CERTIFIED SECURITY AWARE USER

CSAU

Duration: 1 day; Instructor-led | Virtual Instructor-led

OVERVIEW

It's easy for the security message to sound stale and overused given all the news reports about hackers, botnets, and data breaches involving personal information. People find it simple to claim, "It won't happen here." The human factor, or what people do or don't do, is the biggest hazard to information systems and assets, studies and surveys consistently demonstrate. Technology by itself won't be able to secure your company unless we deal with the human problem. The weakest link in the security chain will always be people.

These challenges are addressed in this high-impact security awareness training. By making sure your users are aware that they are targets, training them how to use technology safely, and ensuring your company stays compliant, it motivates and alters behaviour. Additionally, you move beyond just prevention and start establishing human sensors, building a much more resilient company, by training your users the indicators of compromise and how to report occurrences.

OBJECTIVES

- Understand all the Latest Attacks and ways to mitigate them.
- Understand on Why Cyber Security is a Boardroom activity.
- Understand the Way to Move Forward: Mitigating & Managing Cyber Security for your organization.
- Learn how to handle During and After Breach scenarios.
- Map Security Obligations by Role in your organization.

AUDIENCE

All users of the Internet, computers, mobile phones, and social media are welcome to attend this program, which is based on an interactive storyboard and 100% LIVE HACKING Demos. Suitable for ALL; NO Technical Jargon.

COURSE CONTENTS

Module 1: Anatomy of Attack

- What is Security, Vulnerabilities & O-Days
- Attack life Cycle & How much hacker makes by selling your passwords and data?
- Different Attack Vectors, Threats Vs. Risks, Exploit Basics
- Why are Perimeter defences failing?
- Why Anti-Virus is not enough?

Module 2: Latest Attack Trends: 100% Demo

- Business Email Compromise (BEC)
- Ransomware
- Advanced Persistent Threat
- Malvertising
- Mobile Malwares
- Web Attacks
- Identity Theft

Module 3: Social Engineering Attacks

- Drive by Download Attack with Java
- USB / File attachment Attacks
- Phone Call & Sweet Talking
- Facebook and social media-based attacks
- Best Practices for Safer Social Media Usage for Adults and Kids.

Module 4: Password Management & Privacy

- What is strong Password? Why password must be changed at least once in 90 days?
- Why should u not use same password in more than 1 web application?
- Privacy = Extinct
- PII: Personally Identifiable Information & Personal Data Protection Act
- Best Practices for Password Management & Privacy

Module 5: Email & Messaging Security

- Email Spoofing
- Phishing
- Disposable Emails
- WhatsApp, Telegram, and similar Messaging Systems security
- Best Practices for Email Security
- Best Practices for Messaging Software

Module 6: Wireless Attacks

- Understanding WEP, WPA, WPA2
- Why Public Wi-Fi and Free hotspots are dangerous?
- Sniffing and MiTM attacks on Wi-Fi
- How to secure office and house Wi-Fi

Module 7: Mobile Security

- Jail Breaking & Rooting: Why its disaster?
- DO you need Antivirus on a Mobile device? / Why Antivirus don't work > Why MTD
- How hackers hack your phone and control it?
- A Sample Android iOS Malware

GemRain Consulting Sdn Bhd.
33-5.6, Block C, Jaya One, Jalan Profesor Diraja Ungku Aziz, 46200 Petaling Jaya, Selangor, Malaysia
Contact: (+60)3 7931 3036 | (+60)12 613 3667 | Email: enquiry@gemrain.net | Website: www.gemrain.net

- Security best practices for Mobile

Module 8: Cybersecurity MythBusters

- Websites are fully secure once there is a HTTPS Green or Gold lock
- Antivirus will protect us from Viruses
- Wi-Fi Hotspots are safe
- As long as I don't download a file from Internet, I will not be infected
- iPhone is Secure
- Mobile Apps downloaded from Play Store are Secure
- My Business / Data in too small for a cyber attack
- Bringing my own Device is safe
- IT Will take care of everything, we don't have to worry
- 'From' address in an Email confirms that the email is sent by the email user
- My Online business is safe using marketplaces
- Online shopping and Online payment are very safe
- USB devices are the safest storage medium