L'artigiano e

05
SEI

Sicurezza informatica

ArtigianImpresa
PILLOLE INFORMATIVE PER LE IMPRESE ARTIGIANE

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.

L'unico sistema veramente sicuro è quello spento, gettato in un blocco di cemento e sigillato in una stanza rivestita di piombo con delle guardie armate

Eugene Howard Spafford

Professore americano di informatica presso la Purdue University

CHE COS'È LA SICUREZZA INFORMATICA?

La sicurezza informatica (o cybersecurity) è l'insieme di pratiche, tecnologie e strategie volte a proteggere sistemi informatici, reti, dati e dispositivi digitali da accessi non autorizzati, danni, furti o attacchi informatici.

In un mondo sempre più connesso, dove informazioni personali, finanziarie e aziendali viaggiano online, la sicurezza dei dati è diventata una priorità strategica per individui, imprese e istituzioni.

FOCUS
PUNTI FORTI

Consigli pratici per rafforzare la propria sicurezza informatica:

› **Usare password sicure e uniche:** devono essere lunghe almeno 14 caratteri e contenere maiuscole, minuscole, numeri e simboli. Non devono essere utilizzate su più account

› **Attivare l'autenticazione a due fattori (2FA):** aggiunge un ulteriore livello di sicurezza oltre alla password, richiedendo un codice temporaneo o una conferma tramite app o SMS

› **Aggiornare regolarmente software e dispositivi**: gli aggiornamenti correggono vulnerabilità e migliorano la protezione contro malware e attacchi informatici

› **Fare attenzione a e-mail e messaggi sospetti:** non aprire link o allegati da mittenti sconosciuti e diffida di qualsiasi comunicazione che richieda dati personali o bancari

› **Navigare solo su siti sicuri:** controlla che l'indirizzo inizi con https:// e che sia presente il lucchetto accanto alla barra dell'indirizzo

› **Evitare reti Wi-Fi pubbliche per operazioni sensibili:** se necessario, utilizza una connessione protetta o una VPN

› **Effettuare backup periodici:** salva i dati importanti su dispositivi esterni o su cloud sicuri per poterli recuperare in caso di perdita o attacco informatico

› **Installare strumenti di sicurezza:** usa antivirus, firewall e filtri antispam aggiornati per proteggere il sistema da software dannosi

LINK UTILI
CONTENUTI ONLINE

APPROFONDIMENTI

› Cosa si intende per sicurezza informatica?

› Sicurezza informatica: principi e strumenti per proteggere dati e sistemi

› CIA Triad, o Triade CIA: cos'è e perché è importante

› Sicurezza informatica e GDPR: cosa c'è da sapere?

VIDEO

› Passwors: come vengono attaccate e come vengono protette

STRUMENTI UTILI

› 2FA e MFA: come funziona l'autenticazione a due o più fattori

› Dietro il mondo dei malware c'è un mercato illegale di dati: come evitare virus, trojan e worm

› Dovresti fidarti dei gestori di password nel 2025? | I gestori di password spiegati

› Come posso stare al sicuro online? 9 consigli per la tua sicurezza informatica

5 TIPOLOGIE DI ATTACCHI INFORMATICI

01

MALWARE (VIRUS, TROJAN, WORM):

software malevoli progettati per infiltrarsi nei sistemi informatici, danneggiare file o sottrarre dati sensibili. Possono diffondersi tramite allegati infetti, siti compromessi o dispositivi rimovibili

02

RANSOMWARE:

malware sofisticato che cripta file e dati dell'utente o dell'azienda, richiedendo un riscatto per ripristinarli

03

MAN-IN-THE-MIDDLE (MITM):

attacco in cui un criminale informatico intercetta e modifica le comunicazioni tra due parti senza che queste se ne accorgano

04

PHISHING:

messaggi (spesso e-mail o SMS) che imitano comunicazioni legittime per indurre l'utente a fornire credenziali, dati bancari o a cliccare link malevoli

05

ATTACCHI DDOS (DISTRIBUTED DENIAL-OF-SERVICE):

attacco che sovraccarica un server o una rete con traffico massiccio, rendendo il servizio lento o completamente non disponibile

SUGGESTIONI
NON DIMENTICARTI DI ...

La sicurezza informatica si fonda su tre principi fondamentali, noti come triade CIA:

RISERVATEZZA (CONFIDENTIALITY)
I dati devono essere accessibili solo a chi è autorizzato

DISPONIBILITÀ (AVAILABILITY)
I sistemi e i dati devono essere sempre accessibili quando necessarioes. promozioni, novità, scadenze

INTEGRITÀ (INTEGRITY)
Le informazioni non devono poter essere modificate o alterate

CASE STUDY
UNA CAMPAGNA DI SUCCESSO

2014 - Godzilla Attack! Turn Back!

Nella notte del 14 maggio 2014, **alcuni cartelli elettronici stradali a San Francisco sono stati violati da ignoti hacker.** Al posto dei normali messaggi di viabilità, destinati a informare gli automobilisti in occasione della corsa cittadina "Bay to Breakers", sui pannelli apparvero le scritte "Godzilla Attack!" e "Turn Back!".

L'episodio fu classificato come un **atto di hacking** a scopo goliardico, ma mise in luce gravi vulnerabilità nei sistemi di segnalazione elettronica delle infrastrutture urbane.

01
Cos’è l’IA

02
Creare testi con l’IA

03
Privacy Policy

04
Cookies Policy

05

06
Shop online