Social Engineering

Analisi delle tecniche e della sicurezza informatica

By Ruben Fanton

Introduzione

Questa presentazione affronta la sicurezza umana nel contesto digitale, analizzando il social engineering, le reti domestiche IoT e l'impatto ambientale delle infrastrutture.

Approfondiremo anche le tecniche di attacco, le soluzioni di difesa, l'educazione civica e la sostenibilità delle reti comunitarie.

La sicurezza oggi non è solo tecnica, ma anche sociale, psicologica e ambientale.

Internet e le tecnologie di rete portano vantaggi, ma anche rischi da gestire con consapevolezza.

È fondamentale sviluppare competenze digitali e promuovere responsabilità collettiva.

Obiettivo: informare su rischi e soluzioni per una cittadinanza digitale sicura e sostenibile.

01

Tecniche di Social Engineering

Definizione e importanza del social engineering

Il social engineering è una tecnica di manipolazione psicologica usata per ottenere accesso a dati riservati.

Spesso sfrutta la fiducia delle persone per aggirare le misure di sicurezza tecniche.

Le vittime vengono indotte con l'inganno a condividere password, dati bancari o altre informazioni sensibili.

Non si tratta solo di attacchi informatici, ma anche di truffe telefoniche e comunicazioni false.

Gli attaccanti studiano comportamenti e abitudini delle persone per colpirle in modo mirato.

Comprendere come funziona è il primo passo per difendersi.

Relazione con vulnerabilità tecniche

Ci sono alcune truffe digitali molto comuni che usano l’inganno per rubare dati.
Il phishing è quando ricevi email o messaggi falsi che sembrano veri, come quelli della banca o di un social. Ti chiedono dati personali o ti fanno cliccare su un link pericoloso.
Lo spear phishing è simile, ma è fatto su misura per te o per la tua scuola o azienda. L’attacco è più preciso e difficile da riconoscere.
Il pretexting è quando qualcuno si finge un’altra persona per guadagnare la tua fiducia e farti dire informazioni importanti.
Il vishing è come il phishing, ma avviene per telefono: una chiamata in cui ti fanno credere di essere un operatore o un tecnico.
Tutte queste truffe non usano la forza, ma la psicologia. Sapere come funzionano è il modo migliore per evitarle.

Metodi di attacco più comuni

Le tecniche di social engineering sfruttano vulnerabilità umane e tecniche.

Un sistema sicuro può essere compromesso se l'utente non è attento.

L'uso di password deboli o riutilizzate è un rischio frequente.

La mancanza di autenticazione a più fattori facilita l'accesso non autorizzato.

I dispositivi IoT nelle reti domestiche spesso non hanno protezioni aggiornate.

Proteggere le reti richiede attenzione sia tecnica che comportamentale.

02

Educazione sulla Sicurezza

Importanza dell'educazione digitale

L’IoT connette dispositivi come termostati, videocamere e elettrodomestici a Internet.

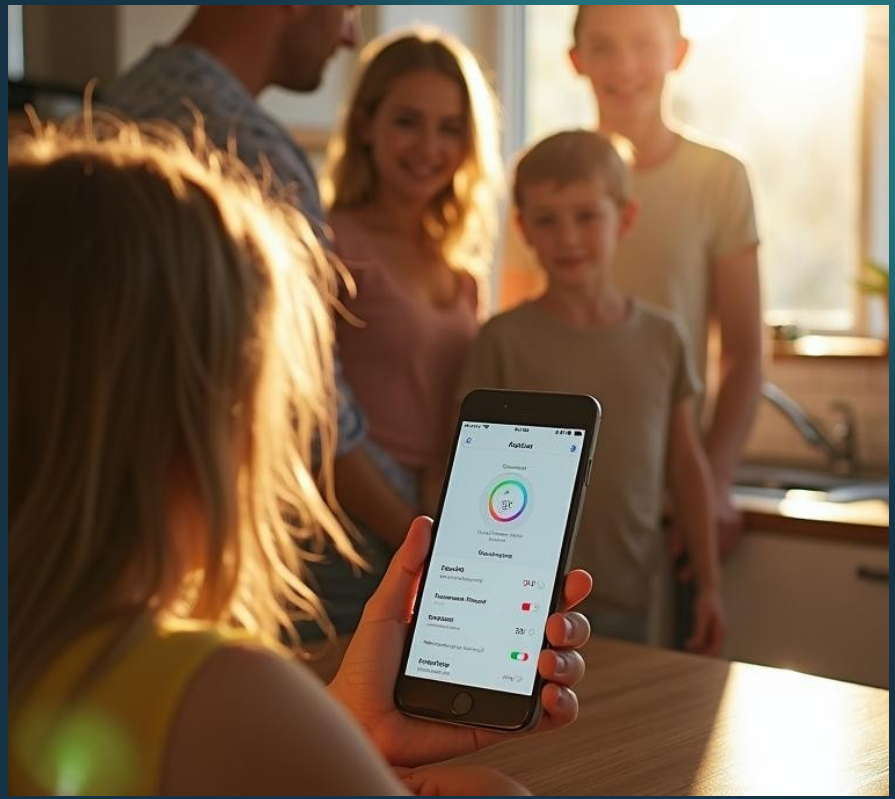
Questi dispositivi sono spesso vulnerabili se non configurati correttamente.

Ogni dispositivo è un potenziale punto di accesso per gli hacker.

Molti utenti non cambiano le credenziali predefinite o non aggiornano i firmware.

La sicurezza delle reti domestiche è diventata una priorità.

Serve una maggiore educazione su come proteggere questi dispositivi.



Impatto sociale delle truffe online

Per proteggerci dai pericoli online ci sono alcune soluzioni che tutti dovremmo usare.
Una delle più importanti è l'autenticazione a più fattori (MFA): oltre alla password, ti viene chiesto un secondo codice che ricevi sul telefono o su un'app. Questo rende molto più difficile per un truffatore entrare nei tuoi account.
Anche aggiornare spesso i dispositivi (come telefono, computer, tablet) è fondamentale. Gli aggiornamenti servono per correggere errori o problemi di sicurezza che gli hacker possono sfruttare per entrare nei tuoi dati.
Poi è importante avere un buon antivirus e un firewall attivi e aggiornati: questi programmi ti aiutano a bloccare virus, malware e siti falsi prima che possano fare danni.
Tutte queste soluzioni, se usate insieme, ti aiutano a stare molto più al sicuro quando usi internet.

Responsabilità individuale e collettiva

Educare alla sicurezza digitale è fondamentale già dalla scuola.

L’alfabetizzazione digitale riduce la vulnerabilità degli utenti.

Serve consapevolezza su privacy, truffe e identità online.

Le istituzioni devono promuovere programmi di formazione civica digitale.

La cittadinanza digitale richiede responsabilità, rispetto e prudenza.

La protezione inizia dalla consapevolezza individuale.

Conclusioni

La sicurezza è una responsabilità condivisa tra individui, aziende e istituzioni.

Ogni utente deve proteggere i propri dati e quelli altrui.

Le aziende devono fornire strumenti sicuri e formare i dipendenti.

Lo Stato deve garantire infrastrutture e regolamentazioni aggiornate.

Collaborazione e trasparenza sono essenziali per la prevenzione.

La sicurezza è un diritto, ma anche un dovere collettivo.