groups, particularly elderly populations.

To combat this escalating threat, Gen Digital (Gen) urges the EU to adopt a robust and coordinated policy response.

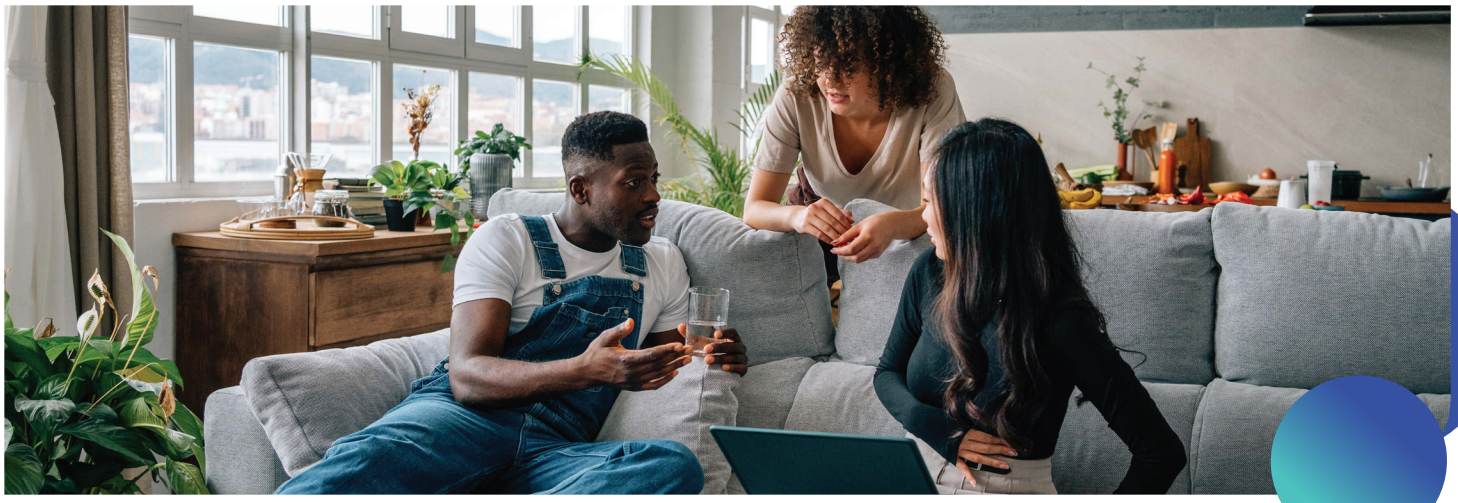
1. **Develop an Action Plan against Online Fraud:**

   Implement proactive measures powered by real-time threat intelligence from frontline cybersecurity providers, stakeholder collaboration and guidelines on how to tackle online fraud at its root.
2. **Establish a multi-stakeholder forum:**
   Establish a multi-stakeholder forum on online scams, bringing together online platforms, cybersecurity providers, financial services, and consumer advocacy groups to develop and implement collective solutions.
3. **Expand ENISA's mandate:**
   Strengthen ENISA role to initiate consumer-focused cybersecurity guidance, targeted public awareness campaigns for vulnerable groups, and collaboration with consumer protection entities.

Addressing these recommendations will be vital for the EU to effectively mitigate the rapidly evolving threat posed by AI-driven online scams.

"Major criminal groups, such as CryptoCore, have extensively employed AI technologies, resulting in substantial losses, including over $10.8 million from cryptocurrency scams in just six months. Such scams are further exploited by criminals for large-scale money laundering, disproportionately affecting digitally vulnerable groups, particularly elderly populations. Addressing these issues will be vital for the EU to effectively mitigate the rapidly evolving threat posed by AI-driven online scams."

Leyla Bilge - Global Head of Scam Research



State of Play: Scams in the EU and the Impact of Generative AI

Online scams, amplified by the misuse of generative AI, have **reached alarming levels across the European Union**. Nearly **half of EU consumers encountered online fraud** in 2024, leading to an immense financial toll. Germans are expected to loose an estimated **€10 billion** in 2025 and at the same time, French citizens, will loose €7.6 billion, and Danish consumers over DKK 6.9 billion (more than €1 billion) [1].

Moreover, Gen Digital's (Gen) threat insights confirm that **generative AI significantly amplifies fraud risk** by enabling scammers to create highly convincing content, such as deepfake videos, synthetic voices, and personalised phishing texts, which evade traditional detection.

Social media is the primary arena for these sophisticated scams. Scammers increasingly exploit the vast user bases and diverse functionalities of social media platforms, employing advanced methods to deceive individuals. A notable example is the "TikTok Elon Musk Scam" in which fraudsters impersonated the tech billionaire to promote fraudulent cryptocurrency giveaways. This scheme effectively preyed on Musk's real-world influence and TikTok's younger, tech-curious demographic, enticing victims to send funds under false promises of substantial returns.

Another of many examples is the CryptoCore group that utilised AI-generated deepfakes of public figures, cloned websites, and hijacked YouTube accounts to impersonate significant media events, particularly targeting cryptocurrency users. In Q4 2024 and Q1 2025 alone, CryptoCore stole over $10.8 million through these sophisticated, social-media-driven scams. Their tactics notably intensified during public events, such as Donald Trump's inauguration, during which they hijacked additional YouTube accounts, rebranding them to appear as official channels associated with prominent figures.

Our unique cross-platform monitoring provides crucial data on this trend. In Q1 2025 alone, Gen's technology acted as a vital preventive measure, blocking more than 4 million individuals from 'Scam-Yourself' attacks. These attacks, where victims are manipulated into compromising their own devices or accounts (also known as trick-install scams), predominantly leveraged AI-generated personas, deepfake influencers and platform-native advertising systems on social media to enhance their credibility before luring users to external malicious applications, demonstrating the need for protection beyond the platforms themselves. For example, a completely AI-created YouTube "influencer" named Thomas Harris guided victims toward installing malicious trading applications.

In another "Trading Bot Scam," over 15 different AI-generated or deepfake personas appear on social media videos telling people how to double their crypto investments.

These examples highlight a fundamental challenge: scams often originate on social media but lead victims to malicious websites or apps on different platforms. This cross-platform journey makes it **difficult for any single platform to have full visibility**, underscoring the necessity of independent cybersecurity solutions that protect the user wherever they go online.
In short, **AI makes scams more personalized and deceptive, bypassing traditional defences** [2]. These schemes disproportionately **harm digitally vulnerable groups**, such as older adults, while also feeding large-scale **money laundering** networks across Europe, as evidenced by Europol [3].

Policy Recommendations for the EU

The convergence between artificial intelligence capabilities and traditional fraud techniques has generated a major threat to EU consumers and the economy, requiring immediate and coordinated action involving all relevant stakeholders.

Gen recommends the following actions:

1. Develop an Action Plan against Online Fraud:

In its ProtectEU Communication, the European Commission committed to develop an Action Plan against Online Fraud. This initiative aims to proactively address fraud and scams at their source, building upon discussions related to the Payment Services Regulation (PSR) and Payment Services Directive 3 (PSD3), which focuses on mitigating the consequences.

We recommend that the Action Plan should incorporate the following elements:

- Clear objective to support consumers, online platforms, and the financial industry (particularly addressing costs and reputational losses).
- A joint task force that brings together law enforcement, payment service providers, online platforms, cybersecurity providers, anti-money laundering authorities and associations representing consumers and vulnerable groups.
- Real-time threat intelligence and data-sharing mechanisms among all involved stakeholders, leveraging the vast, aggregated datasets from consumer cybersecurity providers to gain a comprehensive view of emerging scam tactics.
- Harmonised, accessible channels for incident reporting, alongside clear guidelines for victim support and assistance.

2. Foster multi-stakeholder collaboration to fight scams and fraud on platforms

The existing focus on impersonation fraud targeting Payment Service Providers must be broadened into a comprehensive approach addressing fraud and scam prevention across all online platforms. Success will depend on recognising that consumer cybersecurity services provide a crucial, cross-platform preventive layer. These services monitor for threats across web, social media, and messaging apps, offering protection where platform-native safety measures end.

The Commission should set-up a multistakeholder forum on fighting scams and fraud on platforms. It should include:

- All relevant stakeholders including online platforms, payment service providers, cybersecurity specialists who offer this preventive cross-platform monitoring, consumer groups, and vulnerable group organisations.
- Collective identification and implementation of effective anti-fraud measures.
- Concrete commitments from stakeholders for proactive measures that complement existing legislation like the AI Act, DSA, and PSR.
- Best practices from industry and NGOs.

3. Expand ENISA's mandate to focus on fraud and scams

Amid the ongoing review of the Cybersecurity Act, ENISA's mandate should explicitly prioritise consumer cybersecurity protection. Given that AI-driven scams often exploit a lack of user awareness, strengthening the EU's primary cybersecurity agency's role in public education is critical. Specifically, ENISA should:

- Develop and promote accessible, user-oriented best practices for digital safety, cybersecurity hygiene, and secure everyday technology usage.
- Launch targeted public awareness campaigns aimed at consumers, with particular emphasis on vulnerable demographics such as older adults and minors. These campaigns should provide clear guidance on secure practices in digital platforms, e-commerce transactions, and emerging threats such as social engineering and scams.
- Formalise and deepen collaboration with consumer organisations and cybersecurity firms to ensure consumer perspectives are integrated into cybersecurity policy development and implementation.

About Gen

At Gen (NASDAQ: GEN), our mission is to create innovative and easy-to-use technology solutions that help people grow, manage, and secure their digital and financial lives. Dual headquartered in Prague, Czech Republic and Tempe, Arizona, Gen is a global company dedicated to powering Digital Freedom through its trusted brands including Norton, Avast, LifeLock, MoneyLion and more.

Our family of consumer brands is rooted in providing financial empowerment and cybersafety for the first digital generations. Today, Gen empowers people to live their digital lives safely, privately and confidently for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy, identity protection and financial wellness to nearly 500 million users in more than 150 countries. This scale gives us unparalleled, real-time data on the evolving threat landscape and positions our solutions as a critical preventive layer in the fight against cross-platform online scams.

If you want more information, please contact:

Kim Allman
Head of Corporate Responsibility
& Government Affairs
Kim.Allman@GenDigital.com
Transparency Register n° 083146048556-68

[1] All data is sourced from the Global Scam Alliance report, of which Gen is a member. Additional information can be found in the global report or in the country-specific reports for Germany, France and Denmark.
[2] For more information and examples, check Gen Digital's latest threat reports (Q1/2025, Q4/2024)
[3] EU Serious and Organised Crime Threat Assessment (EU-SOCTA) | Europol

United States: 60 E Rio Salado Pkwy STE 1000 Tempe, AZ 85203
Czech Republic: Enterprise Office Center Pikrtova 1737/1A 140 00 Prague 4