CAMERA DI COMMERCIO MONTE ROSA LAGHI ALTO PIEMONTE
punto impresa digitale

NOTIZIE DIGITALI

PID - Punto Impresa Digitale / #01 - 03.2022

FOCUS 4.0

La CYBERSECURITY:

lo Human Factor come strategia difensiva per le PMI

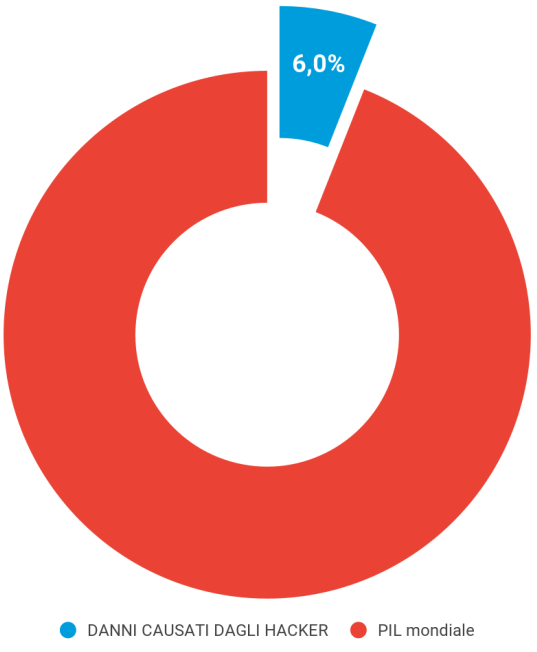
*Photo by Dan Nelson on Unsplash

La sicurezza informatica riveste sempre più un ruolo di primaria importanza per le aziende. Accanto all'aspetto tecnologico, ad incidere enormemente è ancora il fattore umano

Con il termine **Cybersecurity** indichiamo l'uso di strategie, tecnologie e mezzi allo scopo di proteggersi dagli attacchi e dalle minacce presenti in Rete (Cybercrime).

Negli ultimi anni, grazie anche e soprattutto alla diffusione delle tecnologie digitali e della pandemia da Covid-19, il **Cybercrime è diventato un'emergenza globale**.

DANNI CAUSATI DAGLI HACKER
=
3mila miliardi di euro



💥💥💥💥💥💥🏭🏭🏭🏭🏭

6/10 attacchi hacker con impatto
ALTO e **CRITICO**

Per truffare persone e imprese, gli hacker sfruttano le **debolezze psicologiche dell'utente**, in particolare l'intento a fidarsi, la curiosità e quelli che si possono definire **click compulsivi**, ossia l'abitudine a fare clic su un qualsiasi elemento cliccabile, sia esso un link o un allegato, senza valutare con attenzione mittente, messaggio, etc...

La truffa in assoluto più frequente è definita **Phishing**, ovvero una truffa grazie alla quale l'utente viene ingannato e convinto a fornire informazioni e dati personali via e-mail.
Di più, tale attacco può essere utilizzato per veicolare **malware** (un software dannoso con l'obiettivo di infettare e bloccare un pc), soprattutto attraverso allegati.
Nonostante la maggior parte delle email di Phishing venga bloccata dai **filtri antispam**, ancora molte di queste riescono a raggiungere gli utenti.

📧 PHISHING = truffa via email

📲 SMISHING = truffa via sms

📞 VISHING = truffa telefonica

il 97% delle persone non è in grado di riconoscere email truffa

TRUFFE ELABORATE:

→ **RANSOMWARE**: è l'attacco hacker del "blocco con ricatto": vengono bloccati i dati di un utente o di un'azienda con la promessa di sblocco in caso di pagamento di un riscatto.

💸

non ci sono certezze di rientrare in possesso dei propri dati anche dopo aver pagato il riscatto!

→ **CEO Fraud**: l'attaccante, dopo aver studiato conversazioni e stile di scrittura delle vittime e aver scoperto le loro password, si inserisce nella conversazione fingendosi una delle stesse vittime, al fine di convincere l'altro utente a compiere determinate azioni.

L'HACKER

👤 impersona una figura di spicco dell'azienda (un amministratore delegato, un manager, ecc...)

💰 chiede di effettuare bonifici o versamenti

RIDURRE AL MINIMO I RISCHI DEL CYBERCRIME

*Photo by Towfiqu barbhuiya on Unsplash

→ Fare attenzione alle email malevole, che lasciano sempre tracce	📧 indirizzi mail modificati, titoli eclatanti o allarmanti, urgenze e minaccia, utilizzo massiccio di maiuscole o segni, richieste dubbie, allegati e link esterni
→ Mettere in sicurezza le attrezzature aziendali controllando chi ha potere di accesso	💾 hard disk, chiavette, computer portatili, tablet, varia strumentazione elettronica e digitale, etc...
→ Attuare la "3-2-1- Backup Strategy"	💻 3 backup: di cui 2 online (in cloud differenti) e 1 offline
→ Costruire password robuste e mai ripetute	🔒 almeno 12 caratteri, maiuscole e minuscole, segni e numeri
→ Ricorrere ai Password Manager	📂 le "casseforti" per le password, scaricabili dagli store a pagamento
→ Fare formazione periodica al personale aziendale ✍	

di Nicolò Mora e Giulia Bernini

Camera di Commercio Monte Rosa Laghi Alto Piemonte
Servizio PID - Punto Impresa Digitale
www.pno.camcom.it/digitale/pid - pid@pno.camcom.it