Newsletter Digitalmentis

A CURA DI ADOC PIEMONTE

ADOC Piemonte, nell'ambito del Progetto Digitalmentis del Ministero delle Imprese e Made in Italy in collaborazione con la Regione Piemonte, ha redatto una serie di Newsletter in cui verranno affrontati dui temi, ormai sempre più rilevanti, quali la Cybersecurity e l'Intelligenza Artificiale.

Misure di Cybersicurezza per tutti

Ogni tipo di organizzazione è una potenziale vittima di cyber attacchi. Dai servizi pubblici alle aziende private sia grandi che piccole. Anche i privati sono vittime potenziali per ottenere dati di sistema, informazioni private o semplicemente soldi. Sapresti proteggerti dagli attacchi informatici? In questa newsletter forniremo qualche piccolo consiglio per navigare l'internet con serenità.

Lo strumento principale di un hacker è il social engineering, ovvero mettere le persone in condizioni psicologiche tali che non percepiscano il pericolo che corrono. Ci sono molti modi in cui ciò può avvenire.

Questo metodo è chiamato social engineering perché costruisce una falsa promessa tale da attrarre l'attenzione dell'altra persona. Non fa leva sulle capacità informatiche ma sociali dell'hacker. L'obiettivo è far si che per urgenza, per curiosità o avidità della vittima, l'hacker ottenga informazioni o faccia scaricare software malevolo sul computer della vittima.

L'hacker potrebbe mandare email fingendo di essere la tua banca, facendo leva su come tu non potrai più avere accesso ai tuoi soldi a meno che reimposti la password schiacciando su un link. Oppure magari ricevi la minaccia che verrà chiuso il tuo account social a meno che fai reclamo ad un certo link. Magari ricevi un'offerta strepitosa su un prodotto che stavi cercando online oppure per una nuova utenza a basso costo, basta soltanto andare sul sito indicato usando il link promozionale…

Oppure potrebbe impersonificare una persona che conosciamo: un amico o un parente che invia un messaggio siccome ha bisogno urgente di aiuto e non ha più accesso al suo "vecchio" telefonino.

L'obiettivo resta sempre lo stesso: convincerci a visitare siti da cui vengono scaricati automaticamente virus che compromettono i nostri dispositivi oppure su cui noi stessi diamo informazioni sensibili su di noi come età, nome e cognome, luogo di residenza, riferimenti bancari o addirittura password di nostri account usati in servizi online.

Il sistema del social engineering è molto utilizzato perché al giorno d'oggi le misure di sicurezza informatica non consentono più di compiere facilmente un "assalto frontale" ai sistemi. Quindi la migliore scorciatoia per aggirare questi blocchi è avere un accesso diretto all'interno dei sistemi tramite le chiavi di accesso degli utenti.

Iniziativa per le competenze digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024; in Piemonte è realizzata in collaborazione con le Associazioni dei Consumatori presenti sul territorio riconosciute dalla Regione Piemonte, ed è **correlata con la Misura 1.7.2 - "Rete di servizi di Facilitazione Digitale" del P.N.R.R".**

Newsletter Digitalmentis

A CURA DI ADOC PIEMONTE

Esistono modi per arginare i rischi per i propri sistemi informatici e delle precauzioni da prendere così da non cadere preda di queste tattiche.

La prima linea di difesa contro ogni attacco informatico sei tu.

- Quindi dubita dei link nelle comunicazioni che ricevi controllandoli passando il cursore sopra di essi senza cliccare. Se il link non porta dove dice veramente ma ad un'altra destinazione non resta che cestinare la mail indesiderata.
- Non scannerizzare QR code a meno che tu sia certo della loro origine siccome sono link anch'essi.
- Utilizza password lunghe così che i sistemi di sicurezza automatici rivelino tentativi di violazione. Inoltre conserva le password laddove non sono raggiungibili dagli hacker: su agende cartacee. Lasciare password sui sistemi informatici le rende vulnerabili in caso di fughe di dati.
- Utilizza una autenticazione a due fattori laddove sia possibile, così l'hacker non avrà comunque accesso al tuo account siccome non può usare entrambi i dispositivi necessari.

Adoc Piemonte ha preparato anche una videopillola per imparare a conoscere meglio i tipi di attacchi informatici più comuni: https://youtube.com/shorts/Ljm8g5YRilM?feature=share