CAPITOLO 9 – SICUREZZA INFORMATICA E PROTEZIONE DEI DATI

Obiettivi del capitolo

Al termine di questo capitolo il corsista sarà in grado di:

- Comprendere l'importanza della sicurezza informatica.
- Identificare le principali minacce digitali.
- Adottare comportamenti sicuri nell'utilizzo di computer e dispositivi mobili.
- Creare e gestire password efficaci.
- Proteggere i propri dati personali.
- Riconoscere tentativi di phishing e truffe online.
- Comprendere il concetto di backup.
- Applicare le principali misure di prevenzione contro la perdita di dati.

9.1 Introduzione alla sicurezza informatica

La sicurezza informatica comprende l'insieme delle tecniche, delle tecnologie e dei comportamenti utilizzati per proteggere:

- Dispositivi
- Dati
- Account
- Reti
- Informazioni personali

Negli ultimi anni la digitalizzazione delle attività quotidiane ha aumentato notevolmente l'esposizione ai rischi informatici.

Oggi utilizziamo strumenti digitali per:

- Operazioni bancarie
- Acquisti online
- Comunicazioni personali
- Lavoro
- Gestione documentale

La protezione delle informazioni è quindi diventata una competenza fondamentale.

9.2 Perché la sicurezza informatica è importante

Molte persone ritengono di non essere obiettivi interessanti per i criminali informatici.

In realtà qualsiasi utente può essere vittima di:

- Furto di password
- Furto di identità
- Truffe economiche
- Perdita di documenti
- Accessi non autorizzati

Le conseguenze possono includere:

- Perdite finanziarie
- Violazioni della privacy
- Danni reputazionali
- Interruzione delle attività lavorative

La sicurezza informatica non riguarda soltanto le grandi aziende ma ogni singolo cittadino.

9.3 I principi fondamentali della sicurezza

La sicurezza informatica si basa su tre principi fondamentali.

Riservatezza (Confidentiality)

Le informazioni devono essere accessibili soltanto alle persone autorizzate.

Esempio

Le credenziali bancarie non devono essere visibili ad altri utenti.

Integrità (Integrity)

I dati devono mantenere la propria correttezza e completezza.

Esempio

Un documento non deve essere modificato da persone non autorizzate.

Disponibilità (Availability)

Le informazioni devono essere accessibili quando necessario.

Esempio

I documenti aziendali devono essere disponibili anche dopo un guasto tecnico.

9.4 Le principali minacce informatiche

Le minacce possono assumere molte forme diverse.

9.5 Malware

Il termine malware deriva dall'espressione inglese:

Malicious Software

ovvero software dannoso.

Si tratta di programmi progettati per causare danni o ottenere accessi non autorizzati.

Tipologie principali

Virus

Si diffondono infettando file e programmi.

Possono:

- Danneggiare dati

- Alterare il sistema
- Rallentare il computer

Worm

Si propagano automaticamente attraverso le reti.

Non richiedono necessariamente l'intervento dell'utente.

Trojan

Si presentano come software legittimi.

Una volta installati possono:

- Rubare informazioni
- Aprire accessi remoti
- Compromettere il dispositivo

Spyware

Raccolgono informazioni sulle attività dell'utente.

Possono monitorare:

- Navigazione web
- Credenziali
- Dati personali

Adware

Visualizzano pubblicità indesiderata.

Possono rallentare il sistema e compromettere l'esperienza d'uso.

9.6 Ransomware

Il ransomware è una delle minacce più pericolose.

Questi programmi:

1. Cifrano i dati della vittima.
2. Rendono i file inutilizzabili.
3. Richiedono un riscatto economico per il ripristino.

Conseguenze

- Perdita di documenti.
- Interruzione delle attività.
- Danni economici.

Prevenzione

- Backup regolari.
- Aggiornamenti costanti.
- Attenzione agli allegati email.

9.7 Phishing

Il phishing è una tecnica di ingegneria sociale utilizzata per ingannare gli utenti.

L'obiettivo è ottenere:

- Password
- Codici di accesso
- Dati bancari
- Informazioni personali

Come funziona

L'utente riceve una comunicazione apparentemente proveniente da:

- Banca
- Corriere
- Ente pubblico
- Provider di servizi

Il messaggio invita a cliccare un link o inserire credenziali.

Esempio tipico

"Il tuo conto è stato bloccato. Accedi immediatamente per verificare la tua identità."

Segnali di allarme

- Tono urgente o minaccioso.
- Errori grammaticali.
- Mittente sospetto.
- Link insoliti.
- Richiesta di dati riservati.

9.8 Ingegneria sociale

Molti attacchi informatici non sfruttano vulnerabilità tecniche ma comportamenti umani.

L'ingegneria sociale consiste nel manipolare le persone per ottenere informazioni.

Esempi

Telefonata fraudolenta

Un finto operatore richiede password o codici.

Finto tecnico informatico

Chiede accesso remoto al computer.

Finta assistenza bancaria

Invita a comunicare codici di sicurezza.

Regola fondamentale

Non comunicare mai password o codici di autenticazione.

9.9 Le password

Le password rappresentano la prima linea di difesa degli account.

Caratteristiche di una password sicura

Una buona password dovrebbe contenere:

- Almeno 12 caratteri
- Lettere maiuscole
- Lettere minuscole
- Numeri
- Simboli

Esempio corretto

Mio!Corso2026#Digitale

Esempi da evitare

123456

password

qwerty

mario123

9.10 Errori comuni nella gestione delle password

Riutilizzare la stessa password

Se un account viene compromesso, tutti gli altri diventano vulnerabili.

Annotare le password in luoghi visibili

Post-it sul monitor o fogli non protetti rappresentano un rischio.

Condividere le credenziali

Le credenziali devono rimanere personali.

9.11 Password manager

I password manager sono applicazioni che archiviano in modo sicuro le credenziali.

Vantaggi

- Password uniche per ogni servizio.
- Maggiore sicurezza.
- Accesso rapido.

Limiti

È fondamentale proteggere adeguatamente la password principale.

9.12 Autenticazione a due fattori (2FA)

La sola password spesso non è sufficiente.

Per questo molti servizi utilizzano la verifica a due fattori.

Come funziona

Dopo la password viene richiesto un secondo elemento:

- Codice SMS
- Applicazione autenticatrice
- Dispositivo fisico di sicurezza

Vantaggi

Anche conoscendo la password, un attaccante non può accedere facilmente all'account.

9.13 Aggiornamenti software

Gli aggiornamenti correggono vulnerabilità e problemi di sicurezza.

Perché sono importanti

I criminali informatici cercano spesso di sfruttare difetti noti.

Un software non aggiornato è più vulnerabile.

Cosa aggiornare

- Sistema operativo
- Browser
- Antivirus
- Applicazioni

9.14 Antivirus e antimalware

Gli antivirus aiutano a individuare e bloccare software dannosi.

Funzioni principali

- Scansione dei file.
- Monitoraggio in tempo reale.
- Rilevamento delle minacce.

Limiti

Nessun antivirus garantisce una protezione assoluta.

Il comportamento dell'utente rimane fondamentale.

9.15 Backup dei dati

Il backup consiste nella creazione di copie di sicurezza dei dati.

Perché è importante

I dati possono essere persi a causa di:

- Guasti hardware
- Errori umani
- Virus
- Furti
- Eventi accidentali

9.16 Tipologie di backup

Backup locale

Salvataggio su:

- Hard disk esterno
- SSD esterno
- Chiavetta USB

Backup cloud

Salvataggio su servizi online.

Vantaggi:

- Accessibilità
- Protezione da danni fisici

9.17 La regola 3-2-1

Una delle migliori pratiche di sicurezza prevede:

- 3 copie dei dati
- 2 supporti differenti
- 1 copia conservata in luogo diverso

Esempio

- Computer principale
- Disco esterno
- Servizio cloud

9.18 Sicurezza nella navigazione web

Quando si utilizza Internet è importante adottare alcune precauzioni.

Verificare HTTPS

I siti che raccolgono dati personali devono utilizzare connessioni protette.

Evitare download sospetti

Scaricare software solo da fonti affidabili.

Controllare i link

Prima di cliccare verificare attentamente l'indirizzo.

9.19 Sicurezza sui social network

I social media contengono molte informazioni personali.

Rischi

- Furto d'identità.
- Profilazione.
- Truffe.
- Diffusione di informazioni personali.

Buone pratiche

- Limitare le informazioni pubbliche.
- Utilizzare password robuste.
- Attivare l'autenticazione a due fattori.

9.20 Protezione dei dati personali

I dati personali rappresentano una risorsa di grande valore.

Tra questi troviamo:

- Nome e cognome
- Codice fiscale
- Numero di telefono
- Indirizzo
- Dati bancari
- Documenti di identità

Principi di protezione

Condividere soltanto le informazioni strettamente necessarie.

Verificare sempre chi richiede i dati e per quale motivo.

9.21 Sicurezza dei dispositivi mobili

Anche smartphone e tablet devono essere protetti.

Misure consigliate

- PIN o password.
- Blocco biometrico.
- Aggiornamenti automatici.
- Installazione app da store ufficiali.

9.22 Cosa fare in caso di incidente

Se si sospetta una compromissione:

1. Scollegare il dispositivo dalla rete.
2. Modificare immediatamente le password.

3. Eseguire una scansione antivirus.
4. Informare l'assistenza tecnica.
5. Verificare eventuali accessi non autorizzati.

La rapidità di intervento può limitare notevolmente i danni.

Caso pratico: email sospetta

Un utente riceve un messaggio apparentemente inviato dalla banca.

Il testo richiede di cliccare un link per evitare il blocco del conto.

Analisi:

- Linguaggio urgente.
- Mittente insolito.
- Link differente dal sito ufficiale.

Conclusione:

Probabile tentativo di phishing.

Comportamento corretto:

- Non cliccare il link.
- Eliminare il messaggio.
- Contattare direttamente la banca tramite canali ufficiali.

Riepilogo del capitolo

In questo capitolo abbiamo studiato:

- I principi fondamentali della sicurezza informatica.
- Malware e ransomware.
- Phishing e ingegneria sociale.
- Password e autenticazione a due fattori.
- Aggiornamenti software.
- Antivirus.
- Backup dei dati.
- Protezione della privacy.
- Sicurezza nella navigazione web e sui dispositivi mobili.

Esercitazioni pratiche

Esercizio 1

Valutare la robustezza di alcune password di esempio.

Esercizio 2

Analizzare email reali o simulate per individuare possibili tentativi di phishing.

Esercizio 3

Attivare l'autenticazione a due fattori su un account personale.

Esercizio 4

Verificare la presenza di aggiornamenti sul proprio dispositivo.

Esercizio 5

Creare una strategia di backup personale seguendo la regola 3-2-1.

Quiz di autovalutazione

1. Quali sono i tre principi fondamentali della sicurezza informatica?
2. Che differenza esiste tra virus e ransomware?
3. Che cos'è il phishing?
4. Quali caratteristiche deve avere una password sicura?
5. A cosa serve l'autenticazione a due fattori?
6. Perché gli aggiornamenti sono importanti?
7. Cos'è un backup?
8. In cosa consiste la regola 3-2-1?
9. Quali rischi esistono sui social network?

10. Quali azioni intraprendere in caso di sospetta compromissione di un account?

Risposte sintetiche

1. Riservatezza, integrità e disponibilità.
2. Il virus infetta file e programmi, il ransomware cifra i dati chiedendo un riscatto.
3. Una truffa che mira a sottrarre informazioni tramite inganno.
4. Deve essere lunga, complessa e unica.
5. Aggiungere un ulteriore livello di sicurezza oltre alla password.
6. Correggono vulnerabilità e migliorano la protezione.
7. Una copia di sicurezza dei dati.
8. Tre copie dei dati, due supporti diversi, una copia esterna.
9. Furto d'identità, truffe e violazioni della privacy.
10. Cambiare password, verificare gli accessi, effettuare controlli di sicurezza e contattare l'assistenza se necessario.