Cyber Security

Cos’è la sicurezza informatica?

Perché è così importante oggi?

Michele Savino

Cyber Security

- Tutti dovremmo saperne di più sulla **sicurez-za informatica**
- Tutti dovremmo familiarizzare con i diversi concetti di **privacy** e **sicurezza.**

Cyber Security

- Quando ci riferiamo alla **Cyber Security**, la definizione più appropriata è: «***l'insieme delle azioni volte a difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi o accessi non autorizzati.»***
- L'obiettivo è garantire la **riservatezza**, **integrità** e **disponibilità** delle informazioni.

Cyber Security

1) Sicurezza di rete: consiste nella difesa delle ***reti informatiche*** dalle azioni di malintenzionati, sia si tratti di ***attacchi mirati*** che di *malware*

2) Sicurezza delle applicazioni: ha lo scopo di proteggere ***software*** ***e dispositivi*** da eventuali minacce. Un'applicazione compromessa può consentire l'accesso ai ***dati*** che dovrebbe proteggere.

Cyber Security

3) Sicurezza delle informazioni: protegge ***l'integrità*** e la ***privacy*** dei ***dati***, sia quelle in archivio che quelle temporanee.

4) Sicurezza operativa: Comprende tutte le ***autorizzazioni*** utilizzate dagli utenti per accedere a una rete e le procedure che determinano come e dove possono essere memorizzati o condivisi i dati.

Cyber Security

5) Formazione degli utenti finali:

riguarda uno degli aspetti più importanti della ***Cyber Security***:

Le persone.

Chiunque non rispetti le ***procedure di sicurezza*** rischia di introdurre accidentalmente un ***virus*** in un sistema altrimenti sicuro.

Gli utenti devono imparare a eliminare gli allegati e-mail sospetti, a non inserire unità USB non identificate e ad adottare altri accorgimenti importanti e essenziali per la sicurezza.

Cyber Security

Tipi di attacchi informatici

Malware

Malware è la contrazione di "***malicious software***" (software malevolo).

Il ***malware***, una delle minacce informatiche più comuni, è costituito da ***software*** creato da ***cyber criminali o hacker*** con lo scopo di danneggiare o provocare il ***malfunzionamento*** del computer di un utente legittimo.

Spesso diffuso tramite ***allegati e-mail*** non richiesti o ***download apparentemente legittimi***, il ***malware*** può essere utilizzato dai ***cyber criminali*** per ottenere un guadagno economico o sferrare ***cyber attacchi*** per fini politici.

Cyber Security

Esistono numerosi tipi di malware, tra cui:

1) Virus

Un programma capace di ***replicarsi autonomamente***, che si ***attacca*** a un file pulito e si diffonde nell'intero sistema informatico, ***infettandone*** i file con il suo codice malevolo.

2) Trojan

Un tipo di ***malware*** mascherato da ***software legittimo***. I cyber criminali inducono gli utenti a scaricare il ***Trojan*** nei propri computer, dove possono causare danni o raccogliere dati.

Cyber Security

Esistono numerosi tipi di malware, tra cui:

3) Spyware

Un programma che registra segretamente le ***azioni*** dell'utente, per consentire ai cyber criminali di sfruttare tali informazioni a proprio vantaggio. Ad esempio, lo ***spyware*** può acquisire i dati delle carte di credito.

4) Ransomware

Malware che blocca l'accesso ai file e ai dati dell'utente, minacciandolo di ***cancellarli*** se non paga un ***riscatto***.

Cyber Security

Tipi di attacchi informatici

5) Phishing

In un attacco di ***phishing***, i cyber criminali inviano alle vittime e-mail che sembrano provenire da aziende legittime, per richiedere informazioni sensibili.

Gli attacchi di ***phishing*** hanno solitamente lo scopo di indurre gli utenti a fornire i dati della carta di credito o altre informazioni personali.

6) Attacco Man-in-the-Middle

Un attacco ***Man-in-the-Middle*** è una minaccia informatica in cui un cyber criminale intercetta le comunicazioni fra due persone allo scopo di sottrarre dati.

Ad esempio, su una rete Wi-Fi non protetta, l'autore dell'attacco può intercettare i dati scambiati fra il dispositivo della vittima e la rete.

Cyber Security

7) Social Engineering

manipolazione *psicologica* per ottenere informazioni sensibili.

Cyber Security

Protezione utente finale

La protezione dell'***utente finale***, o endpoint security, è un aspetto cruciale della Cyber security.

Dopo tutto, sono spesso le persone (gli utenti finali) a scaricare accidentalmente ***malware*** o altri tipi di minacce informatiche nei propri pc, computer portatili o dispositivi mobili.

Quindi, in che modo le misure di Cyber security proteggono gli utenti finali e i loro sistemi?

I programmi di sicurezza continuano a sviluppare nuove difese, a mano a mano che gli esperti di Cyber security identificano nuove minacce e nuovi modi per combatterle.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

1. Aggiornare il software e il sistema operativo

questo permette di sfruttare le patch (*correzioni*) di sicurezza più recenti.

2. Firewall

sistema che filtra il traffico di rete per bloccare accessi non autorizzati.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

2. Utilizzare software antivirus

Sono software in grado di rilevare e rimuovere le minacce.
Il software deve essere aggiornato regolarmente per garantire il massimo livello di protezione.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

3. Utilizzare password complesse

assicuratevi di utilizzare password difficili da indovinare.

4. Autenticazione a più fattori (MFA)

richiede più metodi di verifica (es. password + codice OTP) per accedere a un account.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

5. Non aprire allegati e-mail di mittenti sconosciuti { potrebbero essere infettati dal malware.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

6. Non fare clic sui link contenuti nei messaggi e-mail di mittenti sconosciuti o in siti web non familiari

è un metodo comune per diffondere il malware.

Cyber Security

Consigli di Cybersecurity
come proteggersi dagli attacchi informatici

7. Evitare di utilizzare reti Wi-Fi non protette negli spazi pubblici

le reti pubbliche espongono i dispositivi agli attacchi Man-in-the-Middle.

Furto d’identità

- È un **reato** in cui un malintenzionato utilizza **informazioni personali** di un'altra persona (come nome, dati bancari, codici fiscali, ecc.) per commettere **frodi** o **attività illegali**

Di seguito alcuni esempi pratici di come può avvenire:

1. Phishing via email

- **Scenario**: Ricevi un'email che sembra provenire dalla tua banca, con un messaggio urgente che ti invita a cliccare su un link per "verificare il tuo account".
- **Come avviene il furto:** Il link ti porta a un sito falso che imita quello della banca. Inserendo le tue credenziali (nome utente, password, codici OTP), il criminale le ruba e le usa per accedere al tuo conto.
- **Esempio concreto:** Nel 2020, molti utenti di PayPal sono stati colpiti da una campagna di phishing che ha portato al furto di migliaia di credenziali.

2. Furto di dati tramite violazioni di database

- **Scenario**: Un'azienda in cui hai un account (es. un negozio online) subisce una violazione dei dati.
- **Come avviene il furto:** I criminali accedono al database e rubano informazioni come email, password, numeri di carte di credito e indirizzi.
- **Esempio:** Nel 2017, Equifax, un'agenzia di credito statunitense, ha subito una violazione che ha esposto i dati di 147 milioni di persone, inclusi numeri di previdenza sociale e informazioni finanziarie.

3. Skimming agli sportelli bancomat

- **Scenario**: Prelevi contanti da un bancomat.
- **Come avviene il furto:** I criminali installano uno skimmer, un dispositivo che legge i dati della tua carta, e una microcamera per registrare il PIN.
- **Esempio concreto:** Nel 2019, in Italia sono stati scoperti skimmer su bancomat in diverse città, con centinaia di carte clonate e utilizzate per prelievi fraudolenti.

4. Furto di identità sui social media

- **Scenario**: Condividi troppe informazioni personali sui social network (es. compleanno, città natale, nomi di familiari).
- **Come avviene il furto**: I criminali usano questi dati per rispondere a domande di sicurezza o per impersonarti.
- **Esempio concreto**: Nel 2021, un utente di Facebook ha subito il furto dell'account dopo che i criminali hanno usato informazioni pubbliche per convincere il supporto tecnico di essere il proprietario.

5. Frodi con carte di credito clonate

- **Scenario**: Fai acquisti online su un sito non sicuro.
- **Come avviene il furto**: I criminali intercettano i dati della tua carta di credito durante la transazione e li usano per fare acquisti fraudolenti.
- **Esempio concreto**: Nel 2020, molti utenti di un noto sito di e-commerce hanno segnalato transazioni non autorizzate dopo aver inserito i dati della carta.

6. Furto di identità tramite malware

- **Scenario**: Scarichi un file infetto da un sito non affidabile o apri un allegato email sospetto.
- **Come avviene il furto**: Il malware installato sul tuo dispositivo registra le tue attività (es. digitazione di password) e invia i dati ai criminali.
- **Esempio concreto**: Il trojan Zeus è stato utilizzato per rubare credenziali bancarie da migliaia di utenti in tutto il mondo.

Come proteggersi dal furto di identità

1. Non condividere informazioni personali su siti non sicuri o con sconosciuti.
2. Usa password complesse e attiva l'autenticazione a due fattori (2FA).
3. Controlla regolarmente estratti conto e report creditizi.
4. Installa antivirus e mantieni aggiornati i tuoi dispositivi.
5. Fai attenzione alle email sospette e non cliccare su link o allegati non verificati.

Proteggersi dal furto di identità e da altre minacce informatiche richiede una combinazione di buone pratiche, strumenti tecnologici e consapevolezza.

Ecco una guida dettagliata su come proteggersi:

1. Gestione delle password

- **Usa password complesse**: Combina lettere maiuscole, minuscole, numeri e simboli ***(es. P@ssw0rd!2023***).
- **Evita password comuni:** Non usare sequenze come "***123456***" o "password".
- **Non riutilizzare le password:** Usa una password diversa per ogni account.
- **Usa un gestore di password:** Strumenti come ***LastPass, 1Password o Bitwarden*** generano e memorizzano password sicure.
- **Cambia le password regolarmente**: Soprattutto per account sensibili (***es. email, conti bancari***).

2. Autenticazione a più fattori (2FA/MFA)

- **Attiva l'autenticazione a due fattori:** Richiede un secondo metodo di verifica oltre alla password (es. un codice OTP inviato al telefono o un'app).
- **Usa metodi di autenticazione avanzati:** Dove possibile, utilizza autenticazione biometrica (impronte digitali, riconoscimento facciale).

3. Protezione dei dispositivi

- **Installa antivirus e antimalware:** Software come ***Bitdefender***, ***Kaspersky*** o ***Malwarebytes*** proteggono da minacce.
- **Mantieni il software aggiornato:** Installa sempre gli ultimi aggiornamenti di sistema e delle applicazioni per correggere vulnerabilità.
- **Usa una VPN:** Una rete privata virtuale (es. ***NordVPN***, ***ExpressVPN***), ***ProtonVPN*** cripta il traffico internet e protegge la tua privacy online.
- **Blocca i dispositivi:** Usa ***PIN***, ***password*** o ***metodi biometrici*** per sbloccare smartphone, tablet e computer.

4. Navigazione sicura

- **Verifica i siti web**: Assicurati che l'URL inizi con https:// (il "s" indica che la connessione è criptata) e che ci sia un'icona di lucchetto nella barra degli indirizzi.
- **Evita reti Wi-Fi pubbliche:** Se necessario, usa una VPN per proteggere i dati.
- **Non cliccare su link sospetti**: Controlla sempre l'URL prima di cliccare, soprattutto in email o messaggi.
- **Usa browser sicuri:** Browser come ***Firefox*** o ***Brave*** offrono protezioni integrate contro phishing e malware.

5. Protezione delle e-mail

- **Non aprire allegati sospetti:** Anche se sembrano provenire da fonti affidabili.
- **Verifica il mittente:** Controlla l'indirizzo email per assicurarti che sia autentico.
- **Usa filtri anti-spam:** Configura il tuo client email per bloccare messaggi indesiderati.
- **Non rispondere a email di phishing:** Segnalale invece al provider email.

6. Gestione dei dati personali

- **Limita la condivisione sui social media:** Evita di pubblicare informazioni sensibili come data di nascita, indirizzo o numeri di telefono.
- **Cancella account inutilizzati:** Riduci il rischio di violazioni eliminando account che non usi più.
- **Usa pseudonimi:** Dove possibile, utilizza nomi utente o indirizzi email che non rivelino la tua identità reale.

7. Monitoraggio finanziario

- **Controlla estratti conto e transazioni:** Verifica regolarmente movimenti sospetti su conti bancari e carte di credito.
- **Attiva notifiche**: Imposta avvisi per ogni transazione effettuata con le tue carte.
- **Congela il credito:** Se sospetti un furto di identità, contatta le agenzie di credito per bloccare richieste di prestiti o carte a tuo nome.

8. Backup dei dati

- **Esegui backup regolari:** Salva copie dei tuoi dati su dispositivi esterni o servizi cloud sicuri (es. Google Drive, Dropbox con crittografia).
- **Usa crittografia:** Proteggi i backup con password o strumenti di crittografia.

9. Formazione e consapevolezza

- **Impara a riconoscere le minacce:** Informati su phishing, malware e altre tecniche di attacco.
- **Partecipa a corsi di sicurezza:** Molte organizzazioni offrono formazione gratuita o a pagamento sulla cybersecurity.
- **Condividi le conoscenze:** Aiuta familiari e amici a proteggersi.

10. Strumenti avanzati

- **Firewall**: Proteggi la tua rete domestica con un firewall hardware o software.
- **Crittografia end-to-end:** Usa app di messaggistica come Signal o WhatsApp per comunicazioni sicure.
- **Monitoraggio del credito:** Servizi come Experian o Credit Karma ti avvisano di cambiamenti nel tuo report creditizio.

Seguendo queste pratiche, puoi ridurre significativamente il rischio di furto di identità e altre minacce informatiche.

11. In caso di furto di identità

- **Segnala immediatamente:** Contatta la tua banca, il provider di servizi e le autorità competenti.
- **Cambia tutte le password:** Aggiorna le credenziali degli account compromessi.
- **Monitora il credito:** Richiedi un report creditizio e verifica attività sospette.
- **Presenta una denuncia:** Rivolgiti alle forze dell'ordine per avviare un'indagine.