

Fraudulent messages

Protecting yourself from fraudulent messages

Recognizing phishing and spoofing attempts

Many individuals encounter fraudulent messages through various channels such as email, SMS, WhatsApp, and phone calls. Scammers often pose as Takii employees, departments, or representatives, making it challenging to distinguish their messages from legitimate ones. It's crucial to be watchful and take preventive measures.

Identifying phishing attempts

What is phishing?

Phishing is an attack that aims to steal your money or identity by tricking you into revealing personal information on fake websites. Cybercriminals may impersonate reputable companies, friends, or acquaintances, using deceptive messages containing links to phishing websites.

How to recognize phishing

- Be cautious of messages asking for personal information like credit card numbers or passwords.
- Verify the legitimacy of emails; Takii will not request validation through links or ask for confidential data.

Understanding spoofing

What is spoofing?

Spoofing involves criminals sending messages (email, SMS, or WhatsApp) using someone else's identity. The message may appear legitimate, with recognizable elements like a company logo and email signature. The goal is to persuade recipients to take specific actions, such as providing confidential data.

How to identify spoofing

- Pay attention to the sender's name and email address; spoofers may use familiar names but have a different email address.
- Be cautious if the message urges urgent or threatening actions.

Guidelines for recognition

To effectively recognize fraudulent messages:

- Takii will never request validation or personal information through links.

- Takii will not communicate urgently or threaten users to click on links or provide confidential data.
- Be cautious of emails announcing changes to Takii's bank account details.

Protective measures

Recommendations

- Use a SPAM filter to intercept malicious emails.
- Verify the domain of the sender's address or links.
- Takii has implemented Domain-based Message Authentication (DMARC) to prevent cybercriminals from sending emails using the takii.eu domain. Exercise caution if another domain is used for Takii-related communication.
- If in doubt, contact a known Takii representative to validate the legitimacy of the message before taking any action.

By following these guidelines and taking proactive measures, you can significantly reduce the risk of falling victim to fraudulent messages. Stay vigilant and prioritize your online security.