Internet Safety Statistics Launches Comprehensive UK Cyber Safety Resource as AI-Powered Threats Surge 87% Worldwide

New online platform provides evidence-based protection guidance for families, schools, and businesses amid escalating digital dangers

How To Stay Safe Online Helping Business Owners

BELFAST, COUNTY ANTRIM, UNITED KINGDOM, January 2, 2026 /EINPresswire.com/ -- Internet Safety Statistics (internetsafetystatistics.com) has launched as a dedicated cyber safety education platform, delivering practical protection resources to UK families, schools, and businesses facing an unprecedented wave of digital threats. The launch comes as government data confirms 43% of UK businesses experienced cyber breaches in 2024 and new research reveals 87% of organisations worldwide have encountered AI-powered attacks in the past year alone.

> The cyber threats facing UK families, schools, and businesses in 2025 bear almost no resemblance to the dangers we warned about even five years ago. AI has fundamentally changed the attack surface."
>
> *Ciaran Connolly, Founder Internet Safety Statistics*

The platform arrives at a critical moment in UK digital safety. The Online Safety Act's child protection codes came into force on 25 July 2025, creating new legal requirements for platforms to shield young users from harmful content. Yet with one in three children experiencing cyberbullying and 70% of teenagers sharing personal information online without understanding the consequences, the need for accessible, independent safety education has never been more urgent.

Addressing the AI-Driven Threat Escalation

Traditional online dangers have transformed dramatically with the rise of artificial intelligence. Phishing attacks powered by AI tools have become virtually indistinguishable from legitimate communications, with research showing these AI-generated scams now achieve a 72% open rate—nearly double that of traditional phishing attempts. Voice

cloning technology enables criminals to impersonate family members convincingly using just seconds of audio captured from social media.

The platform tackles these emerging threats head-on, providing practical guidance that moves beyond outdated "stranger danger" approaches to address the sophisticated psychological manipulation techniques now targeting UK users.

"What concerns us most is the widening gap between how quickly threats are evolving and how slowly awareness is spreading," said Ciaran Connolly, founder of Internet Safety Statistics. "Parents are trying to protect their children with advice that's already years out of date. A teenager today faces AI-generated deepfakes, sextortion scams, and phishing attacks so convincing that even cybersecurity professionals struggle to identify them. Our platform exists to close that knowledge gap with actionable, up-to-date guidance that families can actually use."

Internet Safety Statistics - Start Safe Online

Internet Safety Statistics - Start Safe Online for Business Owners

UK Cybercrime Reality: The Numbers Behind the Headlines
The scale of cyber threats facing UK users is staggering. Recent government surveys reveal approximately 612,000 UK businesses and 61,000 charities identified cyber breaches or attacks in the past year. The total cost of cybercrime to the UK economy stands at an estimated £27 billion annually, with the average cost to businesses reaching £10,830 per incident.

For small and medium enterprises, the picture is particularly concerning. SMEs represent 99.9% of UK businesses yet account for 81% of successful cyberattack victims. Many lack dedicated IT security resources, leaving them vulnerable to sophisticated threats that were once reserved for larger targets.

The 2025 Cyber Security Breaches Survey found phishing remained the dominant attack method, affecting 85% of businesses that reported breaches. Ransomware attacks against UK businesses

doubled from under 0.5% in 2024 to 1% in 2025, affecting approximately 19,000 organisations.

Children at the Digital Frontline

Young people face particular vulnerability in the current threat environment. Research from the Children's Commissioner for England shows the average age at which UK children first encounter explicit material online is 13, with one in ten exposed as early as age nine.

Beyond inappropriate content, children now contend with sophisticated manipulation techniques. Schools report that 60% of secondary schools experienced cyber breaches in the past year, with nearly 20% suffering system misuse. The psychological impact extends far beyond immediate incidents—students experiencing cyberbullying show decreased academic performance, increased absenteeism, and long-term mental health challenges.

The emergence of deepfake technology has created entirely new categories of harm. Students are using these tools to create harassing and sexually explicit content of classmates and teachers, presenting challenges that existing cyberbullying policies were never designed to address.

Internet Safety Statistics provides age-appropriate resources that help parents and educators have informed conversations about these risks. The platform offers practical guidance on parental controls, privacy settings, and recognition of manipulation tactics—equipping families with the knowledge to create safer digital environments.

Supporting Schools Through Regulatory Change

The Online Safety Act has placed new responsibilities on educational institutions to protect students online. Schools must now address not only inappropriate content but also cyberbullying, hateful content, and material encouraging self-harm or eating disorders.

Keeping Children Safe in Education (KCSIE) guidelines and Ofsted inspection criteria increasingly emphasise digital safety. Yet many schools lack the resources to develop comprehensive cyber safety programmes while managing their existing safeguarding responsibilities.

The platform provides educators with practical resources that complement statutory requirements. From age-specific lesson frameworks to guidance on recognising signs of online harm, Internet Safety Statistics supports schools in meeting their obligations while genuinely protecting student wellbeing.

Practical Business Protection in an AI Era

The financial impact of cyber incidents extends well beyond immediate costs. Only 22% of UK businesses have a formal cybersecurity incident management plan in place, and just 31% of businesses undertook a cyber security risk assessment in 2024.

For smaller organisations, this lack of preparation creates existential risk. The average recovery

time from a significant cyberattack for SMEs is 23 days, compared to 16 days for larger enterprises with dedicated security teams. Many businesses never fully recover.

Internet Safety Statistics delivers practical guidance tailored to organisations without dedicated security staff. The platform covers everything from firewall configuration and network protection to staff awareness training and incident response planning—making enterprise-level security knowledge accessible to businesses of all sizes.

Combating Emerging AI Threats

The platform places particular emphasis on AI-powered threats that traditional safety resources fail to address. Deepfake incidents increased by 19% in the first quarter of 2025 alone compared to all of 2024. An estimated 8 million deepfake files will be shared online in 2025, with the volume growing at approximately 900% annually.

Voice cloning presents specific dangers for families. UK police report a 150% increase in cases involving fake audio content, often used in emergency scams targeting parents and grandparents. Criminals can now create convincing voice replicas using just minutes of audio harvested from social media posts.

The platform provides recognition guidance for synthetic media, verification protocols for unexpected requests, and family communication strategies that establish authentication processes before emergencies occur.

Free, Independent, Evidence-Based

Unlike many commercial cybersecurity platforms, Internet Safety Statistics operates as an independent educational resource. Content is developed using verified data from government sources, academic research, and recognised cybersecurity organisations.

The platform regularly updates its resources to reflect evolving threats and regulatory changes. As AI capabilities advance and new attack vectors emerge, Internet Safety Statistics commits to providing current, relevant guidance that keeps pace with the threat landscape.

About Internet Safety Statistics

Internet Safety Statistics (internetsafetystatistics.com) is a cyber safety education platform providing practical protection resources for UK families, schools, and businesses. The platform delivers evidence-based guidance on internet safety, cyberbullying prevention, privacy protection, and threat awareness. Resources are freely accessible and regularly updated to address emerging digital dangers.

Frequently Asked Questions

What makes Internet Safety Statistics different from other cyber safety resources?

The platform focuses on practical, actionable guidance rather than general warnings. Content addresses specific emerging threats including AI-generated phishing, deepfake scams, and voice

cloning attacks that many traditional resources overlook. All guidance uses UK-specific context, referencing relevant legislation like the Online Safety Act and GDPR requirements, and connects users with appropriate UK support services and reporting mechanisms.

How does the platform help parents protect children online?
Internet Safety Statistics provides age-appropriate resources covering everything from parental control setup to conversation guides for discussing online risks with children. The platform addresses current threats facing young people—including sextortion, cyberbullying, and inappropriate content exposure—with practical recognition techniques and response strategies parents can implement immediately.

What resources are available for UK schools?
Educators can access guidance aligned with Keeping Children Safe in Education requirements and Online Safety Act obligations. Resources include age-specific lesson frameworks, signs of online harm recognition, and incident response protocols. The platform supports schools in meeting statutory safeguarding duties while building genuine digital resilience among students.

How can businesses use the platform to improve cyber security?
Small and medium enterprises can access practical security guidance covering firewall configuration, staff awareness training, and incident response planning. Resources are designed for organisations without dedicated IT security teams, making professional-grade protection knowledge accessible to businesses of all sizes. The platform also covers compliance requirements under UK data protection legislation.

Is the information on Internet Safety Statistics regularly updated?
Yes. The cyber threat landscape evolves rapidly, and outdated advice can create dangerous false confidence. The platform commits to regular content updates reflecting new attack methods, regulatory changes, and emerging protection technologies. All statistics and recommendations are sourced from verified government data, academic research, and recognised cybersecurity authorities.

How can I tell if a message or email is an AI-generated phishing attempt?
AI-generated phishing has eliminated many traditional warning signs like spelling errors and awkward phrasing. Instead, look for urgency tactics pressuring immediate action, requests to bypass normal verification procedures, and links that don't match the sender's claimed organisation when you hover over them. Legitimate organisations rarely request sensitive information via email or threaten account closure without prior notice. When uncertain, contact the organisation directly using contact details from their official website—never use phone numbers or links provided in the suspicious message itself.

What should parents know about deepfakes and their children?
Deepfake technology allows anyone to create convincing fake videos or audio of real people. Children face two distinct risks: becoming victims of deepfake harassment where their likeness is

manipulated into inappropriate content, and being deceived by deepfakes impersonating trusted figures. Parents should discuss with children that video and audio can now be fabricated, establish family verification phrases for emergency situations, and encourage children to report any manipulated images of themselves or classmates immediately. Schools should update cyberbullying policies to explicitly address synthetic media creation and distribution.

What are the most common cyber threats facing UK small businesses?
Phishing attacks remain the dominant threat, affecting 85% of businesses that reported breaches in 2024. Business email compromise—where attackers impersonate executives or suppliers to request fraudulent payments—cost UK organisations £135 million last year. Ransomware attacks doubled in prevalence during 2025, now affecting approximately 19,000 UK businesses. Supply chain attacks, where criminals compromise a trusted vendor to access their customers, increased by 35%. Small businesses are particularly vulnerable because attackers view them as softer targets with valuable data but limited security infrastructure.

How do I set up effective parental controls without damaging trust with my child?
Effective digital safety combines technical controls with open communication. Start by explaining why protections exist—frame them as safety measures rather than surveillance. Age-appropriate controls should become less restrictive as children demonstrate responsible behaviour and develop critical thinking skills. Involve teenagers in discussions about which protections make sense for their age and maturity level. Focus on teaching recognition skills alongside technical restrictions—children who understand manipulation tactics make better decisions even when parental controls aren't present. Regular conversations about online experiences build trust and encourage children to report concerns.

What steps should I take immediately if I think I've been targeted by a cyber attack?
First, avoid clicking any links or downloading attachments in suspicious messages. If you've already clicked a link or provided information, change passwords immediately for any potentially affected accounts—starting with email and banking. Enable two-factor authentication where available. Run antivirus scans on your devices. Monitor bank statements and credit reports for unusual activity. Report the incident to Action Fraud (the UK's national fraud and cybercrime reporting centre) and notify your bank if financial information was compromised. For businesses, follow your incident response plan and consider whether the breach triggers notification requirements under data protection legislation.

How often should businesses conduct cyber security training for staff?
Annual training alone is insufficient given how rapidly threats evolve. Best practice combines formal annual training with regular micro-learning throughout the year—brief updates on new scam types, simulated phishing exercises, and seasonal reminders around high-risk periods. The 2025 Cyber Security Breaches Survey found that only 31% of UK businesses undertook any cyber security risk assessment in 2024, and staff awareness represents one of the most cost-effective security investments for small organisations. Training should cover current threats like AI-generated phishing and deepfake impersonation, not just traditional attack methods.

Ciaran Connolly
InternetSafetyStatistics
email us here
Visit us on social media:
LinkedIn
Bluesky
Instagram
Facebook
YouTube
TikTok
X
Other
