CYBER SECURITY POLICY

Quando parliamo di Cyber Security ci stiamo riferendo a tutte quelle best practice e strumenti che servono a difendere i nostri computer, server, dispositivi mobili, reti e dati dagli attacchi informatici. Più in generale, possiamo parlare di sicurezza informatica riferendoci proprio a:

- sicurezza di rete: quando l'obiettivo è difendere le reti informatiche;
- sicurezza delle applicazioni: in questo caso l'obiettivo è proteggere software e dispositivi da eventuali minacce;
- sicurezza delle informazioni: con il compito di proteggere dati personali e privacy;

Quando qualcuno attacca una rete e cerca di reperire dati sensibili siamo in presenza di una minaccia informatica, o *Cyber minaccia*. Queste possono essere di diverso tipo:

- - *Cyber crimine*, quando gli attacchi sono mirati ad ottenere un ritorno economico
- - *Cyber attacchi*, quando l'obiettivo è quello di raccogliere più informazioni possibili da utilizzare per scopi politici
- - *Cyber terrorismo*, quando ciò che si vuole fare è disseminare panico e paura andando a minare la sicurezza dei sistemi elettronici

Come avvengono queste minacce.

Sono diverse e differenti le tecniche che vengono utilizzate per intaccare la nostra sicurezza:

Malware
Questa è una delle minacce più diffuse e consiste in un software realizzato proprio da cybercriminali con l'obiettivo di danneggiare il computer per ottenere ritorni economici o informazioni politiche. I metodi che vengono utilizzati maggiormente per la diffusione di questi malware sono gli allegati di posta elettronica e i download apparentemente legittimi.

Immissione di codice SQL
I cybercriminali che utilizzano questa tecnica spesso hanno l'obiettivo di reperire e rubare i dati di alcuni database.

Phishing e spear phishing
Questa è una delle modalità meno costose e più efficaci per i cybercriminali.
Consiste nell'invio di email truffa. Questi attacchi possono anche essere mirati a persone specifiche e in questo caso prende il nome di spear phishing.

Social engineering
In questo caso, i cyber criminali sfruttano gli errori umani per trarre i loro vantaggi.

Non sono solo queste le tecniche con cui viene minacciata la nostra sicurezza informatica: queste sono solo le più comuni. Le minacce informatiche sono in continua evoluzione, proprio come la stessa tecnologia della quale oggi non possiamo più fare a meno.

Cosa fare per la nostra sicurezza informatica.

Per ridurre la possibilità di subire attacchi di questo tipo:

- La **password** è la miglior alleata in fatto di sicurezza. Per agevolare il ricordo delle nostre password siamo soliti utilizzare nomi e date familiari, ma queste sono quelle che più facilmente vengono recuperate dagli hacker. **Scegliere lunghe sequenze di lettere, numeri e caratteri speciali** e non segnare mai le password sugli appunti, block notes o taccuini; affidarsi piuttosto a piattaforme dedicate.
- Il **backup dei dati** è un'ancora di salvezza nel caso in cui qualcuno riesca ad accedere ai nostri sistemi. E' consigliato anche, per maggior sicurezza, avere più copie del backup aggiornato su dispositivi differenti e luoghi differenti.
- **Aggiornare sempre il software e il sistema operativo** per poter trarre vantaggio dalle patch di sicurezza più recenti.
- Utilizzare software **antivirus** in grado di rilevare e rimuovere eventuali minacce.
- **Evitare di utilizzare reti Wi-Fi non protette** negli spazi pubblici.
- **Non aprire allegati di email provenienti da indirizzi sconosciut**i e non aprire link in siti web non familiari.