CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Proteggere i tuoi dispositivi e account
Linee guida sulle password

Crediamo che l'utilizzo della cd. *Strong Authentication* sia uno dei modi più efficaci ed economici che possono essere utilizzati per rendere sicure le attività delle organizzazioni e degli utenti online.
Durante il World More Than A Password Day, il 10 Novembre 2023, rilasciamo queste semplici linee guida sulle password che tutti possono adottare per essere più sicuri:
Linee guida

1. Utilizza autenticazione senza password

Quando puoi, utilizza l'autenticazione senza password, ad esempio tramite passkeys, semplici da usa re e molto più sicure. Le passkeys si affidano alla crittografia per assicurare il riconoscimento dell'utente su siti web e servizi online, impiegando una chiave segreta che è conservata sul dispotivo dell'utente e mai condivisa. Sono supportate dai principali sistemi operativi, browser e servizi email – cerca in internet "passkey" e il nome del tuo sistema operativo, browser o servizio email per verificare se sono supportate).

2. Metti in sicurezza il tuo account email

Se utilizzi una password per proteggere il tuo account email, assicurati di usare una password forte (lunga, generata casualmente e unica – vedi https://www.cisa.gov/sites/default/files/2023-08/Secure-Our-World-Passwords-Tip-Sheet.pdf per suggerimenti su come scegliere la password). L'Email è il mezzo più comune per resettare le password, anche per questo è fondamentale che nessun'altro oltre te acceda al tuo account.

3. Aggiungi alla password ulteriori misure di sicurezza

L'utilizzo di una chiave di sicurezza hardware, di un'app per l'autenticazione o, se non disponibili le prime due opzioni, di un PIN fornito tramite SMS come "secondo fattore" di autenticazione può aiutare a prevenire il phishing e altri attacchi. Questo processo è denominato MFA, 2FA o verifica a doppio step.

4. Usa un password manager

Specialmente se non fai utilizzo di passkeys o MFA, usa un password manager per evitare di dover memorizzare tutte le tue password. In tal modo, potrai scegliere password forti, generate casualmente e quindi difficili da indovinare. Password managers di tipo software, browser e sistemi operativi che gestiscono le tue password sono ottime scelte. Chiaramente, devi scegliere la password con cui accedere al password manager in modo tale che sia facilmente memorizzabile e al contempo forte. Ricordati di modificare tutte le password nel caso in cui il password manager sia compromesso.
Maggiori informazioni sui password manager possono essere trovate ai link riportati a seguire.
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
https://www.cyber.gc.ca/en/guidance/password-managers-security-itsap30025

5. Usa una tecnica per scegliere le password

Se non ti affidi ad un generatore casuale di password, puoi usare una passphrase o una tecnica come quella delle "tre parole casuali" per scegliere password facili da ricordare ma difficili da indovinare.
Maggiori informazioni ai seguenti link:
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

6. Cambia le password

Le tue password dovrebbero essere cambiate immediatamente se uno dei tuoi dispositivi è stato compromesso, ad esempio a seguito dell'installazione di malware sul tuo computer da parte di un hacker. Inoltre, se un sito web che frequenti o un servizio online che usi è stato violato, cambia la password che usi per quel sito o servizio e, nel caso in cui avessi riutilizzato quella password altrove (pratica assolutamente sconsigliata), modificala anche li.

Effettuare la sottoscrizione al seguente servizio https://haveibeenpwned.com/ è un ottimo modo per verificare se la tua password ha bisogno di essere modificata. Quando si rende necessario il cambio della password, è fondamentale utilizzare un dispositivo che non è stato compromesso.