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

ECC MALTA NEWS

ISSUE 03

We are delighted to bring you the third edition of our newsletter, where we focus on the different types of scams that consumers may encounter. This article is packed with practical tips and advice to help you safeguard yourself and avoid potential mishaps. In this edition, we also share an inspiring success story about a consumer renting a car through a booking platform. Furthermore, we bring you the latest news from the European Commission, which is currently investigating two major companies following numerous complaints and inquiries submitted through the ECC network. We hope you find this edition both informative and engaging. As always, we welcome your feedback and look forward to supporting you in making informed decisions as consumers.

BEWARE OF SCAMS:
Protect Yourself from Deceptive Schemes

In an increasingly connected world, scams have become more sophisticated and widespread, targeting individuals and organisations alike. These deceptive schemes are carefully crafted to manipulate trust, exploit vulnerabilities, and steal money, personal information, or valuable assets. By targeting fear, greed, or ignorance, scammers succeed in causing financial loss and emotional distress to their victims.

As scammers continue to evolve their tactics in response to technological advancements and social trends, it is more critical than ever to stay vigilant and informed. This newsletter aims to shed light on the most common types of scams, how they operate, and what steps you can take to protect yourself and your loved ones. By understanding their methods, you can recognise the warning signs and avoid falling victim to these fraudulent schemes.

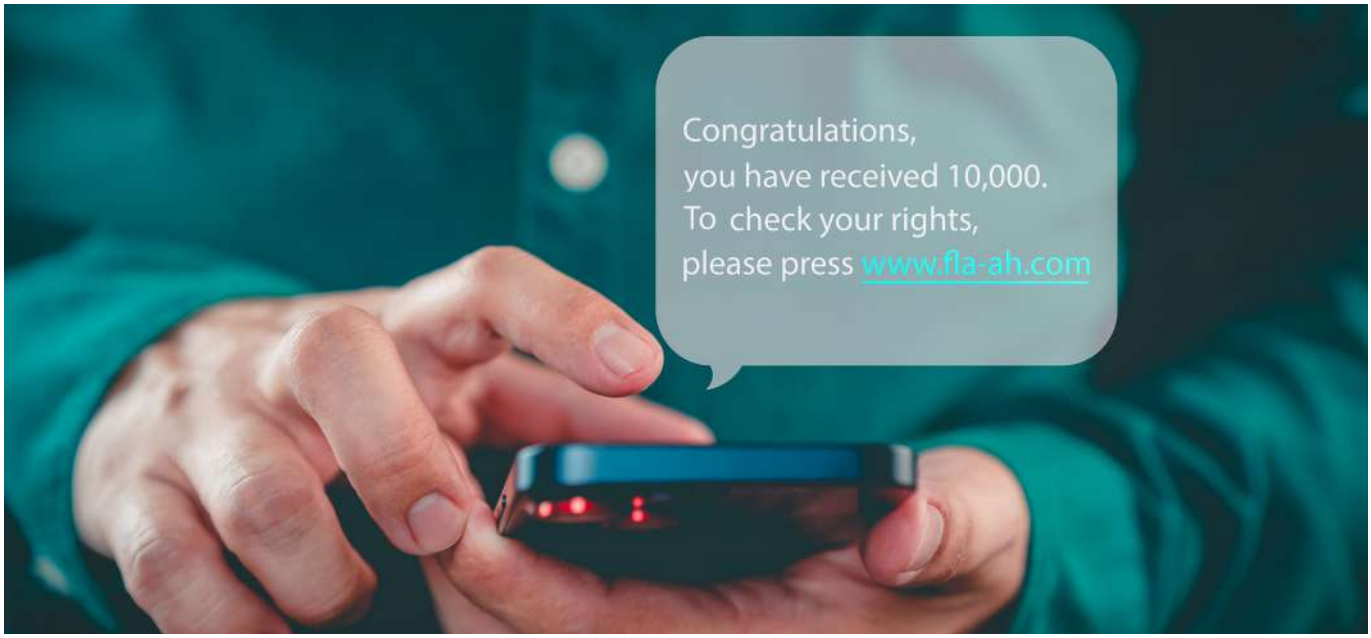
Knowledge is your best defence against scams - let's explore how to stay one step ahead.

Phishing Scams

Scammers typically achieve their aim through fraudulent communications that appear to come from trustworthy entities, such as banks, popular companies, government agencies, or colleagues. Their goal is to steal sensitive information like passwords, credit card numbers, or personal details. Phishing attacks often take the form of:

- **Emails:** Fraudulent emails imitate legitimate organisations, urging recipients to click on malicious links or download harmful attachments.
- **Texts (Smishing):** Similar schemes delivered via SMS, often directing users to fake websites, or prompting replies with sensitive information.

Co-funded by the European Union



- **Phone Calls (Vishing):** Attackers pose as representatives of trusted institutions to extract information over the phone.
- **Websites:** Fake websites copying legitimate ones, tricking users into entering credentials or financial details.

Online Shopping Scams

Online shopping scams are fraudulent schemes designed to exploit consumers by offering fake products, deals, or services on the internet. Common types of online shopping scams

- **Fake Websites:** Scammers create websites that copy well-known brands, offering deals that seem too good to be true.
- **Counterfeit Products**: Sellers advertise luxury or branded items at extraordinary prices but deliver fake or low-quality products.
- **Non-Delivery Scams:** After payment, the seller disappears or provides false tracking details.
- **Social Media Ads**: are the trend today whereby scammers use ads on social platforms to promote fake stores or products.
- **Payment Fraud:** Requests for wire transfers or untraceable payment methods.

Impersonation Scams

In this type of scam, scammers pose as trusted individuals or organisations to deceive victims into sharing personal information, sending money, or disclosing confidential information.

These scams exploit trust and often create a sense of urgency, fear, or authority to manipulate victims into compliance. Examples of such a scam can be:

- **Tax Calls:** Victims are told they owe back taxes and must pay immediately to avoid arrest.
- **Bank Alerts:** Scammers pretend to be bank representatives, warning of suspicious account activity and requesting account details.
- **Social Media Hacking:** Fraudsters use compromised accounts to ask friends or followers for emergency loans.
- **Charity Scams:** Impersonators pose as representatives of charities, especially during crises, to solicit fake donations.

Investment and financial scams

These are deceptive schemes designed to steal money from individuals by promising unrealistic returns or offering fraudulent opportunities. These scams exploit people's desire to grow their wealth quickly, often aiming at those unfamiliar with the complexities of investments or financial markets. Common Types of Investment and Financial Scams:

- **Ponzi Schemes:** Promises high returns with little or no risk, funded by money from new investors rather than legitimate profits. Collapses when there are no new investors to sustain payouts.
- **Pyramid Schemes:** Requires participants to recruit others into the scheme, earning profits from the recruitment rather than actual sales or services. Inevitably fails when recruitment slows.
- **Cryptocurrency Scams:** Scammers promote fake cryptocurrencies, trading platforms, or investment schemes. Victims are attracted by promises of guaranteed profits in the volatile cryptocurrency market.
- **Fake Investment Platforms:** Scammers set up websites or apps that mimic legitimate trading platforms. They disappear with victims' funds after convincing them to deposit money.
- **Boiler Room Scams:** Unsolicited calls or emails promote worthless or non-existent shares, often targeting inexperienced investors.
- **Forex and Binary Options Fraud:** Promises high returns through foreign exchange or binary options trading. Victims often lose their money due to manipulated trading outcomes or hidden terms.
- **Fake Initial Public Offerings (IPOs):** Scammers claim to offer pre-IPO shares at discounted rates, luring victims with the prospect of massive profits.

Lottery and prize scams

These are fraudulent schemes where scammers deceive victims into believing they have won a lottery, prize, or sweepstakes. The goal is to extract money or personal information by creating a false sense of excitement and urgency. These scams exploit people's hope of winning big, even if they never participated in a contest.

Consumers are getting used to this type of scam especially the ones received through email, however, as consumers, we must always keep an eye open when certain details are requested by a friend on social media as this most probably would be a fake profile.

Tech support scams

Scammers pose as tech support agents to convince victims that their devices are compromised by viruses, malware, or technical issues. The scammer's objective is to steal money, gain access to sensitive information, or install malicious software. Scammers reach out through phone calls, pop-up messages, emails, or social media, often claiming to represent well-known companies. They aim to persuade victims to grant remote access to their devices, claiming it is necessary to resolve the issue. Once access is gained, scammers may "find" non-existent issues and demand payment for fake repairs or software or install malicious software to steal passwords, financial information, or other sensitive data.

Romance scams

Fraudsters exploit emotional bonds to deceive individuals into providing money or sensitive information. These scams are prevalent on dating websites, social media platforms, and messaging apps, where perpetrators pose as potential romantic partners to gain their victims' trust and eventually manipulate them for personal gain. Once trust is established, scammers invent urgent financial needs, such as medical emergencies, travel expenses, or family crises, and ask the victim for money. The requests often seem urgent, creating pressure on the victim to act quickly. These manipulative tactics can lead victims to send money or share personal information, unaware they are being deceived.

Work-from-Home Scams

With the rise of remote work, scammers exploit the growing demand for flexible job opportunities, deceiving individuals with false promises of high earnings, minimal effort, and attractive perks. These scams often lead victims to financial loss, identity theft, or both.

How to Protect Yourself from Online Scams

To safeguard yourself and your finances, it is crucial to stay vigilant and follow these essential tips.

1. Always Check the URL

Before entering sensitive information, ensure the website's URL starts with HTTPS://. The "s" signifies security, and a padlock icon in the address bar confirms encryption is in place. Avoid providing personal or financial details on sites lacking this security feature, as they are more vulnerable to hackers.

2. Examine the Domain Name

Fraudulent sites often imitate well-known brands by slightly altering the URL. Watch for minor changes, such as misspelt words or added characters. Double-check the domain to confirm legitimacy before sharing sensitive information.

3. Research the Company

Don't judge a website by its design alone. Before making a purchase, especially from an unfamiliar site, investigate its credibility. Check the domain's age—recently created websites are often suspect—and read reviews from other customers to assess their reliability.

4. Look for Grammar and Spelling Mistakes

Professional websites rarely feature grammatical errors or spelling mistakes, especially on key pages like the homepage or "About Us" section. Poorly written content may indicate the website was hastily created by scammers operating from overseas.

5. Verify Trader Information

Legitimate websites provide comprehensive details about the trader, including their company address, email, phone number, and registration information. Be cautious of websites offering only an email address or insufficient contact information, as this is a common red flag.

6. Understand Refunds and Returns Policies

A trustworthy site clearly outlines its refund and return policies, including how to file complaints. Look for platforms that comply with consumer protection laws. Ensure the site mentions cooling-off periods, during which you can cancel an order without penalties.

7. Use Secure Payment Options
Always use secure payment methods, such as credit cards or verified online payment systems. Avoid bank transfers unless you know the recipient personally. Never share credit card details via email, and carefully review terms and conditions, even if they are written in small print.

8. Beware of Unrealistic Offers
Unrealistic offers, discounts or investments are rare and often signal a scam. Approach such deals with caution to avoid losing money or receiving counterfeit goods.

By following these guidelines, you can reduce your risk of falling victim to online scams. Stay informed, remain cautious, and share these tips with friends and family to promote safer online practices for everyone.

SUCCESS STORY

Consumer Secured a Full Refund in a Car Rental Dispute

A recent case involving a car rental booking has highlighted the importance of consumer rights and the value of swift dispute resolution. A traveller who booked a vehicle through an online platform faced an unexpected hurdle but ultimately emerged victorious after persistent efforts and professional mediation.

The consumer selected the vehicle specifically because it was advertised as accommodating three large pieces of luggage. Despite receiving confirmation from the car rental company, the consumer later discovered a discrepancy as the car rental company maintained that the car could only fit two large bags. Seeking clarification, the consumer turned to the platform, which confirmed that the vehicle could indeed hold three large suitcases.

However, upon arriving at the car rental desk on July 3, 2024, the situation took another turn. Instead of the reserved vehicle, the car rental company offered another type of vehicle. When the consumer insisted that they required a vehicle that meets their luggage needs, the agent explained that the chosen vehicle was not available and stated that car bookings are based on categories rather than specific models.

Faced with limited options, the consumer was compelled to pay €400 for an upgrade to secure a suitable car. The car rental company later claimed that the vehicle was unavailable because the consumer arrived late to collect the vehicle.

Unwilling to accept this outcome, the consumer sought assistance from our centre. Acting promptly, we collaborated with the UK International Consumer Centre (UK ICC), which contacted the booking platform on the consumer's behalf. Following this intervention, the trader acknowledged the issue, and the car rental company agreed to refund the extra amount paid to the consumer.

The consumer confirmed receiving the full amount, bringing the matter to a satisfactory close.

News

EU Commission investigating Temu over Digital Services Act Compliance

The European Commission has formally launched an investigation into Temu, a leading online platform, to determine whether it has violated the stringent requirements of the Digital Services Act (DSA).

The European Commission has identified four critical areas of concern in its investigation into Temu's compliance with the Digital Services Act (DSA): The probe will assess whether Temu has effective systems to prevent the sale of non-compliant goods within the EU. This includes examining measures to block rogue traders previously suspended and ensuring the removal of prohibited items. The investigation will evaluate potential risks associated with game-like reward features on the platform, focusing on whether Temu adequately mitigates harm to users' physical and mental well-being. Regulators will scrutinize Temu's compliance with DSA requirements for transparency in its recommendation algorithms. This includes verifying if users are offered the option to access non-profiling-based content recommendations. Authorities will examine whether Temu is providing adequate access to publicly available data, as mandated under the DSA, to facilitate independent research into its operations and impacts.

If breaches are confirmed, Temu could be found in violation of several provisions of the DSA, including Articles 27, 34, 35, 38, and 40. Such findings could lead to regulatory action and penalties. This investigation reflects the EU's broader commitment to enforcing its digital marketplace regulations. The Commission is collaborating with national consumer protection and market surveillance authorities to ensure compliance with both the DSA and EU consumer laws. Temu was officially designated a Very Large Online Platform (VLOP) in May 2024, following its rapid growth to 45 million active monthly EU users. By September 2024, this number had soared to 92 million, prompting increased scrutiny of the platform's practices.

The outcome of this case could establish a significant precedent for how the EU enforces the DSA against other major platforms. By holding Temu accountable, the Commission aims to reinforce transparency, enhance safety for digital consumers, and support researchers in accessing critical data. This landmark investigation highlights the EU's unwavering dedication to ensuring fairness and accountability in the digital marketplace.

EU Authorities Urge Apple to End Geo-Blocking Practices

The European Consumer Protection Cooperation (CPC) Network, in collaboration with the European Commission, has called on Apple to address alleged violations of EU anti-geo-blocking regulations. Investigations led by consumer authorities in Belgium, Germany, and Ireland have flagged discriminatory practices in Apple Media Services, including the App Store, Apple Arcade, and iTunes.

Key Issues Identified
Online Access Restrictions - Apple Media Services provides different user interfaces based on the country where an account is registered. Consumers face significant obstacles when attempting to access interfaces from other EU countries, a practice prohibited under EU geo-blocking rules.

Payment Method Limitations - Purchases on Apple platforms often require payment methods issued in the country of account registration, limiting cross-border payment flexibility for EU consumers.

App Accessibility - Consumers are unable to download apps available in other EU or EEA countries, even when travelling or temporarily residing abroad. This restriction violates EU rules ensuring cross-border service access.

These practices breach the Geo-blocking Regulation, which prohibits unjustified discrimination based on nationality or residence within the EU. They also contravene the Services Directive, which mandates equal access to services across member states unless such restrictions can be objectively justified. Apple has been given one month to address these concerns and propose solutions. If the issues remain unresolved, national authorities may escalate enforcement actions. While dialogue between the CPC Network and Apple is possible, stricter measures will follow if compliance is not achieved.

The outcome of this case could have significant repercussions for cross-border consumer rights in the EU. By addressing these concerns, regulators aim to ensure equal access to digital services and uphold the principles of fairness in the online marketplace.

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.