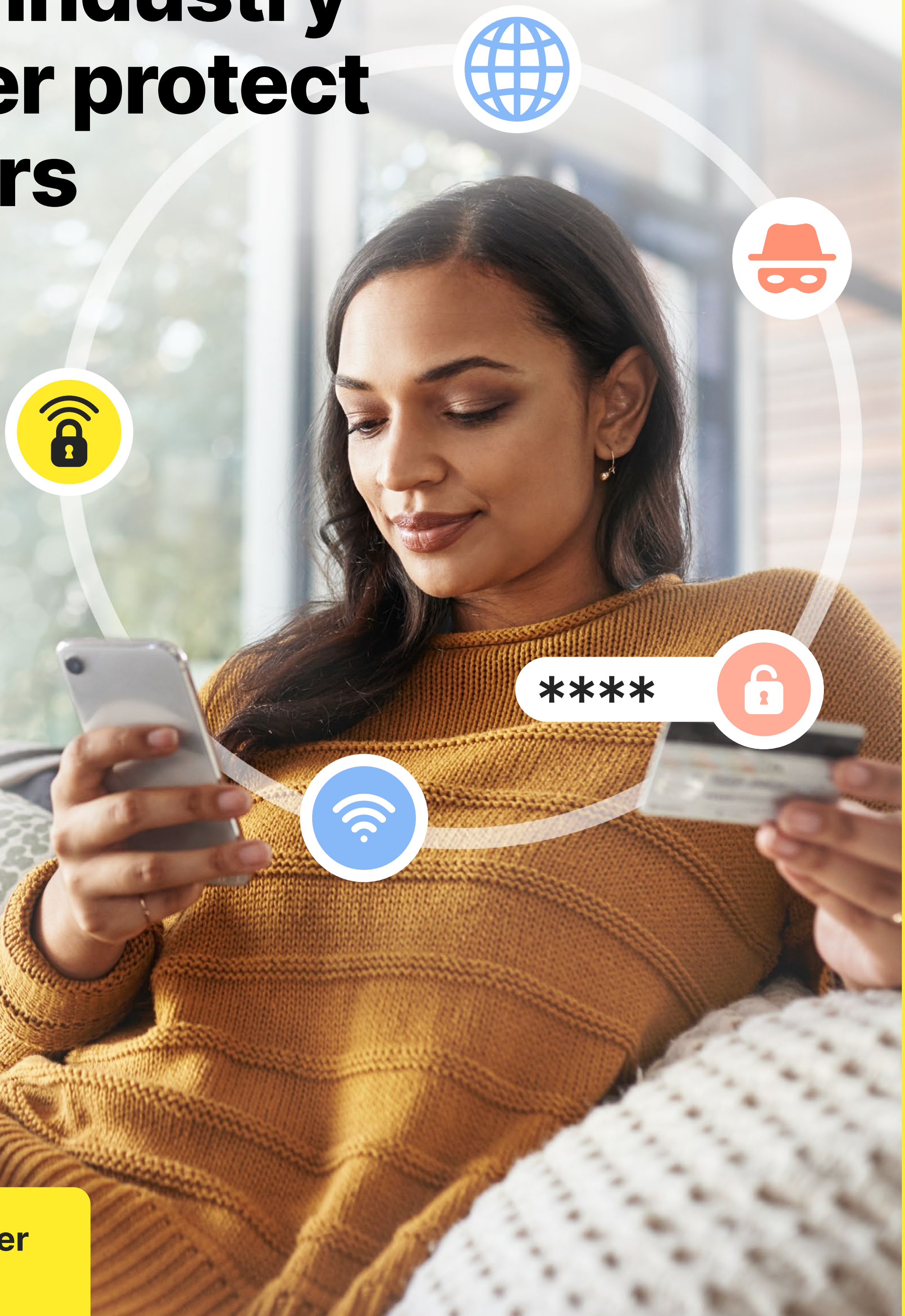
norton™

How the financial services industry can better protect customers

Learn why your portfolio should offer solutions that safeguard customers from online fraud and scams.



norton.com/partner

Digital threats are increasing: your customers' financial assets could be at risk

Many consumers are at risk of being impacted by cybercrime. The financial services industry has a tremendous opportunity to incorporate Cyber Safety tools and services into product portfolios to help protect their customers from digital scams, fraud, and online threats. Offering services that help protect businesses, privacy, family, and identity can also help to enhance customer satisfaction and engagement.

Cybercrime is on the rise

€7.5 trillion
The estimated annual cost of cybercrime worldwide in 2023[1]

70%
The expected growth of cybercrime by 2028[1]

€1.4 billion
The cost of fraud and scams to the UK financial services industry[2]

The impact is felt by you, and your customers

1 in 2
Victims across 8 countries were impacted financially[3]

€1500
The average loss by consumers due to scams in Germany and France[4]

76%
Of scams and fraud happen online[2]

€148 billion
The annual cost of rising cybercrime on Germany's economy[5]

€330,000
The average insurance claim amount for a ransomware attack[6]

85%
of individuals surveyed believe financial institutions should offer cybersecurity solutions to their customers[7]

The scale of online scams and fraud

How the financial services industry pays the price.

In 2023, one in two consumers lost money to scammers, with the typical loss in Europe exceeding €1000 per victim.[4] And that same year in the US, people lost $10 billion[8] to scams. Throughout the UK, losses from fraud were £1.2 billion[2], representing 40% of all crimes reported. Even some of the best performing European countries (e.g., Netherlands) lost 0.18% of GDP to fraud, money that is not easily recoverable.

However, consumers don't always lose out financially

Because cybercrime losses are often refunded to the consumer, society and governments are increasingly expecting the financial services industry to help protect them from the fraud and scams that have resulted in authorised payments to cybercriminals.

"The best way to tackle fraud is to stop it happening in the first place, and our collective efforts should focus on that.

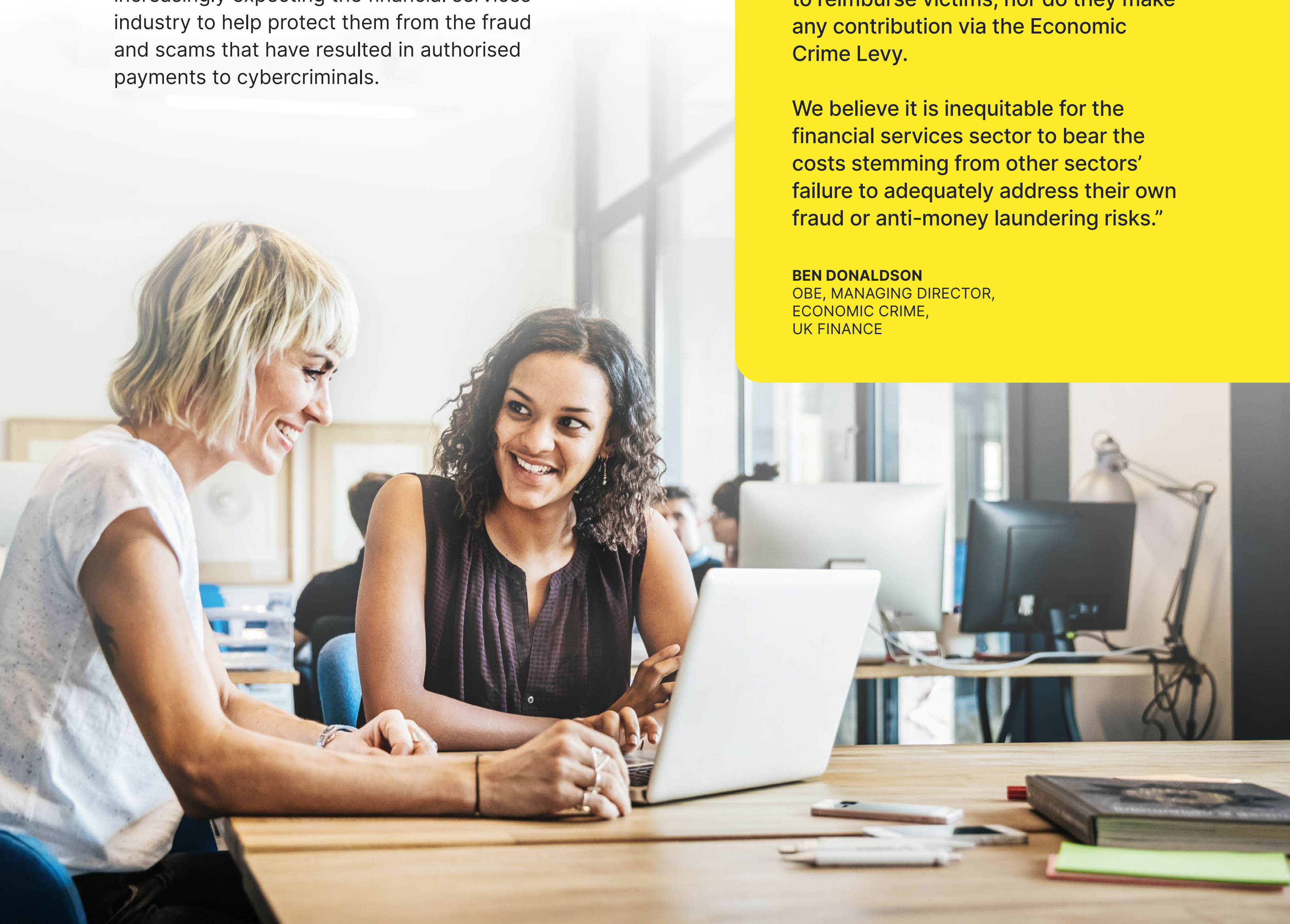
We have long called for other sectors to step up and stop the criminal activity that is proliferating on their platforms, sites, and networks.

In 2023, 76% of authorised push payment fraud cases originated from online sources, and a further 16% from telecommunications.

Despite this, these sectors do not have to reimburse victims, nor do they make any contribution via the Economic Crime Levy.

We believe it is inequitable for the financial services sector to bear the costs stemming from other sectors' failure to adequately address their own fraud or anti-money laundering risks."

BEN DONALDSON
OBE, MANAGING DIRECTOR,
ECONOMIC CRIME,
UK FINANCE



Social engineering

Social engineering lies at the heart of many types of fraud and scams, including ransomware, phishing, and identity theft. Many cybercriminals are experts in the art of human manipulation. They use socially engineered attacks to deceive people into sending money or allowing the criminal to take over their accounts. It is often highly sophisticated, manipulative, and, in the case of romance scams, cruel.

Ransomware

Ransomware is recognised as one of the costliest cyberthreats by the financial service industry. In 2023, Germany reported more than €1 billion of ransomware payments.[9] And this threat spans many sectors: in fact, Munich Re identified that manufacturing, business & professional services, retail, and healthcare were the leading industries for ransomware claims, exceeding 60% of claims combined.[10]

How does ransomware work? It's a type of malware that's downloaded onto a vulnerable PC or Mac. It then encrypts data on the device and presents a ransom demand to the user. But paying the ransom doesn't guarantee the data will be recovered from the infected device — the data may be lost forever and is sometimes stolen by the cybercriminal and resold on the dark web. Becoming a victim of ransomware can be inconvenient and emotionally distressing for a consumer, but for a company, it can literally put them out of business.

The UK insurance industry estimates that a ransomware attack will typically cost a small and medium-sized enterprise (SME) between £25,000 and £100,000.[11] Because they often lack cybersecurity expertise, very small businesses are particularly vulnerable to ransomware attacks.

Dark Web Monitoring

It's estimated that there are tens of thousands of active dark web websites, including thousands of forums and marketplaces, selling everything from stolen credit card details to drugs and weapons.

Email and password combinations from breached companies are often openly sold on the dark web. Credit card numbers (with CVC data) can be sold for as little as a few tens of Euros.[12] Apart from preventing this information from being stolen in the first place, consumers and businesses alike should use Dark Web Monitoring to find out if their data is being traded on the dark web, so they can be aware of the breach and take action to help protect themselves.

Phishing

Phishing uses social engineering to trick victims into revealing private data such as credit card or bank account details. Often received in an SMS, WhatsApp, or email, the message conveys a sense of financial urgency or authority. This leads the victim to click on a link that takes them to a malicious website, drawing them into a world of deceit where they are prompted to enter key personal information such as full credit card numbers, bank account details, home address, and driving license. Quite often, cybercriminals use that personal information to commit fraud, and then sell it on the Dark Web.

Once compromised, the stolen information may be used to commit unauthorised payment fraud, but ultimately the financial services industry takes the responsibility to compensate the victim.

Identity theft

Identity fraud, or 'ID theft', involves the use of stolen personal details to commit fraud or enable scams. Personal details such as home address, bank account details, credit card numbers, passport, and driving license information are traded between cybercriminals on the Dark Web. Once fraud is committed using stolen personal details, it can be incredibly costly and stressful for the victim to clean up the mess left behind by the cybercriminal, and often the bank or the insurer ends up compensating the victim.

Privacy

Encouraging customers to install a dedicated private browser (or adding a safe browser extension to an existing browser) can help stop online attacks. These tools can alert the user to potentially risky websites and block access to sites that are used for phishing, hosting malware, or downloading ransomware. Although cybercriminals often use social engineering techniques to encourage their victims to enter their personal information on compromised websites, private browsers and safe browser extensions add a very effective layer of protection to help prevent many types of online scams and fraud.

Other tools can also enhance privacy and reduce the risk of data theft. For example, Virtual Private Networks (VPNs) can help customers secure their communications on a public WiFi network. Another tool is a password manager, which enables users to create a unique, complex password for each site visited, reducing the impact of a data breach.

Identity Restoration

No security software can guarantee protection. Even the most secure companies can be breached and lose their customers' data to cybercriminals. When customers become aware that their personal data has been compromised, they will look for support and advice, and this is where Identity Restoration services can help.

Although the role may vary by country, the role of an identity restoration specialist is to provide guidance to customers to help them resolve their identity theft issues. This will include helping customers contact and resolve the issue with relevant parties such as merchants, credit card companies, financial institutions, collection agencies, and government agencies.

Alongside the preventative nature of cybersecurity and the after-event financial support provided by a cyber insurance policy, identity restoration can help support customers as they deal with fraud or scams that have resulted in identity compromise.

Creating a strategy to help protect customers

The financial service industry understands the importance of protecting customers against fraud and scams.

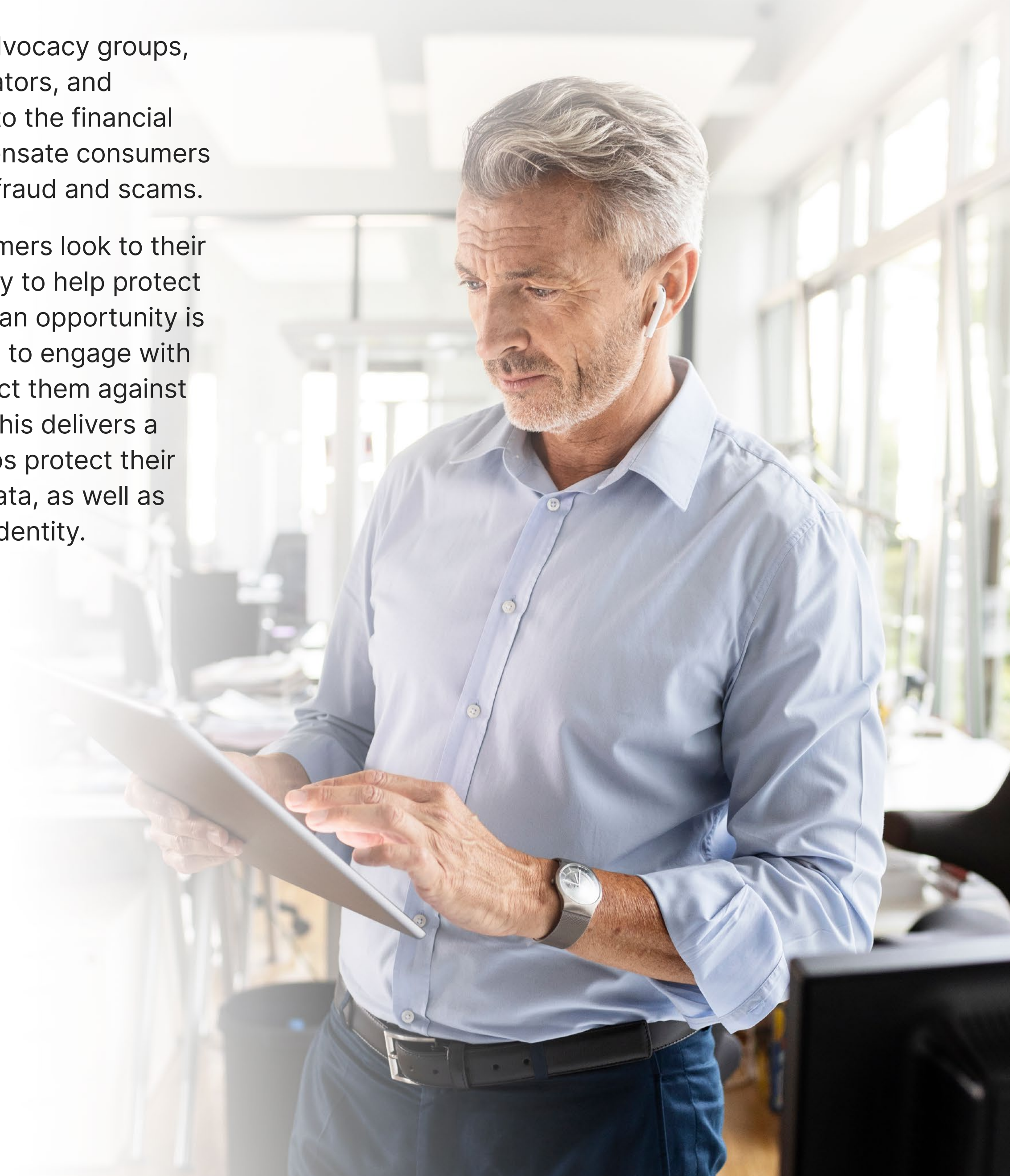
But despite investing in advanced security systems, meeting complex regulations on money laundering, implementing identity verification and transaction security, their customers continue to lose money to cybercriminals.

Increasingly, consumer advocacy groups, the media, financial regulators, and governments are looking to the financial service industry to compensate consumers who lose money through fraud and scams.

And because many customers look to their financial services company to help protect them from online threats, an opportunity is created for that company: to engage with customers and help protect them against online fraud and scams. This delivers a scalable solution that helps protect their customer's devices and data, as well as their privacy, family, and identity.

Three ways to help safeguard customers against digital threats

1. **Offer a personal cybersecurity product** as part of your services.
2. **Support customer knowledge** of digital threat landscape by adding educational content into outreach communications.
3. **Partner with a leader** in cybersecurity that can deliver the device, privacy, and identity protection customers need.



Why partner with us

Partnering with Norton offers a valuable opportunity to leverage our expertise and comprehensive cybersecurity and identity solutions, helping provide robust protection and peace of mind against evolving digital threats.

Our in-country partner specialists already work with many of the leading consumer-facing brands in Europe. As a global leader in cybersecurity, we design solutions that meet the needs of our partners, and help educate and help protect the customer, whether they are a consumer or a small business.

How we help you protect your most valuable assets: your customers

Financial services companies that leverage our solutions can deliver more for customers, including:

- Help desk and restoration services
- Identity protection tools
- AI-enhanced financial health monitoring and alerts
- Online privacy
- Protection against online scams and fraud

Increasing value and engagement with the customer

About Norton

Your customers are your most valuable assets; helping protect them is our priority. Stay one step ahead of cybercriminals and the competition by offering solutions to help protect their digital lives.

With four decades of experience in consumer cybersecurity, we have earned the trust of over 500 million users through our award-winning products and member services.

Our high brand awareness, combined with award-winning products and services, perfectly positions us to help you develop a new innovative portfolio.

Strong brand recognition and proven experience

Offering one of the most comprehensive protection solutions on the market solidifies your commitment to helping protect your customers' assets.

AV-TEST, "Best Protection 2022 Award" for Norton 360, January-December 2022.

Tom's Guide - Best Antivirus Software 2022

A trademark of Ziff Davis, LLC. Used under license; Reprinted with permission. © 2021 Ziff Davis, LLC. All Rights Reserved.

Help provide peace of mind with our robust cybersecurity solutions

- Norton 360 Advanced
- Norton AntiTrack
- Norton Private Browser
- Norton Security Ultra

Innovation

Norton Labs is a global team dedicated to researching emerging digital threats. These insights feed into our product development and engineering to help protect our members. We have more than 1,000 patents, including our proprietary technology that scans for identity threats.

Norton technology blocks millions of cyberthreats every day

✓ **2.7 billion** cyberthreats blocked in 2023

✓ **219 million phishing and scam threats** blocked in 2023

✓ **5,100 attacks blocked** per minute in 2023

✓ **1.4 million** malware attacks on mobile devices blocked in 2023

Visit us at www.Norton.com/partner

Gen™

norton™ Avast™ LifeLock™ by norton Avira™

AVG REPUTATION DEFENDER™ by norton CCleaner

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

Gen is a global company with a family of trusted consumer brands and has one of the world's largest consumer Cyber Safety networks, protecting people around the globe against advanced online threats. We are committed to protecting Digital Freedom and the personal information of our nearly 500 million users in more than 150 countries.

[1] Statista
[2] UK Finance Annual Fraud Report
[3] Based on an online survey of 8022 adults in 8 countries, of which, 3,043 experienced cybercrime in the past 12 months. Conducted by The Harris Poll on behalf of Gen™ (formerly NortonLifeLock), November - December 2022.
[4] Global Anti-Scam Alliance Report: Global State of Scams 2023
[5] Euronews
[6] Coalition
[7] Based on an online survey of 7,080 adults in 7 countries conducted by Dynata on behalf of Gen from June 29th to July 10th, 2023
[8] FTC
[9] BKA
[10] Munich RE
[11] Association of British Insurers
[12] Privacy Affairs

No one can prevent all cybercrime or identity theft.

norton™