Sicurezza digitale

Per progettare e fare azioni di disobbedienza civile utilizziamo piattaforme, applicazioni e dispositivi con le quali scambiamo le informazioni necessarie. È molto importante proteggere queste informazioni da occhi e orecchie indiscrete, per evitare che le azioni possano essere bloccate ancora prima di iniziare.

Proteggere l'accesso agli account

Gli account che usiamo quotidianamente, non solo per le piattaforme XR, richiedono credenziali di accesso (nome utente e password) che solo il/la proprietaria dell'account conosce. Bisogna fare in modo che nessuno possa scoprire queste credenziali, ovvero scoprire la password. Per questo **è importante scegliere una password complessa**, che non abbia riferimenti a nostri dati o interessi che altre persone potrebbero sapere o scoprire attraverso le nostre attività online.
Una buona password:

- è lunga **almeno 12 caratteri**;
- è composta da **più parole**, prive di significato;
- contiene lettere minuscole e maiuscole, numeri e caratteri speciali (nota: lo spazio è un carattere valido!);
- è **generata casualmente** da un applicativo;
- è **diversa** da ogni altra password che usiamo nei vari account.

Ricordare tutte le password di accesso ad account e dispositivi diventa sempre più difficile al crescere del numero di account che utilizziamo.
Per alleviare il peso di ricordare tutte queste stringhe lunghe e prive di senso, la tecnologia ci viene in aiuto con **i gestori di password**: sono degli applicativi che funzionano da "cassaforte", nella quale è possibile salvare le nostre password e visualizzarle/copiarle, dopo aver aperto la cassaforte: ricordando un'unica "combinazione"(la password per accedere al gestore, che deve ovviamente essere molto robusta), possiamo accedere a tutte le altre senza doverle ricordare.
Un buon gestore di password

- **è offline**: l'applicazione si installa sul telefono/PC ma non salva il database delle password su un cloud né condivide il database con altri tuoi dispositivi. L'ideale è averla sullo smartphone, così che è sempre a portata di mano;
- permette di **esportare il database**, cifrato, in modo da porterlo salvare come backup su un altro supporto/dispositivo o mandarselo per email (purché sia cifrato!). Se lo smartphone si blocca o si rompe, possiamo sempre recuperare il database di backup e importarlo tramite l'app su un nuovo dispositivo.

Un buon gestore di password che soddisfa questi requisiti è ad esempio KeePass.

Le regole sulle password degli account si applicano anche ai codici di accesso allo smartphone e/o al PC. Inoltre

- è sconsigliato utilizzare sblocchi biometrici come impronta digitale o riconoscimento facciale;
- sullo smartphone si può usare un pattern di sblocco (quello con i 9 o 16 pallini disposti in un quadrato), purché sia molto complesso;

Un'ulteriore barriera contro eventuali accessi non autorizzati è **l'autenticazione a due fattori** (in inglese Two Factor Authentication, 2FA). Se chi sviluppa la piattaforma su cui abbiamo l'account fornisce questo servizio è consigliabile attivarlo sempre.
Al momento dell'accesso, inserendo le credenziali corrette, viene inviata una sequenza numerica generata casualmente su un dispositivo di nostra scelta, tramite SMS o altro mezzo. Oppure il codice viene generato dall'utente tramite apposita applicazione. Vedi ad esempio Authy.

Proteggere i dati dei dispositivi in caso di sequestro

È importante fare in modo che un dispositivo che finisce in mani altrui non sia utilizzabile e i dati al suo interno non possano essere esfiltrati.
Il modo più sicuro per farlo è cifrare il disco, in modo che senza la chiave di cifratura (collegata alla password necessaria a sbloccare il dispositivo stesso) i dati salvati al suo interno siano assolutamente illeggibili.
La procedura per cifrare il disco dipende dal dispositivo considerato:

- Android → *Impostazioni di sicurezza*
- iPhone → *nativa sul dispositivo*
- MacOS → *FileVault + password del BIOS. Nativa su dispositivi più recenti*
- Linux → *LUKS (partizioni o intero disco con sblocco all'avvio)*
- Windows → *VeraCrypt[EN] (NO Bitlocker!)*

Piattaforme e app di messaggistica

- No whatsapp e telegram per organizzare azioni o comunicare durante le azioni
- Mattermost e Cloud per organizzare azioni
- Wire o Signal per comunicare durante l'azione
- e-mail: usare cifratura PGP. ProtonMail la implementa automaticamente (a patto che entrambi gli interlocutori utilizzino ProtonMail)

Buone pratiche pre/durante/post azione

Durante le riunioni:

- **spegnere gli smartphone** e metterli in un'altra stanza;
- se possibile, allontanare anche i PC desktop.

In azione:

- se sei in un ruolo ad alto rischio, valuta di non portare con te il tuo smartphone
- se devi portarlo, valuta di avere un device con il minimo indispensabile all'azione (idealmente una SIM e solo Wire/Signal installato, nient'altro).

Post-azione:

- in caso di arresto:
  - spegnere il device prima di consegnarlo (bisogna aver cifrato il disco)
  - non si dovrebbe essere obbligati a sbloccare il dispositivo. Nel caso, il codice di sblocco può essere dimenticato, specie se sotto stress. L'impronta o il riconoscimento facciale, invece, no...
  - se il dispositivo viene requisito e poi restituito, è da considerarsi compromesso. Bisogna come minimo ripristinarlo alle impostazioni di fabbrica e chiedere all'operatore telefonico di sostituire la SIM
- in caso di perquisizione domestica
  - spegnere PC e/o smartphone prima di consegnarlo (bisogna aver cifrato i dischi)
  - come sopra, se preso e restituito il device è da considerarsi compromesso

---

Versione #1
Creato 19 ottobre 2023 17:41:40 da Admin
Aggiornato 15 aprile 2024 15:29:55 da Admin