I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

PREVENZIONE AL CONTRASTO DEI FENOMENI DI CYBERBULLISMO DI CUI ALLA LEGGE 71/2017

GHOST ENEMY

I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

Cyber Security (protezione dei dati e della privacy)

- Cyber security: cos'è e perché è importante?
- Privacy vs protezione dati personali: attenti alla differenza
- Diritto di accedere ai propri dati personali.
- Diritto alla rettifica, alla cancellazione, alla limitazione del trattamento, alla portabilità dei dati personali.

I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

Cyber security cos'è e perché è importante?

La cybersecurity è la pratica che consiste nel *difendere i computer e i server, i dispositivi mobili, i sistemi elettronici, network e dati da attacchi pericolosi.* È anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche. Il termine abbraccia un ampio raggio di settori e si applica a qualunque cosa: dalla sicurezza dei computer al ripristino di emergenza e all'istruzione degli utenti finali

Le minacce che la cybersecurity cerca di contrastare hanno una triplice natura: il *Cybercrimine*, che include singoli attori o gruppi che attaccano i sistemi per un guadagno economico, *la guerra cibernetica*, che spesso comprende la raccolta di informazioni per fini politici e infine *il cyberterrorismo*, intento a minare i sistemi informatici per scatenare il panico o il terrore.

Primario obiettivo della sicurezza informatica è quello di proteggere reti, computer, programmi e dati da possibili attacchi o accessi non autorizzati, per evitare che questi provochino danni sulla reputazione di aziende o sull'economia.

Modalità di Attacchi Informatici?

Gli attacchi "comuni", campagne di phishing e diffusione di malware e minacce derivate da dipendenti senza grosse competenze, sono la causa di un aumento incontrollato delle vulnerabilità delle aziende.

Gli attacchi "avanzati", particolarmente sofisticati, fanno leva sull'inefficacia o inadeguatezza dei sistemi di sicurezza per aprirsi un varco nei sistemi IT aziendali.

Gli attacchi "emergenti" sono quelli che destano più preoccupazione. Si tratta di attacchi più articolati e imprevedibili che sfruttano i dispositivi interconnessi e gli oggetti smart, scovando le vulnerabilità poco note delle nuove tecnologie IoT per infiltrarsi nelle organizzazioni creando danni ingenti.

I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

Cybersecurity: Consigli per non finire in trappola

- **Aggiornare software**. Una buona politica di cybersecurity prevede l'aggiornamento di tutti i software alle ultime versioni consigliate dal produttore. La presenza di dispositivi e software che non sono più aggiornabili mette in pericolo la sicurezza delle reti informatiche.
- **Diversificare le password**. Bisogna prestare grande attenzione alle password. Ogni account deve averne una diversa dall'altra.
- **Autenticare in due step.** Sempre restando nel campo delle password, una strategia efficace nella cyber security è quella dell'autenticazione a due fattori, soprattutto per l'accesso alla posta o altri gestionali dell'azienda.
- **Creare password complesse**. Una password efficace è quella composta da almeno otto caratteri con un misto di numeri e lettere, in maiuscolo e minuscolo. Importante è non inserire all'interno informazioni personali

I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

Non lasciare password in giro. Anche se questa potrebbe sembrare una banalità ci sono ancora tante persone che hanno l'abitudine di scrivere le password su foglietti attaccati al pc.

- **Non condividere dati delicati all'esterno**. I criminali informatici reperiscono molti dei dati che utilizzano per violare sistemi proprio sui social network.
- **Non aprire link nelle email.** Quello dei link è uno dei metodi più usati dagli hacker per infettare pc e dispositivi. Se non si è sicuri su un link, non bisogna cliccarci.
- **Non cliccare sui pop up.** Anche i pop up possono essere usati dai criminali informatici per infettare i dispositivi. Inserire un ad blocker può evitare di esporsi a rischi.

I.S.I.S. ENRICO CARUSO Napoli

Ministero dell'Istruzione, dell'Università e della Ricerca

MIUR

REGIONE CAMPANIA

Fare acquisti solo su siti sicuri. Anche se non sono esenti da eventuali attacchi, meglio usare piattaforme affidabili per fare acquisti online che siti che ad esempio, fanno offerte e sconti "miracolosi".

- **Controllare i post sui social media**. Facebook, Twitter, LinkedIn, come Instagram, sono degli strumenti che gli hacker usano per reperire informazioni utili e avviare degli attacchi. Gli esperti di cyber security consigliano di rivedere i post pubblicati sui social e fare attenzione a che non contengano alcuna informazione personale.