I.I.S.S.
"GALLO"
AGRIGENTO

Erasmus+

LA CYBER SECURITY NELLE SCUOLE

Prof.ssa Adriana Cipolla
Prof.ssa Claudia Marcantonio
Prof.ssa Cristina Vindigni

CYBER SECURITY IN SCHOOLS

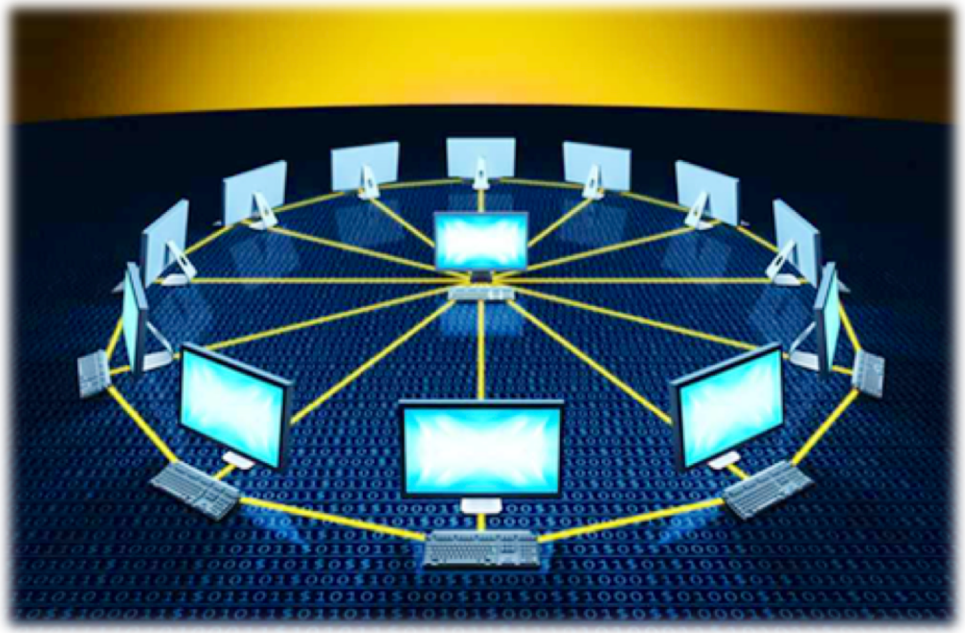
With the support of the Erasmus+ Programme of the European Union

eTwinning

IL NOSTRO SLOGAN

CYBERSECURITY IS A SHARED RESPONSABILITY: The more systems we secure, the more secure we all are!

COS'È LA CYBERSECURITY?



- La cybersecurity è un insieme di persone, processi e tecnologie che si fondono per proteggere le aziende, le persone o le reti dagli attacchi digitali.

- La cybersecurity è la prassi di proteggere i sistemi, le reti e i programmi dagli attacchi digitali. Questi attacchi informatici sono solitamente finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni sensibili, nonché all'estorsione di denaro agli utenti o all'interruzione dei normali processi aziendali.

- L'implementazione di misure di cybersecurity efficaci è particolarmente impegnativa oggi perché ci sono più dispositivi che persone e gli hacker stanno diventando sempre più innovativi

GUARDA UN ATTACCO INFORMATICO IN AZIONE

- HTTPS://WWW.CISCO.COM/C/IT_IT/PRODUCTS/SECURITY/WHAT-IS-CYBERSECURITY.HTML?SOCIALSHARE=VIDEO-BLADE-CYBERATTACK

DI COSA SI OCCUPA LA CYBERSECURITY?

- Un approccio di cybersecurity di successo ha diversi livelli di protezione distribuiti su computer, reti, programmi o dati che si intende mantenere al sicuro. In un'azienda, le persone, i processi e la tecnologia devono integrarsi a vicenda per creare una difesa efficace dagli attacchi informatici.
- Un sistema unificato di gestione delle minacce può accelerare le funzioni principali delle operazioni di sicurezza: rilevamento, indagine e correzione.

PERSONE

Gli utenti devono comprendere e rispettare i principi di sicurezza dei dati di base, come scegliere password complesse, diffidare degli allegati nelle e-mail e eseguire il backup dei dati.

PROCESSI

Le aziende devono avere un framework per il modo in cui trattano sia gli attacchi informatici tentati che quelli andati a buon fine.
Un framework largamente accettato può guidarti. Spiega come è possibile identificare gli attacchi, proteggere i sistemi, rilevare e rispondere alle minacce e recuperare dagli attacchi riusciti.

TECNOLOGIA

La tecnologia è essenziale per offrire alle aziende e agli individui gli strumenti di sicurezza informatici necessari per proteggersi dagli attacchi informatici. Tre entità principali devono essere protette: i dispositivi endpoint come computer, dispositivi intelligenti e router; nonché le reti e il cloud. La tecnologia comune utilizzata per proteggere queste entità include i firewall di nuova generazione, il filtro DNS, la protezione dal malware, il software antivirus e le soluzioni di sicurezza e-mail.

PERCHÉ LA CYBERSECURITY È IMPORTANTE?

Nel mondo connesso di oggi, tutti beneficiano di programmi di cyberdefense avanzati. A livello individuale, un attacco di cybersecurity può causare tutto, dal furto di identità, ai tentativi di estorsione, alla perdita di dati importanti come le foto di famiglia. Tutti si affidano a infrastrutture critiche come centrali elettriche, ospedali e aziende di servizi finanziari. Proteggere queste e altre aziende è essenziale per mantenere il funzionamento della nostra società.

TIPI DI MINACCE DI CYBERSECURITY

PHISHING

Il phishing è la prassi di inviare e-mail fraudolente che assomigliano a e-mail provenienti da fonti affidabili. L'obiettivo è quello di sottrarre dati sensibili come i numeri delle carte di credito e le informazioni di accesso. È il tipo di attacco informatico più diffuso. Puoi contribuire alla tua protezione attraverso l'istruzione o una soluzione tecnologica che filtra le e-mail dannose.

RANSOMWARE

- Il ransomware è un tipo di software dannoso. È progettato per estorcere denaro bloccando l'accesso ai file o al sistema informatico fino al pagamento del riscatto. Il pagamento del riscatto non garantisce che i file verranno recuperati o che il sistema venga ripristinato.

MALWARE

- Il malware è un tipo di software progettato per ottenere un accesso non autorizzato o per causare danni a un computer.

SOCIAL ENGINEERING

- Il social engineering è una tattica che gli hacker utilizzano per indurre l'utente a rivelare informazioni sensibili. Possono richiedere un pagamento in denaro oppure ottenere l'accesso ai dati riservati. Il social engineering può associarsi a una qualsiasi delle minacce elencate sopra per renderti più propenso a fare clic sui link, scaricare il malware o fidarti di una fonte malevola.