Rischi Cyber e Resilienza

Percorso Cyber Security e Phishing

Modalità di Fruizione:
Modulo 1: on line asincrono
Modulo 2: aula virtuale o frontale
Modulo 3: webinar
Rivolto a:
Modulo 1: corso base per tutti i dipendenti
Modulo 2: corso avanzato esperti sicurezza, sistemi IT, responsabili di servizi, referenti privacy
Modulo 3**:** corso base di awareness per tutti
Test di valutazione: previsto per il corso online asincrono

Descrizione del percorso

In un mondo sempre più interconnesso e digitale, la sicurezza informatica e la protezione dei dati sono diventati temi di cruciale importanza. La diffusione delle tecnologie digitali ha creato nuovi rischi e minacce per la privacy, la sicurezza dei dati e la stabilità delle infrastrutture critiche. L'espansione del lavoro remoto, delle piattaforme cloud e dei dispositivi mobili ha aumentato la superficie di attacco e reso più complesso il controllo delle attività informatiche.

Il percorso formativo si propone l'obiettivo di migliorare la consapevolezza delle persone sui temi della sicurezza informatica e della protezione dei dati, attraverso una serie di iniziative formative modulari volte a promuovere la cultura della cybersecurity e ad aumentare la resilienza degli enti.

Il percorso formativo, suddiviso in moduli fruibili anche singolarmente, si struttura in attività differenziate, per le diverse tipologie di destinatari coinvolti al fine di massimizzare l'efficacia didattica degli interventi.

MODULO 1

Il corso online di livello base, della durata di 2 ore, si articola in video lezioni auto-consistenti e sottotitolate, presentazioni interattive, momenti di autovalutazione, per un graduale percorso di apprendimento. Partendo dai concetti alla base della cybersecurity, si analizzano aspetti specifici come le tipologie di minacce cyber, le vulnerabilità dei sistemi, le insidie più comuni del web e si illustrano le buone pratiche per garantire la sicurezza dei dispositivi che utilizziamo nel lavoro e nella vita privata.

Il corso si compone dei seguenti argomenti:

- Panorama generale delle minacce (consapevolezza del rischio cyber, cultura della sicurezza e reticenza della denuncia, framework di modellazione delle minacce
- Gestione dell'identità
- Rischi associati alla vita online (navigare in sicurezza, best practice per il lavoro a distanza, rischi associati alla vita online
- Gestione degli incidenti (riconoscere e segnalare un incidente, analisi di incidenti famosi)

DESTINATARI

Tutti i dipendenti

TEMPISTICHE

Disponibile da gennaio 2025

MODALITA' DI EROGAZIONE

Corso Fad (asincrono)

MODULO 2

Il modulo 2, di livello avanzato, della durata di 2 a 4 ore sulla base delle esigenze di approfondimento dell'ente, si focalizzano sulle tematiche Phishing e Cybersicurezza con un approccio laboratoriale di simulazione di attacchi e di esercitazioni pratiche e prevedono il coinvolgimento di più docenti per garantire la massima efficacia didattica.

- Prima sessione: Phishing
    - Le tipologie di minacce e di attacchi phishing, come riconoscerli e gestirli. Esempi reali di attacchi ed esercitazione pratica.

- Seconda sessione: Cybersicurezza:
    - Il modulo ha l'obiettivo di far comprendere le principali tecniche di attacco e di illustrare la "cyber kill chain" al fine di intraprendere le più efficaci metodologie di risposta agli incidenti; il corso può prevedere la pianificazione (progettata ex-ante con l'ente) di alcune simulazioni di incidenti al fine di misurare il grado di competenza del personale e di rilevare eventuali gap (competenze, procedurali, di processo, etc..).

DESTINATARI

Esperti sicurezza, sistemi IT, responsabili di servizi, referenti privacy

TEMPISTICHE

Disponibile da gennaio 2025

MODALITA' DI EROGAZIONE

Aula fisica (max 20 partecipanti)

(presso Ente o presso la sede di CSI Piemonte)

MODULO 3

Il ciclo di webinar si pone l'obiettivo di consolidare e rafforzare la consapevolezza Cyber in relazione anche alle nuove leggi e direttive (es. Legge 90/2024, Direttiva NIS2).

I webinar, della durata di due ore ciascuno, possono essere fruiti come ciclo oppure singolarmente. Prevedono il coinvolgimento di una pluralità di relatori.

- La gestione della cybersecurity e della privacy nella catena di fornitura
- La gestione degli incidenti IT (contenimento, segnalazione alle autorità, remediation, continuità operativa, etc..)
- Legge 90/2024 e NIS2: l'impatto sui servizi della PA
- La gestione del rischio Cyber

DESTINATARI

Tutti i dipendenti (ad eccezione del webinar Legge 90/2024 e NIS2: l'impatto sui servizi della PA rivolto a esperti sicurezza, sistemi IT, responsabili di servizi, referenti privacy)

TEMPISTICHE

Disponibile dal secondo trimestre 2025

MODALITA' DI EROGAZIONE

Webinar (ca 300/400 partecipanti a webinar)

(tramite piattaforma di CSI con messa a disposizione della registrazione del webinar)