distance network academy

CYBER SECURITY

E-LEARNING

Entrare in contatto con realtà lontane da noi, e delle più varie, scegliere tra un ampio ventaglio di prodotti e servizi, accedere a risorse di elaborazione e archiviazione nella misura e per il tempo necessari, senza acquistare apparecchiature dedicate e disporre dello spazio fisico per collocarle, sono solo alcuni dei vantaggi che ci offrono le moderne tecnologie informatiche.

A fronte di questi innegabili vantaggi, la diffusione di queste tecnologie, e la rapida e costante evoluzione, comportano un approccio non sempre consapevole. Ciò è particolarmente vero in tema di sicurezza, poiché anche le minacce ai nostri dispositivi e ai nostri dati evolvono e si diffondono altrettanto velocemente.

Se, quindi, da una parte i moderni strumenti di difesa garantiscono elevati standard di sicurezza, lo stesso non si può dire per l'atteggiamento degli utenti nei confronti delle minacce.

Troppo spesso comportamenti non sufficientemente consapevoli dei rischi compromettono non solo i dispositivi utilizzati nella vita privata, ma anche i sistemi critici per l'attività professionale, per gli obiettivi di impresa, e per i servizi di pubblica utilità.

Tutti questi sistemi si trovano costantemente sotto la minaccia di violazioni perpetrate dagli hacker, alla ricerca di informazioni preziose e di vie di accesso per utilizzarne indebitamente le risorse di elaborazione, oppure per prenderli in ostaggio, letteralmente, e chiedere un riscatto al titolare. A tale proposito è stata coniata l'espressione: "Advanced Persistent Threat" (APT). Virus, phishing, ransomware e truffe informatiche mettono quotidianamente in pericolo la serenità di tutti noi.

Difendersi da queste minacce è possibile, attraverso la presa di coscienza del crimine informatico nelle sue numerose, e pericolose, sfaccettature, la conoscenza degli strumenti tecnologici dedicati, ma soprattutto l'adozione di comportamenti che evitano di esporre i sistemi a inutili rischi.

Oggetto di questo corso sono il reato informatico, le sue minacce, gli strumenti per difendersi da esso, i comportamenti che riducono il rischio di rimanerne vittima, la tutela dei dati personali, con l'obiettivo di fornire quel grado di consapevolezza che permetterà di affrontare con il corretto atteggiamento il tema della sicurezza informatica nella nostra quotidianità.

Codice: 23-SFT-CBS-01-EL
Livello: Introduttivo
Durata: 3 ore
Modalità: E-learning

IL CYBERCRIMINE

Il reato informatico
Chi sono i cybercriminali, cosa cercano, come operano
Ethical hacking: black hat/white hat

IL MALWARE

Virus
Botnet
Zero-day vulnerability
Phishing
Social engineering
Man-in-the-middle
Ransomware

LE DIFESE

Antivirus
Backup
Password
Crittografia
Firewall e VPN
Autenticazione a due fattori

PRUDENZA

WiFi pubblico

Riconoscere le false e-mail

Riconoscere le truffe

Furto di credenziali

Need-to-know

PRIVACY

I dati personali

La tutela legale della privacy

Il GDPR

Accettare i trattamenti (e revocare i consensi)