MIM
Ministero dell'Istruzione
e del Merito

SICURNAUTI
LA TUA GUIDA NELLA GALASSIA DIGITALE



LA SICUREZZA INFORMATICA

www.unica.istruzione.gov.it

INDICE DEI CONTENUTI

1 INTRODUZIONE: COS'È LA SICUREZZA INFORMATICA 3

2 L'IMPORTANZA DELLA CONSAPEVOLEZZA DEI RISCHI: IL RUOLO DEI DOCENTI 3

3 CHI SONO GLI *HACKER* 4

4 ATTACCHI INFORMATICI E VULNERABILITÀ NEL MONDO DELL'ISTRUZIONE 6



1 INTRODUZIONE: COS'È LA SICUREZZA INFORMATICA

L'utilizzo sempre più diffuso delle tecnologie digitali ha modificato radicalmente il modo di vivere, lavorare e comunicare, permeando così in ogni aspetto della nostra società. Questa trasformazione, se da un lato offre significative opportunità, dall'altro ci espone a rischi considerevoli.
Ogni dispositivo elettronico e ogni piattaforma *online* possono essere vulnerabili a minacce informatiche che potrebbero mettere a rischio la sicurezza delle informazioni e la continuità delle attività quotidiane.

La sicurezza informatica non è più una prerogativa esclusiva di singole entità e di esperti di settore, ma rappresenta una **forma di responsabilità condivisa** da tutta la società.
La protezione delle infrastrutture digitali è fondamentale non solo per la sicurezza delle aziende ma per l'intera "infrastruttura sociale" costituita da aziende private ma anche da Istituzioni, scuole e soprattutto persone.

Ogni attacco informatico, infatti, non impatta soltanto su reti e sistemi informativi causandone malfunzionamenti o interruzioni ma mette a rischio anche la *privacy* degli utenti, l'economia, erode la fiducia nelle istituzioni, nelle tecnologie e può compromettere la stabilità e lo sviluppo delle comunità nel loro insieme.



2 L'IMPORTANZA DELLA CONSAPEVOLEZZA DEI RISCHI: IL RUOLO DEI DOCENTI

Nell'ottica di un coinvolgimento attivo da parte di tutti è fondamentale sviluppare una piena **consapevolezza del rischio informatico**, imparando a **riconoscere le minacce digitali** e **adottare comportamenti corretti** per prevenirle e mitigarle. Tali abilità devono diventare competenze trasversali essenziali richieste a chiunque, indipendentemente dal ruolo ricoperto o dal settore di appartenenza.

In questo percorso, i **docenti** e le **istituzioni scolastiche** rivestono **un ruolo centrale**: diffondere la cultura della cybersicurezza fin dall'età scolastica significa **formare cittadini digitalmente consapevoli**, capaci di agire con responsabilità e sicurezza nello spazio virtuale. Si tratta di un **investimento strategico per l'ecosistema digitale del futuro**, perché le abitudini e le competenze acquisite oggi costituiranno il fondamento di una società più resiliente e pronta ad affrontare le sfide della trasformazione digitale.

3 CHI SONO GLI *HACKER*

Per comprendere appieno l'importanza della consapevolezza e della diffusione di buone pratiche di sicurezza informatica, è necessario soffermarsi su chi opera dall'altra parte dello schermo: gli ***hacker***. La figura dell'*hacker*, inizialmente associata alla curiosità e al desiderio di esplorare i limiti delle tecnologie digitali, si è progressivamente trasformata e diversificata.

Oggi **il termine "*hacker*" identifica soggetti molti diversi tra loro**, la cui distinzione non è solo terminologica ma riflette approcci, obiettivi e impatti differenti. Originariamente, negli anni '50-'60 al *Massachusetts Institute of Technology* (MIT), il termine "*hacker*" indicava una soluzione ingegnosa e creativa a problemi tecnici. Con l'avvento dei *computer* negli anni '70-'80, si riferiva a chi sperimentava con *hardware* e *software* per comprenderne i segreti o migliorarne le funzionalità. Successivamente, i media hanno enfatizzato l'accezione negativa del termine, associandolo a chi viola sistemi agendo illegalmente.

Attualmente, è possibile distinguere **diverse tipologie di *hacker***:

- ***white hat***: **utilizzano competenze di *hacking* in modo etico**, su richiesta e con autorizzazione, per identificare e correggere vulnerabilità nei sistemi contribuendo a **migliorare la sicurezza aziendale**;

- ***gray hat***: operano in una zona grigia **tra etico e illecito**; individuano vulnerabilità senza permesso, talvolta le segnalano ma agiscono senza autorizzazione, spesso senza fini criminali;

- ***black hat***: sfruttano vulnerabilità di sistemi informatici senza permesso, con **intenzioni malevole** come furto di dati, estorsione o sabotaggio, agendo sempre in modo illegale.

In questa ambivalenza convivono creatività tecnica e uso illecito delle competenze; comprendere queste differenze è fondamentale per valutare rischi, comportamenti e strategie di difesa.



Le azioni dei *black hat* possono essere ulteriormente comprese analizzandone le motivazioni:

- **motivazioni economico-finanziarie (criminali informatici)**: gli *hacker* che agiscono per motivazioni economico-finanziarie sono comunemente definiti criminali informatici. Operano con finalità di profitto, conducendo attività quali estorsione, furto e rivendita di informazioni sensibili, frodi online, ecc. Si tratta spesso di gruppi strutturati, con modelli organizzativi simili a quelli della criminalità tradizionale;

- **motivazioni politiche (*state sponsored* o *nation-state*)**: gli *state-sponsored hacker* sono gruppi o individui che conducono attività informatiche offensive su incarico diretto o indiretto di uno Stato o governo. Questi attori sono dotati di elevate risorse, competenze avanzate e motivazioni strategiche. Le principali attività in cui questi attori sono coinvolti sono relative a spionaggio, sabotaggio e disinformazione;

- **motivazioni ideologiche / politiche (*hacktivisti*)**: gli *hacktivisti* utilizzano strumenti e tecniche proprie dell'*hacking* per sostenere cause politiche, sociali o ideologiche. Gli *hacktivisti*, malgrado siano convinti di agire per promuovere buone cause, mai per profitto, sono comunque da considerarsi al di fuori della legge.

La varietà di profili e motivazioni nel mondo degli *hacker* mette in luce la complessità delle minacce informatiche e degli attori coinvolti. Dai gruppi di criminali informatici agli attivisti digitali, fino agli attori sponsorizzati da Stati, le tecniche e gli obiettivi possono differire in modo significativo; tuttavia, la linea che separa questi attori è spesso più sottile di quanto si immagini.
In questo scenario, il settore scolastico rappresenta un bersaglio privilegiato per vari motivi:

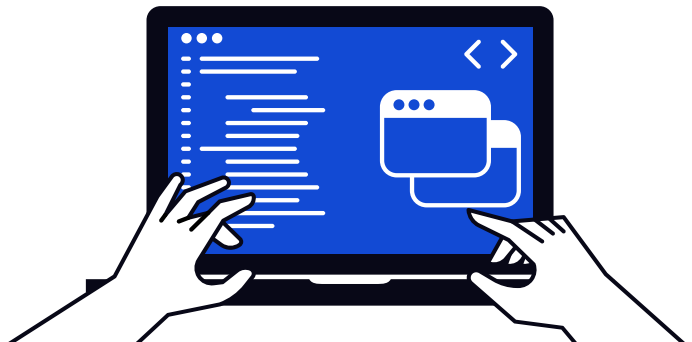
- **grandi volumi di dati sensibili**: le scuole raccolgono informazioni personali di studenti, insegnanti e famiglie, incluse informazioni sanitarie e finanziarie, dati preziosi che possono essere oggetto di furto d'identità e frodi;

- **infrastrutture spesso vulnerabili**: molte istituzioni scolastiche dispongono di sistemi di difesa non sempre aggiornati, con numerosissimi accessi da parte di famiglie, studenti e personale interno;

- **impatti su società e opinione pubblica**: attacchi alle scuole possono causare gravi disservizi, minare la fiducia pubblica nell'istituzione e diventare veicolo di protesta o propaganda ideologica per *hacktivisti* o nazioni ostili;

- **obiettivi geopolitici**: organizzazioni paragovernative possono mirare a destabilizzare governi e società colpendo i servizi pubblici, influenzare l'opinione pubblica con *fake news* o raccogliere informazioni strategiche.

Questi aspetti rendono il settore scolastico un *target* particolarmente attraente e vulnerabile, richiedendo un'attenzione specifica e urgente sulla sicurezza informatica nelle scuole.



4 ATTACCHI INFORMATICI E VULNERABILITÀ NEL MONDO DELL'ISTRUZIONE

All'inizio dell'anno scolastico 2024-2025, le scuole italiane si sono trovate ad affrontare uno scenario senza precedenti, caratterizzato da un incremento significativo di attacchi informatici mirati. Secondo i dati di *Check Point Research*, nel mese di settembre 2025 il settore dell'istruzione, oltre a risultare il più colpito a livello globale, ha registrato in media 4.175 attacchi informatici settimanali per organizzazione.

Tra le minacce più diffuse emergono le campagne di *phishing*, che nel solo mese di luglio hanno visto la creazione di oltre 18.000 nuovi domini associati *a* istituzioni scolastiche. Di questi, 1 su 57 è stato classificato come malevolo o sospetto. Alcuni attacchi hanno simulato credenziali istituzionali o documenti relativi a pagamenti, riuscendo a sottrarre dati sensibili appartenenti a docenti, studenti e personale amministrativo.

Questi dati delineano una realtà preoccupante, in cui il mondo della scuola si configura come uno dei bersagli privilegiati della criminalità informatica.

ATTACCHI REALI

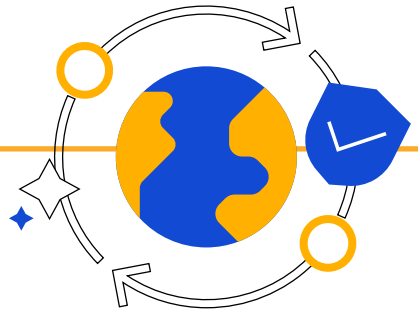
EVIDENZE DI ATTACCHI INFORMATICI NELLE SCUOLE

Maggio 2024 - Attacco informatico ad un Istituto Comprensivo della provincia di Venezia

Nella primavera del 2024 un Istituto della provincia di Venezia ha pubblicato sul proprio sito *internet* una comunicazione rivolta alla comunità scolastica, informando di aver subito un attacco informatico ai *server* della segreteria. Tale attacco ha comportato la sottrazione illecita e non autorizzata di documenti contenenti dati personali. Episodi di questa natura rientrano nella categoria di *data breach*: non si limitano ad interrompere i servizi, ma mirano a rubare e rivendere informazioni sensibili, quali elenchi di studenti, relazioni e verbali interni o comunicazioni amministrative.

Giugno 2024 - Attacco informatico ad un Istituto Tecnico nel Milanese

Nell'estate del 2024 un Istituto della città di Milano è stato vittima di un attacco *ransomware*. In questa tipologia di attacco, i criminali informatici riescono ad infiltrarsi nei sistemi informativi dell'ente e a crittografare *file* e archivi, rendendoli di fatto inaccessibili e potendo, inoltre, richiedere un riscatto economico per la decrittazione degli stessi. Tale attacco è stato ricondotto al Gruppo ElDorado ed ha comportato la pubblicazione di circa 40.50 GB di dati.





Intervento realizzato dal Ministero dell'Istruzione e del Merito e finanziato a valere sul Fondo per la gestione della cybersicurezza nell'ambito della misura 71 e 73 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Agenzia per la Cybersicurezza Nazionale

www.unica.istruzione.gov.it