



CYBER SECURITY  
ACADEMY



# SECURITY AWARENESS

## Corso di consapevolezza sulla sicurezza informatica

Un corso per **tutti**, per rafforzare l'anello debole della catena della sicurezza: **NOI!**

I recenti fatti di cronaca hanno riportato una crescente diffusione di attacchi informatici su vasta scala che hanno colpito aziende, organizzazioni governative e infrastrutture critiche in tutto il mondo, creando danni economici e reputazionali molto importanti. Il tutto affiancato dal quotidiano stillicidio di attacchi informatici a PMI e persone singole, famiglie e organizzazioni varie, finalizzati ad estorcere denaro o minare la reputazione di persone e aziende per i più svariati fini, al furto di informazioni sensibili o business critical.

Non è più pensabile delegare la sicurezza informatica al solo reparto IT, o all'amico dell'amico, o al fai-da-te, ma è indispensabile stimolare un approccio di consapevolezza pervasivo all'interno delle aziende e delle organizzazioni, che promuova una cultura della sicurezza informatica a tutti i livelli.

Obiettivo di questo mini-corso, rivolto a tutti gli utilizzatori di tecnologia informatica connessa a internet, è di aumentare il livello di consapevolezza delle persone, attraverso decine di esempi di attacchi informatici presi dal quotidiano, imparando a riconoscerli e ad evitarli.

Creare una cultura sulla sicurezza informatica, insegnando poche semplici abitudini nell'uso quotidiano della tecnologia, a beneficio di tutti i collaboratori, tutta l'organizzazione aziendale e alle singole persone nell'utilizzo privato.

## Modalità

Il corso è destinato a tutte le persone che utilizzano le tecnologie informatiche quali personal computer, smartphone e tablet sia per scopi professionali che personali.

**Non è richiesta alcuna competenza tecnico-informatica specifica.**

Durante lo svolgimento del corso, **il docente spiega i rischi informatici e le modalità per evitarli** attraverso l'ausilio di moltissimi **esempi pratici presi dalla realtà**, focalizzandosi sull'utilizzo delle email, della navigazione internet, e sulla protezione della propria identità digitale.

Al termine del corso viene distribuito un decalogo, con i principali suggerimenti di sicurezza informatica. Il corso può prevedere un mini esame online, al fine di verificare l'apprendimento degli argomenti.

### > Introduzione

*Fattori di rischio*

*Chi sono gli hacker e per chi lavorano*

*Il valore di un sistema compromesso*

### > Navigazione web

*Navigare in sicurezza*

*Riconoscere i contenuti malevoli*

*Identificare i siti truffa*

### > E-mail

*Riconoscere le truffe (phishing e scam)*

*Evitare le infezioni*

### > Ingegneria sociale

*Evitare il trapelamento di informazioni*

*Cosa non ti dovrebbe mai essere richiesto*

*Le richieste truffa al telefono*

### > Sicurezza dei dati

*Cosa succede quando perdo un dispositivo?*

*Proteggere le informazioni sensibili*

*L'importanza dei backup*

### > Proteggere la propria privacy

*Ripulire i dispositivi*

*Evitare il furto di identità*

*Condividere con attenzione*

### > La reputazione

*Verificare la reputazione di persone e servizi web*

### > Gestione delle password

*Linee guida di utilizzo delle password*

*Memorizzare le password in modo sicuro*

### > Pratiche comuni di protezione

*Il decalogo per proteggersi*

## Security Lab

Security Lab si propone al mercato come azienda di consulenza nell'ambito della Cyber Security, annoverando tra i suoi clienti aziende che operano nei settori finanza, banking, health care, farmaceutico, Industriale e information technology in diverse nazioni.

Security Lab si avvale di personale altamente specializzato nei settori della sicurezza organizzativa e tecnologica, con significative esperienze internazionali.

La costante attività di Security Lab di monitoraggio del mondo del crimine digitale e della scena underground consente di abbinare ad un approccio metodologico la conoscenza derivante dalla continua ricerca sulle vulnerabilità ed i crimini nella rete.

## About Zone-H

Zone-H, osservatorio digitale indipendente e open-source dal 2001, è oggi una voce autorevole in Internet in materia di crimine informatico. La home page di [www.zone-h.org](http://www.zone-h.org) registra 35.000 singoli accessi al giorno per un totale di circa 800.000 click.

I dati raccolti da Zone-h costituiscono uno dei più grossi archivi digitali al mondo sui crimini informatici, includendo più di 12.000.000 di incidenti registrati e verificati, includendo informazioni sul profilo degli attaccanti, le relative motivazioni, e le metodiche di intrusione.

I programmi di formazione di consapevolezza ed Ethical Hacking sono frutto del know-how e dell'esperienza di Zone-H, che organizza corsi e seminari in diversi paesi, trattando gli aspetti fondamentali della Internet security con lo scopo di promuovere la fusione della filosofia dell'osservatorio di prevenzione e il costante aggiornamento dei sistemi di difesa informatici e della governance tra i professionisti IT.



[www.zone-h.org](http://www.zone-h.org)

