Be mindful

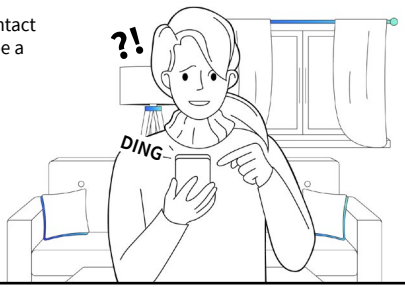
of fraudulent messages

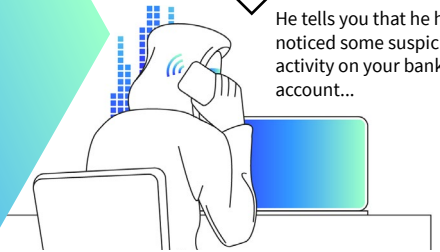
Every day, phishing emails, messages or SMS imitating official LuxTrust messages proliferate.

Here is a common example of phishing and how to protect yourself.

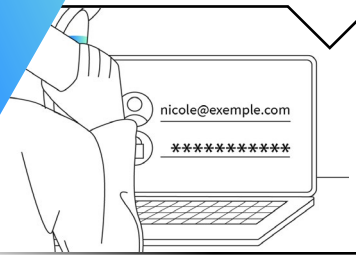
Sharing access codes

Someone might contact you pretending to be a LuxTrust employee.



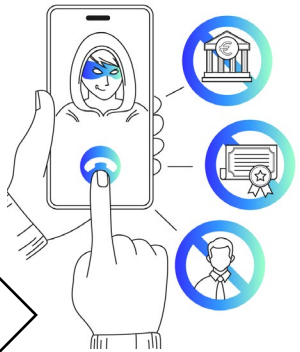


He tells you that he has noticed some suspicious activity on your bank account...



and asks you to share your LuxTrust credentials (UserID, password, etc.) in order to block your certificate and accounts.

There are three good reasons to hang up immediately:



1. LuxTrust is not a bank and has no access or control over your accounts.
2. LuxTrust does not need your UserID and password to change the status of your certificate (suspension or revocation).
3. LuxTrust does not contact its clients directly by phone and definitely never outside office hours (8am-6pm).

LUXTRUST
Enabling a digital world

In case of doubt, our team is here to help you.

+352 24 550 550 questions@luxtrust.lu

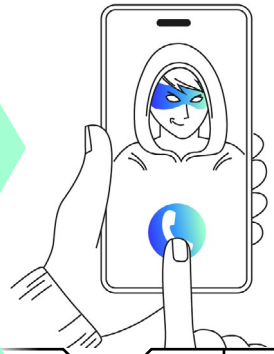
Be mindful

of fraudulent messages

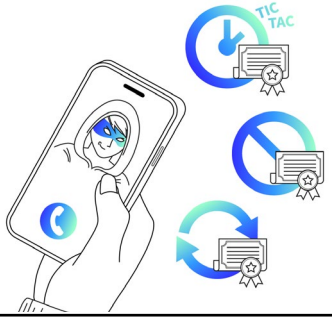
Every day, phishing emails, messages or SMS imitating official LuxTrust messages proliferate.

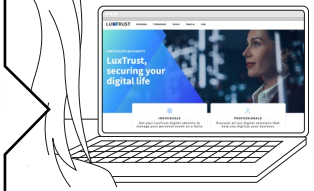
Here is a common example of phishing and how to protect yourself.

Certificate renewal



If you receive a phone call, text message or email asking you to renew your certificate as soon as possible or risk having your access blocked, be careful.

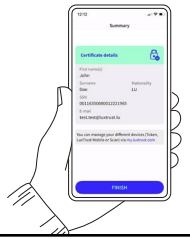




Go to our official website by typing www.luxtrust.com directly into your browser's address bar (never click on links) and check the status in My LuxTrust / My Certificate / Test my certificate.

OR open your LuxTrust Mobile app.

Before doing anything, check the validity or status of your certificate yourself (activated, suspended, revoked):



Go to:

- Menu
- My certificate

LUXTRUST
Enabling a digital world

In case of doubt, our team is here to help you.

+352 24 550 550 questions@luxtrust.lu