

28-31/3/2025

Modulo 5 - IT Security

Valerio Catullo

Formatore



Concetti Fondamentali della Sicurezza IT

- Comprendere la terminologia di base relativa alla sicurezza informatica e all'hacking".
- Riconoscere le minacce alla sicurezza dei dati provocate da singoli individui, fornitori di servizi e organizzazioni esterne.
- Essere consapevoli delle minacce ai dati provocate da circostanze straordinarie come incendi, inondazioni, guerre e terrorismo Riconoscere le minacce ai dati provocate dall'uso del cloud computing, con particolare attenzione alla potenziale perdita di riservatezza (privacy).
- Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità e disponibilità (C.I.A. triad o C.I.D. in italiano).
- Comprendere i motivi per proteggere le informazioni personali e di lavoro.
- Identificare i principi comuni per la protezione, la conservazione e il controllo dei dati e della riservatezza, inclusi i concetti di trasparenza, legittimità, proporzionalità e conservazione.
- Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT e come fare per ottenerle.

Il Mondo del Malware

- Comprendere il termine "malware" e riconoscere i diversi modi con cui il malware si può nascondere.
- Riconoscere i diversi tipi di malware infettivo e comprenderne come funzionano, come virus, worm e trojan.
- Riconoscere i tipi di malware che mirano al guadagno economico, come spyware, adware, keylogger e dialer.
- Comprendere come funziona il software antivirus e quali limitazioni presenta nella protezione totale.
- Riconoscere che il software anti-virus dovrebbe essere installato su tutti i sistemi informatici e mantenuto aggiornato.
- Comprendere il termine "quarantena" e l'operazione di mettere in quarantena file infetti/sospetti da parte del software antivirus.
- Utilizzo di risorse online per la diagnostica e la risoluzione di un attacco malware.

Fondamenti di Sicurezza nella Rete

- Comprendere il termine "rete" e riconoscere i più comuni tipi di rete, come LAN (rete locale), WLAN (rete locale wireless), WAN (rete geografica) e VPN (rete privata virtuale).
- Comprendere la connessione di una rete e le implicazioni di sicurezza, inclusi i rischi di accessi non autorizzati e vulnerabilità.
- Comprendere il ruolo dell'amministratore di rete nella gestione degli account utente e nell'assegnazione/revoca delle autorizzazioni, assicurando il rispetto delle politiche di sicurezza, del traffico di rete e del trattamento del malware rilevato sulla sua rete.
- Comprendere la funzione e i limiti di un firewall in ambiente personale e lavorativo.

Firewall, Sicurezza Wireless e Hotspot

- Attivare e disattivare un firewall personale e comprendere come bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.
- Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) e WPA2 (Wi-Fi Protected Access 2), il filtraggio MAC (Media Access Control) e l'SSID (Service Set Identifier).
- Essere consapevoli che una rete wireless non protetta si va incontro ad abusi, violazioni di comunicazioni private (man in the middle).
- Comprendere l'importanza di aggiornare regolarmente i vari tipi di software, quali antivirus, browser web, plug-in, applicazioni e sistema operativo.
- Comprendere il termine "hotspot personale" e come attivare e disattivare un hotspot personale sicuro, connettersi in modo sicuro e disconnettersi da dispositivi informatici.

Controllo degli Accessi e One-Time Password

- Identificare i metodi per impedire accessi non autorizzati ai dati, come l'autenticazione basata su password, PIN e biometria.
- Comprendere il termine "one-time password" ed il suo utilizzo tipico per una singola transazione o sessione di lavoro.
- Comprendere lo scopo di un account di rete e l'importanza di proteggere le credenziali di accesso (nome utente e password).
- Accesso alla rete con nome utente e password, e blocco dell'account quando non viene usato.

Tecniche Biometriche e Gestione delle Password

- Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, come la scansione della retina, il riconoscimento facciale e la geometria della mano.
- Riconoscere come rendere sicura la propria password, seguendo buone pratiche come l'utilizzo di password complesse e la loro gestione riservata.
- Comprendere le funzioni e le limitazioni dei software di gestione delle password (password manager) per memorizzare e generare password sicure.

Uso Sicuro del Web e Phishing

- Completamento automatico e salvataggio automatico nella compilazione di un modulo web e le relative implicazioni per la sicurezza.
- Eliminare i dati privati dal browser, come la cronologia di navigazione, i cookie e le password salvate.
- Utilizzare una connessione di rete sicura per le attività in rete, prestando attenzione al protocollo HTTPS e al lucchetto nel browser.
- Identificare le modalità con cui confermare l'autenticità di un sito web, quali la verifica del certificato di sicurezza.
- Comprendere il termine "pharming" come una tecnica di reindirizzamento fraudolento verso siti web dannosi.

Comunicazioni Elettroniche Sicure e Minacce Email

- Cifrare e decifrare un messaggio di posta elettronica utilizzando la firma digitale per garantire autenticità e integrità.
- La firma digitale (o "firma elettronica qualificata") e il suo valore legale.
- Identificare i possibili messaggi fraudolenti e indesiderati (phishing), riconoscendone le caratteristiche tipiche come richieste urgenti di dati personali, errori grammaticali e link sospetti.
- Essere consapevoli dei rischi di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.

Sicurezza sui Social Media e Dispositivi Mobili

- I più comuni modi per assicurare la sicurezza fisica di computer e dispositivi mobili, inclusa la protezione da furto e smarrimento.
- Effettuare copie di sicurezza (backup) per ovviare alla perdita di dati da computer e dispositivi mobili, comprendendone l'importanza e le diverse tipologie (completo, incrementale, differenziale).
- Comprendere le implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali e i rischi associati alle autorizzazioni richieste dalle app.
- Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, come il blocco da remoto e la cancellazione dei dati.
- Applicare le impostazioni di privacy ai propri account di reti sociali per limitare la visibilità delle informazioni.
- Comprendere i potenziali pericoli connessi all'uso di siti di reti sociali, come il cyberbullismo e il furto di identità.

Gestione Sicura dei Dati e Rimozione

- Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, inclusa la protezione da accessi non autorizzati.
- Effettuare la copia di sicurezza dei dati su un supporto quale unità disco/dispositivo locale, unità esterna, servizio su cloud.
- Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna o servizio su cloud.
- Distinguere tra cancellare i dati ed eliminarli in modo permanente, comprendendo che la semplice cancellazione non è sufficiente per la sicurezza.
- Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili, soprattutto in caso di smaltimento o cessione.
- Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente e verificare le politiche del fornitore.
- Identificare i metodi più comuni per distruggere i dati in modo permanente, come l'uso di software di data wiping o la distruzione fisica dei supporti.



GRAZIE PER L'ATTENZIONE!

EDUCATION.MRDIGITAL.IT

Via Liguria 76/78 - 20025 Legnano (MI)

Email formazione@mrdigital.it

