

Internet Safety.

In this section, you will learn how to use the internet more safely. You will see how to recognise suspicious messages and scams, protect your personal information, and create secure passwords.

Find an educational
video on our website:



Internet Safety.

Recognising fake Bank or GeSY messages.

Recently, many people in Cyprus have received SMS messages that appear to come from their bank or from GeSY, but are actually scams. Their purpose is to make you click a link and provide your passwords or card details.

Recognising fake Bank or GeSY messages.

Here are ways to recognise them:

1

Messages that rush you

They say that something “has a problem” or “must be fixed immediately” to make you act without thinking.

2

Links inside the message

A genuine message from a bank or GeSY will never ask you to click a link to provide passwords.

3

Requests for personal information

The Health Insurance Organisation (HIO) and banks never ask for passwords, card details, or a one-time password (OTP) through SMS or email.

4

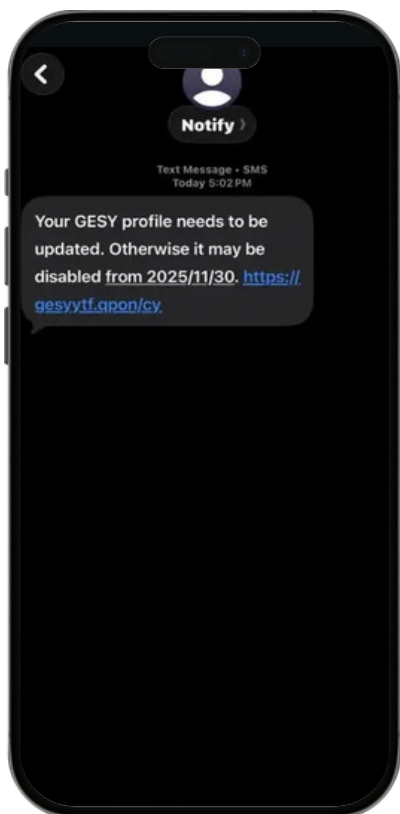
Spelling mistakes or strange wording

Fake messages often contain mistakes or do not address you by name.

Recognising fake Bank or GeSY messages.

Examples of scams

An SMS asks you to click a link, claiming that your GeSY profile needs updating or it will be deactivated.



An SMS asks you to call a number, claiming that a suspicious transaction has taken place in your bank account.

