

Duration: 3 hours

Prerequisites:

- No prior knowledge of cybersecurity required.
- Access to a computer with an Internet connection.

Teaching methods:

- Online training, asynchronous
- Training materials included

Skills acquired by the end of the course:

- Understand cybercrime threats and trends
- Protect personal information and organizational data
- Adopt sound security practices day to day

Certificate: yes

DESCRIPTION

Fraudsters and hackers are everywhere. They are opportunistic, creative, and the consequences of an incident are significant — in cost, in reputation and in time. How do they operate? What are the current trends and best practices? How do you protect your clients, your teams and your organization? How do you keep years of effort from evaporating in a single click? Nobody wants their information, or their clients' information, stolen and shared. Awareness and prevention are your greatest allies.

PROGRAM:

General objective

- Raise awareness and equip participants to protect personal information.
- Promote good practices, online and offline.

Specific objectives

- Dispel common misconceptions about cybercrime.
- Identify the emotions cybercriminals exploit.
- Recognize current trends and understand the threat.
- Clarify what constitutes personal information.
- Recognize a privacy incident.
- Understand what qualifies as serious harm.
- Ensure the security and integrity of data.
- Handle data securely.
- Adopt better practices for email.
- Test password strength and opt for a high level of security.
- Authenticate safely.
- Maintain good practices remotely and on public Wi-Fi networks.

QUESTIONS/ANSWERS