INQUEST

INQUEST SECURITY AWARENESS TRAINING

Benefits:

- Empowering your employees to recognize and classify different types of cyber-threats

- Encouraging a culture of trust, communication and incident reporting on potential cyber-attacks on the company level

- Reducing risk of successful phishing attacks and malware infections by up to **90%**

- Introducing employees to common cyber incident scenarios, collected from real-world business environments

"

YOUR BUSINESS'S CYBER SECURITY IS ONLY AS STRONG AS YOUR WEAKEST EMPLOYEE

More than 90% of successful cyber-attacks today begin with a phishing email, and nearly every fourth phishing email ends up open by one of your employees.

By promoting cyber security awareness, instead of being a negligent accomplice, you can make your employee become your **first line of defense** against cybercrime.

Relying upon over a decade's worth of expertise in cyber security, we have created a training program that allows you to achieve the intended outcome.

Inquest Cyber Security Awareness training program is designed to cover all key aspects vital to raising the awareness of your employees about their specific role in enterprise cyber security ecosystem and is to be considered useful for both IT sector specialists and employees engaged across other sectors.

Our training program and real-world examples the training specialist assigned guides you through during the session, will enable your employees to take a more careful approach when it comes to company resources equipping them with practical knowledge to build a skill set necessary to protect your company against most common sophisticated cyber-threats.

RAISING RISK AWARENESS

RISK BEHAVIOUR ASSESSMENT

REDUCED RISK EXPOSURE
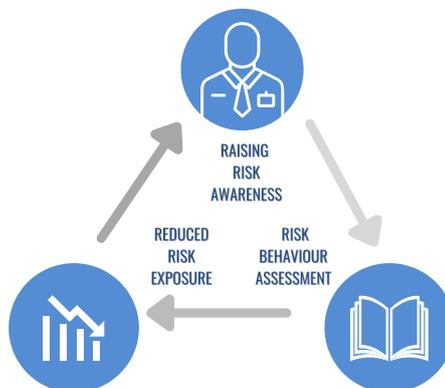
TOPICS TO DISCUSS:

Targeted email phishing and social engineering: through real-world examples, your employees will learn how to recognize phishing and what to focus on when they receive malicious emails. In addition to the above, other techniques of social engineering (SMiShing, vishing) shall be discussed.

Browser security: This module discusses what the browser knows about its users and what it shares with other stakeholders, what to be careful about and what steps to take to further improve browser security.

Mobile device protection: within the context of this module, training participants will be able to learn how to check and improve the security of business mobile devices and apps installed.

Password management: the segment concerning the importance of creating strong passwords for each and every account your employees use in work environment. Training envisages several real-world ready-to-use techniques intended for use by your workforce immediately upon completion of the training, in order to prevent potential cyber attackers from coming into possession of their passwords for malicious activity and data breach purposes.

Public Wi-Fi Security: In the final part of the training, your employees will be introduced to dangers lurking in the background on devices using public WiFi network connections.

Our company provides a great opportunity to opt for an **in-house** professional training covering various areas of cyber security ensuring modules tailored to suit specific needs of your business environment.

LEARN MORE

For additional information on Cyber Security Awareness training programs, please contact us:
seminari@cybersecurity.rs
+381 11 6351500

COMPANY BACKGROUND:

Inquest Ltd. was founded in 2008 aiming to provide Serbian and regional markets with cutting-edge IT security and digital data protection software solutions and services. Over the past 13 years of business, we have gained significant experience in this field, and became one of the leading regional partners specializing in innovative and reliable cyber security solution delivery.

INQUEST