

THE CYBER PALACE

Informatica



DURATA: 2 ORE E 30 MIN.

*Modalità compatibile con tutte
le piattaforme e pertanto fruibile
sia su piattaforma ANIA SAFE
che propria del cliente*

OBIETTIVI



▶ **ACQUISIRE**

le nozioni di base, in termini di strumenti e metodi,
per affrontare il tema della cyber security in azienda

▶ **CONOSCERE**

le principali minacce informatiche

▶ **APPROFONDIRE**

gli accorgimenti utili per difendersi dalle minacce informatiche

IL CORSO È COMPLIANT ALLA NORMATIVA IVASS

- *Contiene quiz intermedi e test finale per la verifica delle conoscenze*
- *Gli elementi didattici (video, job stop, ...) sono vincolati*
- *I contenuti del corso sono costruiti e validati da docenti con pluriennale esperienza e requisiti richiesti*



CONTENUTI

MODULO 1

CYBER SECURITY E COMPORAMENTI UMANI

- ▶ Clean Desk Policy
- ▶ Blocco della workstation
- ▶ Dispositivi portatili
- ▶ Stampa di un documento

MODULO 2

LA SICUREZZA DEGLI SMARTPHONE E TABLET

- ▶ E-mail senza livello di classificazione
- ▶ Need to Know: cc
- ▶ Need to Know: separazione dei contenuti

MODULO 3

LA RIDONDANZA DEL DATO E IL BACKUP

- ▶ Clean desk policy: HD di backup
- ▶ Clean desk policy: USB key
- ▶ Clean desk policy: DVD e documenti
- ▶ Supporti di memoria rimovibili

MODULO 4

LA SICUREZZA NEL PROCESSO DI AUTENTICAZIONE

- ▶ Utilizzo di supporti rimovibili di provenienza ignota
- ▶ Software scaricato da Internet
- ▶ Download di materiale coperto di diritto d'autore
- ▶ Programmi ricevuti via e-mail o chiave usb



CONTENUTI

MODULO 5

I PROFILI DI AUTORIZZAZIONE

- ▶ Strumenti di anonimizzazione
- ▶ Pubblicazione su Internet di documenti uso interno
- ▶ Accesso all'area share

MODULO 6

IL "PESO" DEL DATO E LA SUA CIRCOLAZIONE

- ▶ Scambio di materiale coperto da diritto d'autore
- ▶ Connessione non autorizzata di periferiche
- ▶ Download di materiale coperto da diritto d'autore mediante peer-to-peer
- ▶ Software peer-to-peer

MODULO 7

LA DIFESA DAL PHISHING, DAL RANSOMWARE, DALLE FRODI E DAL FURTO DI DATI

- ▶ Utilizzo della password aziendale su siti esterni
- ▶ Login su pagina non sicura
- ▶ Link nelle e-mail di phishing
- ▶ Phishing

MODULO 8

LA PROTEZIONE DAI VIRUS

- ▶ Spam
- ▶ Catene di S.Antonio
- ▶ Risposta a messaggi di spam
- ▶ Catene e hoax



CONTENUTI

MODULO 9

LA SICUREZZA DELLE CREDENZIALI E I TEST DEL SISTEMA AI FINI DELLA SICUREZZA

- ▶ Condivisione della password
- ▶ Annotazione della password in luogo non sicuro
- ▶ Tutela delle informazioni di accesso ai sistemi informatici
- ▶ Social Engineering
- ▶ Accesso ai sistemi informatici

MODULO 10

LA CIFRATURA DEI DATI

- ▶ Computer-to-computer network
- ▶ PC portatile con chiavetta usb wireless con spia accesa
- ▶ PC portatile collegato a Internet con chiavetta esterna e contemporaneamente alla rete aziendale direttamente via cavo.
- ▶ Modifica dei parametri di configurazione per la connessione alla rete
- ▶ Access point non autorizzati

Ania

SAFE
FORMAZIONE

www.aniasafe.it



formazione@aniasafe.it

skilla

