

## How to protect yourself from online scams?

Online scammers posing as legitimate companies such as eSky.com are on the rise. Their tricks are becoming more and more sophisticated, so it's important to stay vigilant and informed. In this article, you will learn how to protect yourself and others from falling victim to phishing.

### How to avoid eSky.com impersonators?

When communicating online, always be skeptical of unsolicited messages and verify the legitimacy of the source before taking any action. When it comes to eSky.com, look out for these **two tell-tale signs**.

#### 1. Messages on WhatsApp or Telegram

**eSky.com does not use platforms such as WhatsApp or Telegram for recruitment.** No eSky.com employee will ever contact you on these platforms to offer you a job, request personal information or ask for payment. If someone claiming to be from eSky.com contacts you via these channels, it is certainly a scam.

#### 2. Requests for unauthorized money transfers

Beware of imposters who pose as eSky.com recruiters or travel agents. Rest assured that **all legitimate transactions with eSky.com are made through our official platforms or authorized payment partners.** Links to payments via our payment partners are sent by eSky employees using email addresses in the @esky.com domain. Please note that we do not process payments for services in cryptocurrencies, and all our IBAN numbers start either with PL, BG or RO.

### Other precautions

To avoid falling victim to scammers pretending to be from eSky.com, you should take these **five important precautions**:

- Always check the sender's contact details, domain names (@esky.com), and website URLs to ensure they match eSky's official channels.
- Compare the information provided by the person contacting you with the official information available on eSky.com's website or through its official customer support.
- Report suspicious activities to the support of social media platforms on which you notice fraud (Facebook, Instagram, LinkedIn, WhatsApp, Telegram).
- Be skeptical of job offers that seem too good to be true, such as exceptionally high pay for simple tasks.

### Reporting the incident

If you suspect a fraudulent attempt or have already been scammed, you should report the incident immediately by emailing **security@esky.com**. Forward any suspicious web addresses, WhatsApp or Telegram messages, emails or other forms of contact so that eSky.com's security team can investigate the matter further.

**In your message, you should include:**

- WhatsApp/Telegram account addresses of the fraudsters,

- screenshots of chats showing the fraud,
- full chat exports,
- bank account numbers provided by the scammers,
- web addresses used for phishing scams.

You should also **report the fraud to your local authorities**. It will help track down the scammers and prevent them from harming other people. Remember to keep any evidence of the fraud, such as screenshots, messages, emails, receipts, etc.

---

Does this article have the information you were looking for? [Yes](#) | [No](#)

