



RJM STRATEGY GROUP

PLAN. PREPARE. PROTECT.



CYBERSECURITY - LEVEL I

(IN PERSON OR VIRTUAL)

The Cybersecurity Level I session provides essential insights into safeguarding digital environments from threats. The session covers various topics, starting with the fundamental question: How to avoid a virus?

Attendees are educated on the diverse ways through which computer viruses can infiltrate systems. This includes email attachments, internet downloads, infected USB drives and compromised websites, emphasizing the importance of vigilance whenever data is received.

The discussion then delves into unseen threats, highlighting "MITM" attacks (Man-in-the-Middle) and WI-FI-based attacks. Participants are made aware of the risks associated with credential harvesting over open networks, particularly concerning when individuals reuse passwords across multiple services.

Scams and Ads are identified as potential hazards, and the session provides practical guidance on recognizing warning signs and avoiding falling victim to deceptive tactics. Attendees are equipped with the knowledge to navigate the digital landscape safely.

The concept of social engineering is introduced, shedding light on manipulative tactics employed by cybercriminals to exploit human psychology. Practical tips are shared on protecting oneself against social engineering, emphasizing the importance of skepticism and caution.

The session concludes with insights on overall cyber-attack protection strategies. Participants are prompted to evaluate their online presence, asking whether they might share too much on social media.

The Cybersecurity Level I session delivers a comprehensive overview of common threats, protective measures and best practices to fortify one's digital space against potential cyber-attacks.

TAMBIÉN TEMENOS INSTRUCTORES DE ESPAÑOL.

RAY@RJMSTRATEGYGROUP.COM | 630-360-1965

WWW.RJMSTRATEGYGROUP.COM

