20 years ECC-Net
Help and advice for consumers in Europe
European Consumer Centre Malta

ECC MALTA NEWS

ISSUE 01

We are pleased to share with you the first edition of our 2025 newsletter, which focuses on the various types of scams that consumers may encounter. In this edition, we begin with an article highlighting emerging scam trends affecting both consumers and businesses. This is followed by an overview of the different types of scams currently circulating, to help raise awareness and promote vigilance. We also feature an article dedicated to the ECC Network's recent position paper on the car rental sector, outlining the need for stronger consumer protection measures. Finally, we share a success story related to flight compensation, showcasing how consumer rights can be effectively enforced. As always, we value your feedback and look forward to continuing to support you in making informed and confident decisions as consumers.

Scams in 2025: How Artificial Intelligence is Changing the Game

Scams are nothing new, but in 2025, they look very different from the lottery-win emails of the past. With the rise of **artificial intelligence (AI)**, fraudsters are now able to craft **highly realistic messages, voices, and even videos** that convincingly imitate trusted sources to deceive people into revealing sensitive information or sending money.

This article aims to raise awareness of how scams have evolved in today's hyper-connected world. Modern scams are **sophisticated, targeted, and widespread**, designed to manipulate trust, exploit human vulnerabilities, and cause both financial and emotional harm.

A recent local newspaper podcast highlighted the scale of the problem. During this podcast, a representative from a major bank revealed that nearly **€3 million was lost to fraud**, while an additional **€2 million in attempted scams was successfully prevented**. In total, **€5 million** was targeted in just one year, from businesses and customers of a single bank. The true national impact is likely to be even greater, considering the presence of other banks operating in Malta that may have encountered similar incidents.

The Role of AI in Modern Scams

AI is a powerful tool, but like any technology, it can be misused. One of the most concerning trends is the rise of **deepfakes**. Deepfakes are when scammers use synthetic audio or video that convincingly imitates a person's face, voice, or mannerisms. With just a few seconds of publicly available material from a video, voicemail, or social media post, scammers can generate realistic clips or voice recordings. These tools are now inexpensive and widely accessible, making it easier for fraudsters to impersonate friends, family members, or officials, making it harder for victims to notice if it's real.

How to Protect Yourself

As AI tools become more advanced, the line between real and fake content blurs. Protecting yourself requires caution, verification, and secure online habits:

- **Verify Sources and Links -** Before interacting with online content, check the source carefully. When shopping, visit the official website directly instead of clicking on links in social media ads or promotional emails. On social media, verify accounts by checking for verification badges, reviewing post history, or contacting the company through official channels.
- **Be Sceptical of "Too-Good-to-Be-True" Offers -** Adverts, messages, or emails promising huge discounts, free products, or guaranteed profits are common traps. Examine website domains for spelling errors, unusual endings, or extra words. Avoid any offer that requests untraceable payment methods like gift cards, wire transfers, or cryptocurrency.
- **Strengthen Account Security -** Use strong, unique passwords for every account and enable multi-factor authentication. Even if a scammer gains access to one account, the multi-factor authentication can prevent them from compromising others.

Co-funded by the European Union

- **Limit What You Share Online -** Scammers often use public information to create realistic impersonations. Be selective about what you post, such as your birthday, address, or workplace, and adjust privacy settings to restrict visibility to trusted contacts only.
- **Keep Devices and Software Updated -** Install updates regularly and use security tools such as antivirus software, phishing detection browser extensions, and ad-blockers. These will help prevent exposure to malware or malicious websites.
- **Learn to Recognise AI-Generated Content -** Familiarise yourself with the signs of AI manipulation, such as unnatural voice tones, distorted visuals, or inconsistencies in messages. Awareness can help you spot deepfakes before they cause harm.
- **Confirm Suspicious Requests -** If you receive an unusual message, verify it through an independent channel. Contact the person or company directly using official contact details before taking any action. Reporting suspicious adverts, websites, or messages to the platform or relevant authorities helps protect others, too.

Common AI-Enhanced Scams in 2025

AI technology is now used to make traditional scams more convincing, including:

1. **Phishing** – Fraudulent emails, texts, or calls impersonating trusted sources.
2. **Online Shopping Scams** – Fake websites and counterfeit products.
3. **Impersonation Scams** – Fraudsters posing as banks, officials, or acquaintances.
4. **Investment & Financial Scams** – Ponzi schemes, fake platforms, cryptocurrency fraud.
5. **Tech Support Scams** – Attackers claiming to fix non-existent computer issues.
6. **Romance Scams** – Emotional manipulation on dating platforms to solicit money.
7. **Work-from-Home Scams** – Fake job offers leading to identity theft or financial loss.

Stay Smart. Stay Safe.

AI is transforming how scams operate. Awareness and caution remain the best protection. Always verify information, think twice before sharing personal details, and maintain strong online security habits. By staying alert, you can navigate the increasingly AI-driven digital world safely and confidently.

Types of Scams: Stay Alert and Protect Yourself

Phishing Scams - Phishing scams involve fraudulent communications that appear to come from trusted sources, such as banks, companies, government agencies, or colleagues. The goal is to steal sensitive information like passwords, credit card numbers, or personal details. Common forms include:

- Emails – Fake emails urging recipients to click on malicious links or download harmful attachments.
- Texts (Smishing) – SMS messages directing users to fake websites or prompting replies with sensitive information.
- Phone Calls (Vishing) – Impersonation of trusted institutions to extract personal or financial information.
- Websites – Fake sites designed to mimic legitimate ones, tricking users into sharing login credentials or payment details.

Online Shopping Scams -These scams exploit consumers with fake products, deals, or services online. Examples include:

- Fake Websites – Sites imitating well-known brands offering deals that are "too good to be true."
- Counterfeit Products – Advertised luxury items delivered as low-quality or fake goods.
- Non-Delivery Scams – Sellers disappear after payment or provide false tracking information.
- Social Media Ads – Fake ads promoting bogus stores or products.
- Payment Fraud – Requests for wire transfers, cryptocurrency, or other untraceable payment methods.

Impersonation Scams - Fraudsters pose as trusted individuals or organisations to steal information or money. These often rely on urgency or fear:

- Tax Calls – Threats of arrest unless alleged back taxes are paid immediately.
- Bank Alerts – Fake notifications requesting account details.
- Social Media Hacking – Compromised accounts soliciting money from friends or followers.
- Charity Scams – Fraudsters posing as charities, especially during crises, to collect fake donations.

Investment and Financial Scams - These target those seeking quick financial gains:

- Ponzi and Pyramid Schemes – Promises of high returns funded by new investors.
- Cryptocurrency Scams – Fake coins, trading platforms, or guaranteed-profit schemes.
- Fake Investment Platforms – Fraudulent websites or apps mimicking legitimate trading platforms.
- Boiler Room Scams – Aggressive calls or emails selling worthless shares.
- Forex, Binary Options & Fake IPOs – Manipulated platforms offering unrealistic returns or discounted shares.

Lottery and Prize Scams - Victims are falsely told they've won a prize or lottery. Scammers create urgency to extract money or personal details. Social media "friends" may also be fake accounts seeking money.

Tech Support Scams- Scammers pose as tech support, claiming a device is infected. They may demand payment for fake repairs, install malware to steal data, or fabricate issues to pressure payment.

Romance Scams - Fraudsters build trust on dating sites or social media, then create fake emergencies (medical bills, travel costs, family crises) to solicit money.

Work-from-Home Scams - Scammers advertise remote jobs with high pay and minimal effort. Victims risk financial loss or identity theft after paying fees or sharing personal information.

Driving Change: Stronger Consumer Protection in the Car Rental Sector

This month, ECC-Net issued a position paper addressing the challenges facing the car rental sector. Although representing only 3–4% of complaints received by the Network, these complaints reveal persistent unfair practices, unclear responsibilities, and weak enforcement, demonstrating a structural imbalance in which businesses hold significant power over consumers. The complexity of multi-service bookings and problematic practices from intermediaries, tour operators, and rental companies have contributed to this imbalance, limiting consumer choice and options for redress.

While ECCs have engaged with the industry in recent years, cooperating on codes of conduct and promoting voluntary improvements, these efforts are inconsistently applied. In some cases, even sub-branches of companies publicly claiming to follow these codes fail to comply. As a result, ECC-Net concludes that binding regulation is the only viable next step to ensure consistent standards and fair treatment across the sector.

The paper proposes supplementing existing EU Directives, such as:

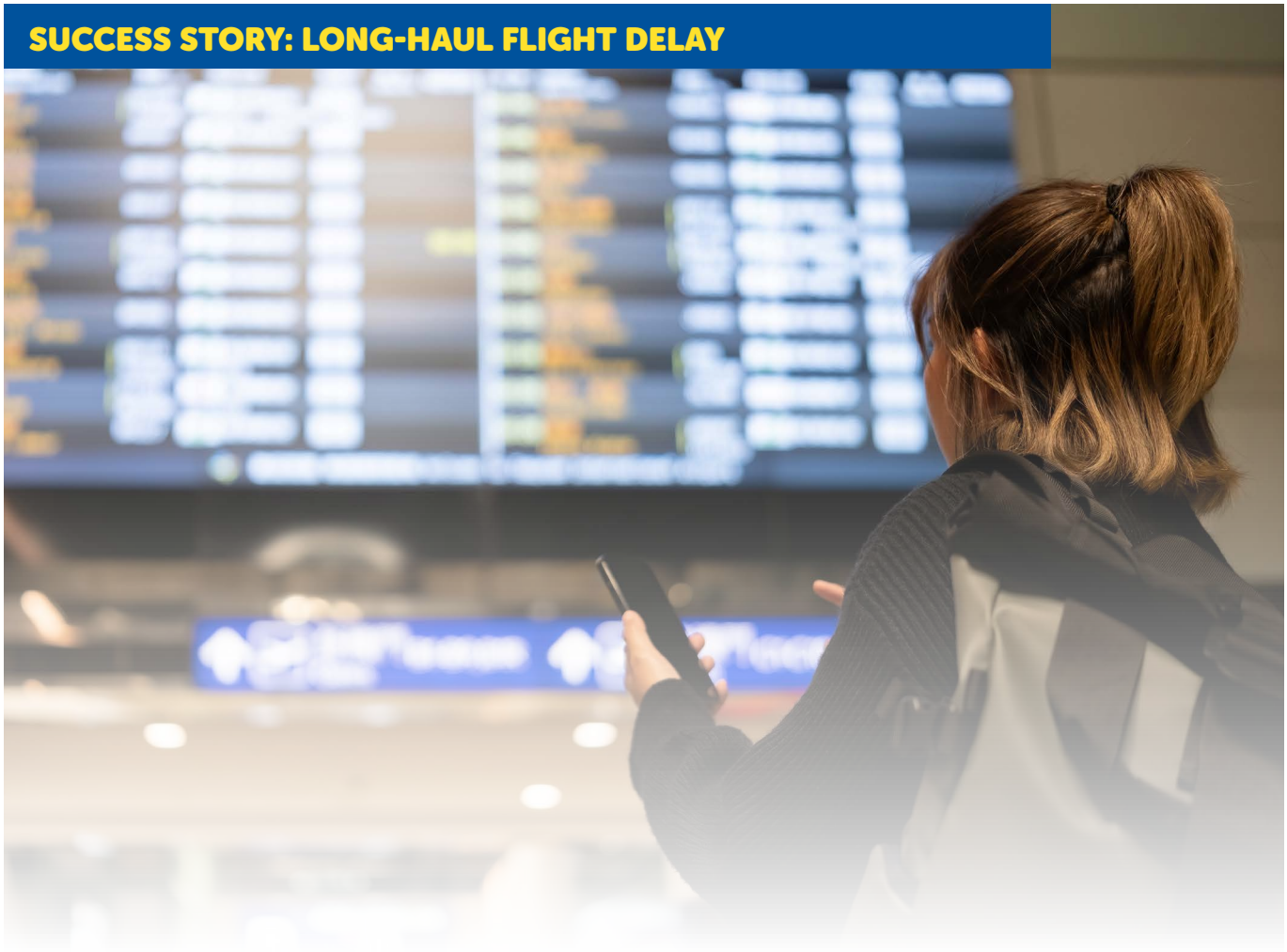
- **Directive 2011/83**: enhanced information requirements, including standardised product sheets, model contracts, clear insurance exclusions, and inspection protocols.
- **Directive 93/13**: prohibition of unfair contract clauses, such as excessive processing fees, refuelling costs, and cancellation charges.
- **Directive 2005/29**: preventing unfair commercial practices, including forced insurance add-ons.

Recommendations:
However, ECC-Net recommends a standalone legal framework for car rentals to provide a coherent set of rules tailored to the sector. Key measures include:

- Clear allocation of responsibility among involved companies, like the package travel directive.
- Allowing deposits via debit card instead of mandatory credit cards.
- Mandatory pre- and post-rental inspections in the consumer's presence.
- Recognition of existing insurance coverage from cards or household members.
- Detailed rules on insurance exclusions.
- Standardised handover procedures, multilingual checklists, and photographic documentation;
- Consumer rights to report preexisting damages within 24 hours, with rental companies bearing the burden of proof.

Implementing binding EU legislation would establish transparency, fairness, and consistent consumer protection across the sector, fostering trust and a more equitable marketplace for car rentals throughout Europe.

SUCCESS STORY: LONG-HAUL FLIGHT DELAY



In January 2025, a passenger faced a significant flight delay while travelling from the Dominican Republic to Poland. The flight was scheduled to depart at 17:30 and arrive the following morning at 08:30, but was delayed by approximately seven hours.

The passenger, who had booked the tickets through an intermediary, submitted a complaint requesting compensation of €600 per passenger, in line with EU passenger rights legislation for long-haul delays exceeding three hours. Despite repeated follow-ups, the airline ceased responding directly, providing only a single update in August 2025 stating that the case was "under review."

Frustrated by the lack of progress, the passenger turned to ECC Malta for assistance. The case was escalated through ECC channels, and the airline subsequently informed the consumer that the required compensation would be issued.

Thanks to ECC Malta's timely intervention, the passenger successfully received full compensation, bringing the case to a satisfactory close.

European Consumer Centre Malta

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Innovation Council and Small and Medium-sized Enterprises Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for them.