EORTC
European Organisation for Research
and Treatment of Cancer

Using clinical trials tools: security fundamentals

Site training

Version 1.0

27 Nov 2023

The future of cancer therapy

Web application some security tips

- Avoid public Internet access point
- Activate multi-factor authentication (if available)
- Use a strong and unique password per web application
- Use an up-to-date computer with antivirus
- Beware of emails asking you to change your password
- Never share your account
- Save your password in a password manager software
- Use your corporate computer

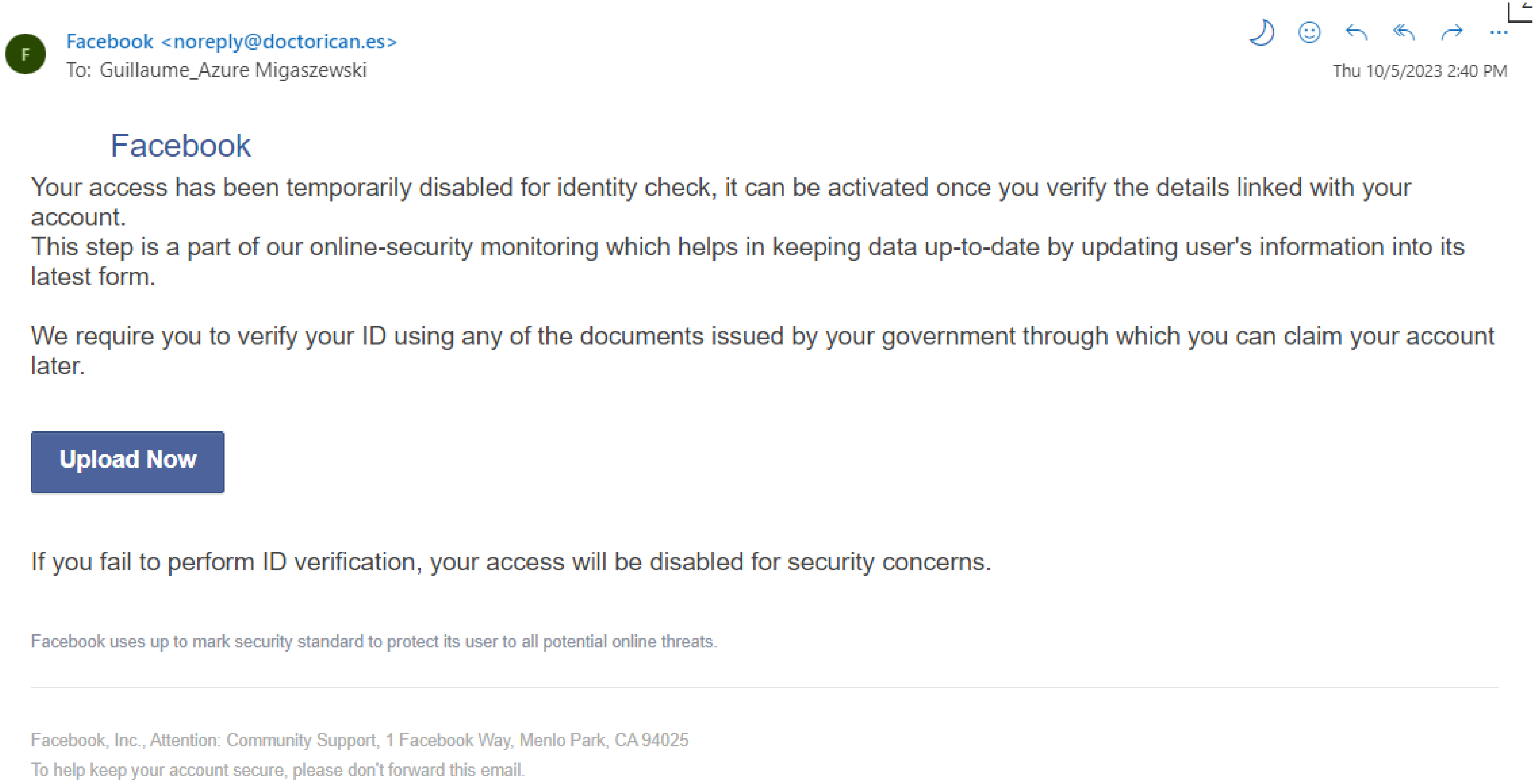
Phishing

- **Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker**
- Beware of emails asking you to change/update your password, it might be a phishing
- **Social engineering** common vectors are emergency, fear, desire to help, desire to solve problem.

How to spot a phishing email

- Beware of use of emergency or threatening language
- Check carefully sender email address
- Hover over web hyperlinks before you click
- Pay attention to poor spelling and grammar
- Inconsistencies in email Addresses, Links and Domain Names
- Suspicious attachments
- Request for credentials

Phishing email example I



Facebook <noreply@doctorican.es>
To: Guillaume_Azure Migaszewski

Thu 10/5/2023 2:40 PM

Facebook

Your access has been temporarily disabled for identity check, it can be activated once you verify the details linked with your account.
This step is a part of our online-security monitoring which helps in keeping data up-to-date by updating user's information into its latest form.

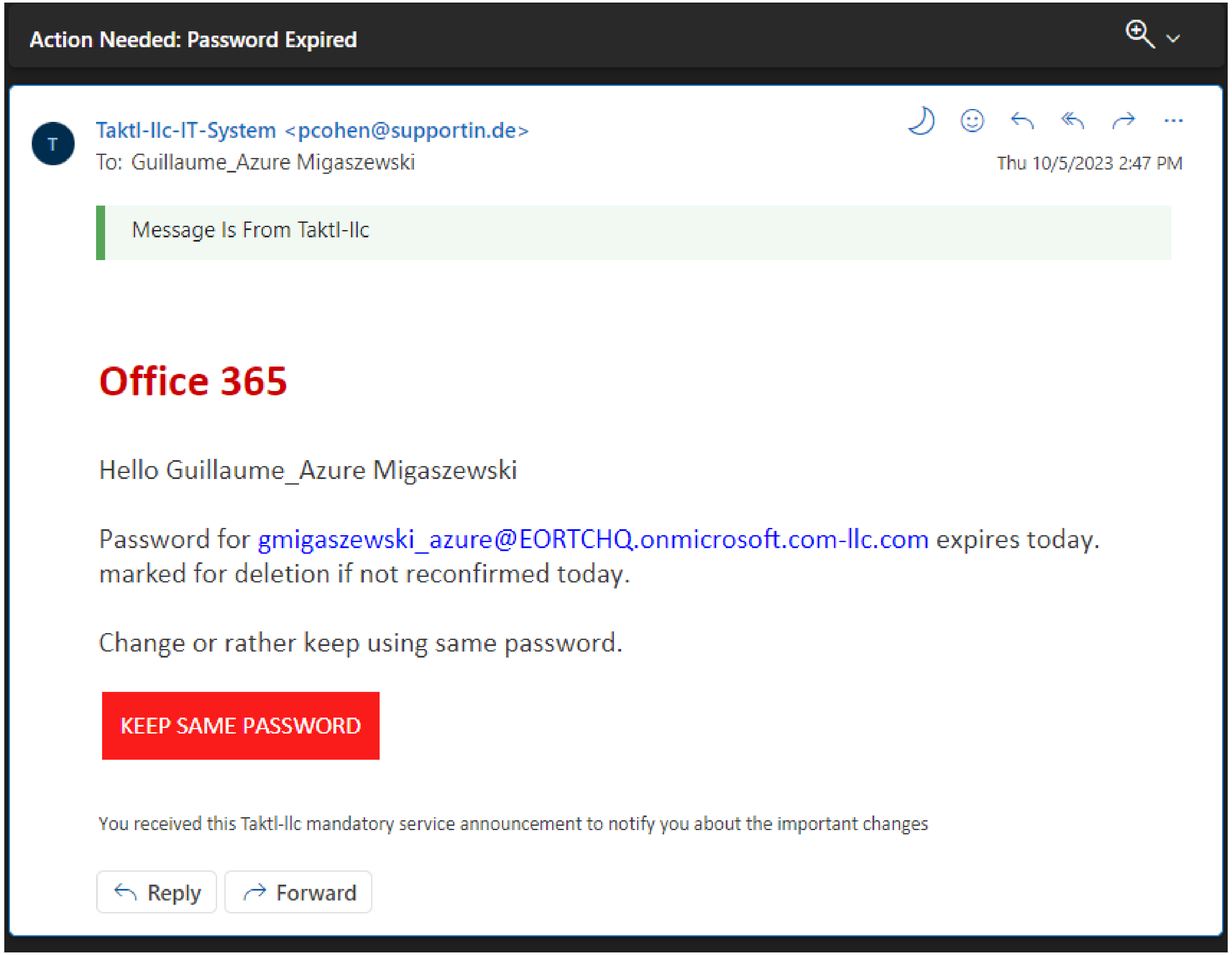
We require you to verify your ID using any of the documents issued by your government through which you can claim your account later.

If you fail to perform ID verification, your access will be disabled for security concerns.

Facebook uses up to mark security standard to protect its user to all potential online threats.

Facebook, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025
To help keep your account secure, please don't forward this email.

Phishing email example II



Action Needed: Password Expired

Taktl-llc-IT-System <pcohen@supportin.de>
To: Guillaume_Azure Migaszewski

Thu 10/5/2023 2:47 PM

Message Is From Taktl-llc

Office 365

Hello Guillaume_Azure Migaszewski

Password for gmigaszewski_azure@EORTCHQ.onmicrosoft.com-llc.com expires today.
marked for deletion if not reconfirmed today.

Change or rather keep using same password.

KEEP SAME PASSWORD

You received this Taktl-llc mandatory service announcement to notify you about the important changes

Reporting a security incident

- Mail security@eortc.org for any security incident or related question
  - Account compromised
  - Major cyber incident impacting your IT systems
  - Computer infected by a virus
  - Computer stolen or lost
  - Phishing attempt targeting your EORTC web application account (abnormal password reset email, etc.)