



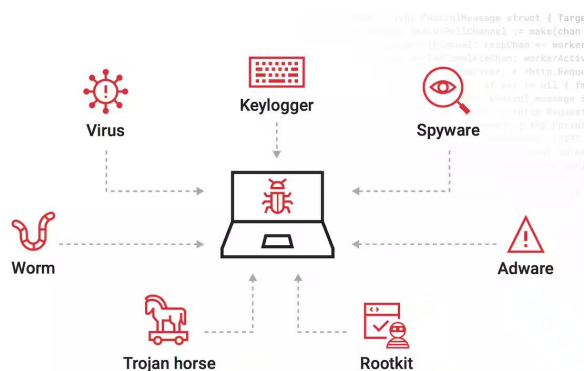
# CYBER SECURITY

Lorenzo Lega,  
Lorenzo Mangia,  
Marco Marasco

# Cos'è la sicurezza informatica o cybersecurity?

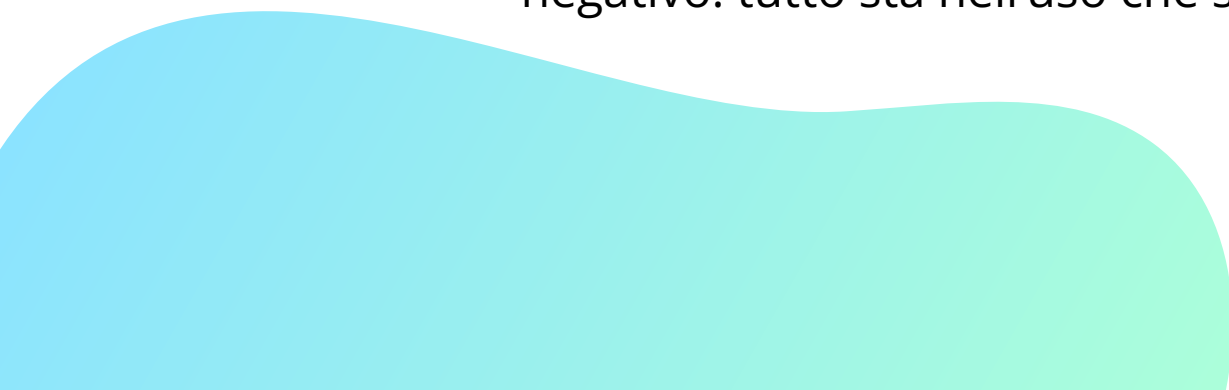
La (o cybersecurity) è l'insieme di misure tecniche, organizzative e comportamentali finalizzate a proteggere sistemi informatici, reti e informazioni e dati sensibili.

Si tratta di strumenti utili anche a proteggere le persone da malware, phishing, spyware e moltissimi altri attacchi usati dagli hacker black hat per rubare dati



# Cos'è un Hacker e come si classificano?

Un hacker è una persona che è molto ferrata in materia di informatica e di reti, che è in grado di esplorare, modificare o approfittare dei sistemi informatici, del software e dei protocolli, magari trovando delle falle nei sistemi. Tuttavia, non sempre la parola "hacker" è da intendersi con un senso negativo: tutto sta nell'uso che se ne fa.



# Gli hacker si classificano in:

## White Hat:

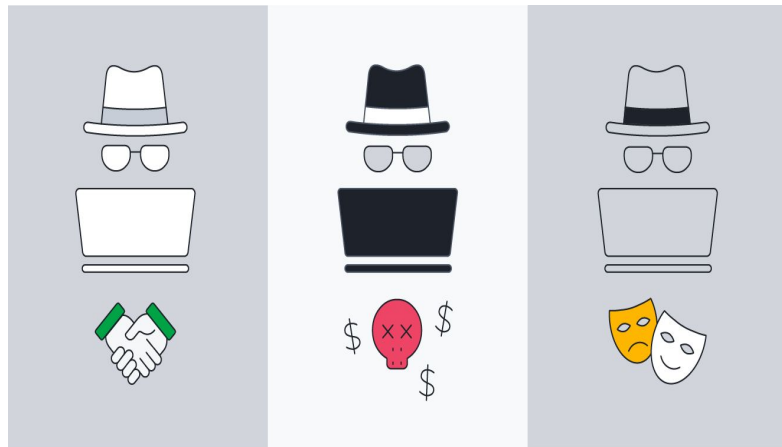
sono hacker etici e aiutano le aziende.  
Eseguono test di penetrazione (penetration test) per trovare falle nei sistemi.

## Black Hat:

Sono criminali informatici e sfruttano le vulnerabilità al fine di rubare dati sensibili

## Grey Hat:

Sono una via di mezzo.  
Agiscono senza autorizzazione, ma non sempre con scopi dannosi.  
Possono segnalare falle di sicurezza scoperte per "giustizia etica", ma senza seguire i canali ufficiali.



# Le Minacce informatiche

Nel mondo digitale in cui viviamo, ogni nostra azione online può esporci a rischi. Le minacce informatiche sono pericoli reali e in continua evoluzione, capaci di colpire non solo aziende e istituzioni, ma anche singoli utenti.

Questi attacchi possono rubare informazioni personali, bloccare l'accesso ai nostri dati o addirittura causare danni economici. Spesso si presentano in modo subdolo e perciò è necessario conoscerle e sapersi difendere

# Quali sono i più conosciuti tipi di minaccia informatica?

## 1. Malware

Include virus, worm, trojan, spyware e ransomware.

lo scopo infettare il dispositivo, rubare informazioni o bloccare l'accesso ai dati.

Ad esempio, un ransomware cifra tutti i file dell'utente e chiede un riscatto per sbloccarli.

## 2. Phishing

Tecnica di ingegneria sociale per ingannare l'utente e ottenere dati sensibili.

Si presenta come email o messaggio finto

Ad esempio, cliccare su un link fasullo che porta a un sito clone per rubare credenziali.

## 3. Furto di identità digitale

Consiste nell'uso illecito di dati personali per accedere a conti, fare acquisti o commettere reati.

Spesso avviene tramite phishing o database violati.

Ad esempio, qualcuno usa le tue credenziali per entrare nella tua email o nel tuo home banking.



# Quali sono i più conosciuti tipi di minaccia informatica?

## 4. Spyware e keyLogger

Spyware e Keylogger sono Software nascosti che registrano le attività dell'utente (inclusi tasti premuti e password).

Utilizzati per spiare comportamenti o rubare informazioni.

Ad esempio un keylogger registra ogni cosa digitata sulla tastiera, inclusi PIN e credenziali.

## 5. SQL Injection e Exploit di vulnerabilità

Attacchi tecnici che sfruttano errori di programmazione nei siti o nei software e quindi, possono permettere a un hacker di ottenere l'accesso non autorizzato a dati o funzionalità riservate.



# Come ci si difende da queste minacce?

Il primo passo è usare password forti, lunghe e difficili da indovinare. È importante non usare la stessa password su più siti e, quando possibile, attivare l'autenticazione a due fattori: un sistema che richiede un secondo codice di verifica oltre alla password, rendendo molto più difficile l'accesso non autorizzato. Anche aggiornare regolarmente il proprio dispositivo e i software è una difesa fondamentale. Gli aggiornamenti non servono solo a migliorare le funzionalità, ma spesso correggono falle di sicurezza che potrebbero essere sfruttate dagli hacker. Lo stesso vale per l'antivirus, che deve essere sempre attivo e aggiornato.

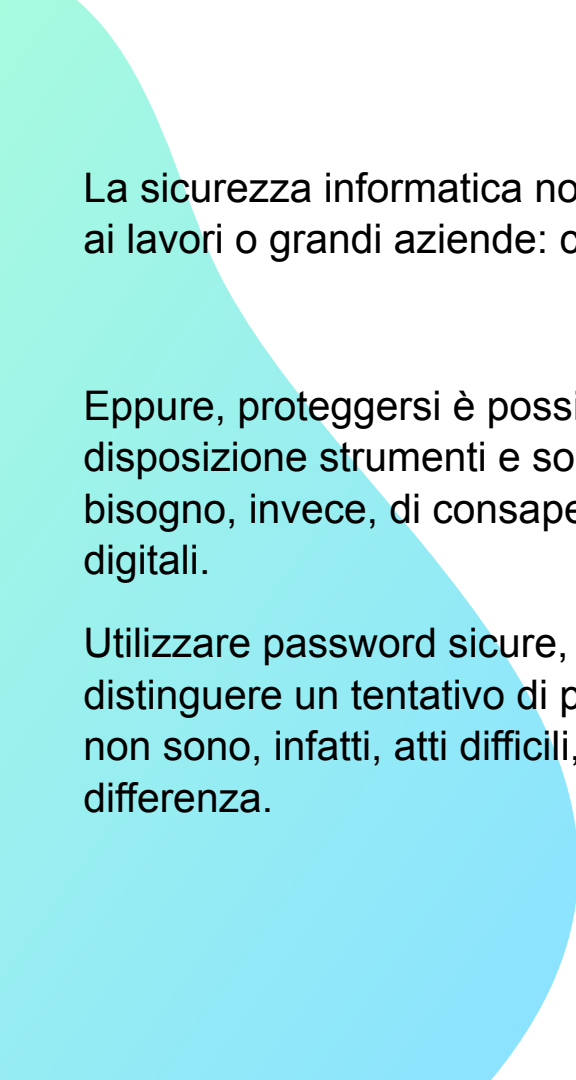




# Come ci si difende da queste minacce?

Una delle minacce più diffuse è il phishing, ovvero quei messaggi (email, sms, messaggi su social) che cercano di ingannare l'utente con link falsi o allegati pericolosi. È importante prestare attenzione: non cliccare su link sospetti, verificare sempre il mittente e non fornire mai i propri dati personali a cuor leggero. Quando si naviga, meglio farlo in modo sicuro: usare solo connessioni https, evitare le reti wi-fi pubbliche per operazioni delicate (come accedere alla banca online) e controllare sempre l'indirizzo dei siti. Un'altra buona abitudine è fare backup regolari dei dati importanti, su supporti fisici o in cloud. In caso di attacco ransomware o guasto del computer, potrai recuperarli senza perdite.





La sicurezza informatica non è un argomento soltanto per addetti ai lavori o grandi aziende: ci riguarda tutti, ogni giorno.

Eppure, proteggersi è possibile, e non è necessario avere a disposizione strumenti e soluzioni particolarmente complessi: c'è bisogno, invece, di consapevolezza, attenzione e buone abitudini digitali.

Utilizzare password sicure, aggiornare i propri dispositivi, saper distinguere un tentativo di phishing, fare regolarmente i backup non sono, infatti, atti difficili, ma che possono fare una grande differenza.