CORSO CYBER SECURITY AWARENESS PER UTENTI AZIENDALI

Durata: 3,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

PROGRAMMA

MODULO 1: PERCHÉ LA CYBER SECURITY RIGUARDA TE

1.1 Il rischio reale

- I rischi informatici oggi: dati e numeri concreti
- Non è "solo un problema dell'IT»
- Cultura no-blame: perché segnalare un errore subito, senza paura, salva l'azienda

1.2 Il valore delle informazioni

- Perché proteggere i dati conta strategicamente
- Impatti economici e reputazionali: casi reali

1.3 Cenno normativo

- NIS2: la sicurezza è anche un obbligo, non solo buon senso

MODULO 2: SOCIAL ENGINEERING — IL MECCANISMO DIETRO AGLI ATTACCHI

2.1 Come ci manipolano

- Le leve psicologiche: urgenza, autorità, fiducia, paura
- Perché funzionano anche su chi è attento
- OSINT: come i criminali costruiscono l'esca perfetta dai tuoi profili social

2.2 L'AI cambia le regole del gioco

- La truffa del CEO, ieri e oggi
- Deepfake vocali e video: quando voce e volto non bastano più come prova
- Caso reale: bonifico autorizzato dopo una videochiamata clonata

2.3 Come difendersi

- Verifica su un secondo canale indipendente
- "Sembra vero" non è più una prova

MODULO 3: PHISHING E DERIVATI — L'ATTACCO PRENDE FORMA

3.1 Phishing nell'era dell'AI generativa

- Identificazione e prevenzione
- Basta con "controlla gli errori grammaticali": l'AI scrive email perfette
- Esempi reali aggiornati al 2026

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO CYBER SECURITY AWARENESS PER UTENTI AZIENDALI

Durata: 3,5 ore

3.2 Vishing e smishing

- Phishing vocale e via SMS
- Smishing su Teams/Slack: la fiducia nei canali interni come trappola

3.3 Quishing e nuove varianti

- QR code malevoli: finte multe, volantini, menu
- Attacchi combinati: più tecniche, stesso tentativo

3.4 Esercitazione pratica

- Analisi guidata di messaggi reali: "fidati o non fidati?«

MODULO 4: QUANDO L'ATTACCO RIESCE — LE CONSEGUENZE

4.1 Ransomware

- Come funziona: caso reale passo passo
- Doppia estorsione: cifratura + minaccia di pubblicazione dati
- Supply chain attack: l'email "legittima" da un fornitore compromesso

4.2 Furto dati senza cifratura

- La minaccia silenziosa: rubare senza bloccare nulla
- Rischio reputazionale e legale, anche senza riscatto

MODULO 5: SICUREZZA DEGLI ACCESSI — LA DIFESA PRATICA

5.1 Password e credenziali

- Password sicure e password manager

5.2 Autenticazione a più fattori

- MFA: come funziona e perché è indispensabile
- MFA fatigue: notifiche a raffica che puntano sulla stanchezza
- Passkey e biometria: il futuro è senza password

5.3 Quando qualcosa non torna: l'accesso compromesso

- Segnali da non ignorare: accessi insoliti, MFA non richiesto, sessioni sospette
- Cosa fare, in ordine: cambia password, chiudi le sessioni, segnala
- Nel dubbio, segnala comunque: meglio presto che troppo tardi

CONTATTI

info@nexsys.it

www.nexsys.it

CORSO CYBER SECURITY AWARENESS PER UTENTI AZIENDALI

Durata: 3,5 ore

NEXSYS
LEARN IT, TRANSFORM IT

OVERVIEW DEL CORSO

Il corso cyber security awareness di Nexsys è il percorso formativo aziendale pensato per istruire dipendenti e personale non tecnico sui rischi informatici quotidiani, aggiornato alle minacce più recenti generate dall'intelligenza artificiale. La causa non è quasi mai una falla tecnica: è un clic, una distrazione, una decisione presa troppo in fretta. Il nostro obiettivo è trasformare il personale da potenziale anello debole a prima linea di difesa attiva.

Antispam, MFA, EDR e policy tecniche riducono il rischio, ma non eliminano il punto in cui molte minacce diventano operative: la decisione della persona. Un clic su un link, l'apertura di un allegato, l'approvazione di una richiesta MFA non attesa o la fiducia in una voce o un volto che sembrano autentici possono trasformarsi in data breach, furto di credenziali, frode o blocco operativo.

Il corso Cyber Security Awareness Nexsys crea un livello di comportamento sicuro per tutta l'organizzazione, con linguaggio chiaro, casi pratici aggiornati al 2026 e riferimenti concreti alla vita lavorativa quotidiana. Un elemento centrale è la cultura no-blame: segnalare subito un errore o un dubbio, senza paura, perché è la velocità della segnalazione a fare la differenza tra un incidente contenuto e un danno serio.

A CHI È RIVOLTO IL CORSO?

La nostra formazione è indirizzata ad aziende, enti e professionisti ed è calibrata per:

- Dipendenti e collaboratori di tutti i reparti aziendali (Amministrazione, HR, Sales, Marketing)
- Titolari d'azienda e liberi professionisti
- Figure manageriali e Responsabili di area che gestiscono dati sensibili

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Riconoscere i segnali di un attacco: email, link, allegati, QR code e pagine di login sospette.
- Capire come funzionano phishing, smishing, vishing, quishing, ransomware e social engineering, anche nella versione potenziata dall'AI generativa.
- Riconoscere deepfake vocali e video e sapere che "sembra vero" non è più una prova sufficiente.
- Gestire password, MFA e dispositivi aziendali con maggiore consapevolezza, incluse passkey e biometria.
- Distinguere urgenze reali da pressioni manipolative usate dagli attaccanti.
- Sapere quando fermarsi, verificare su un secondo canale indipendente e segnalare un evento sospetto, senza paura di sbagliare.
- Riconoscere i segnali di un accesso compromesso e sapere come reagire, in ordine.

CONTATTI

info@nexsys.it

www.nexsys.it