
PASSWORD

Password Manager e 2FA

COME DEVE ESSERE?

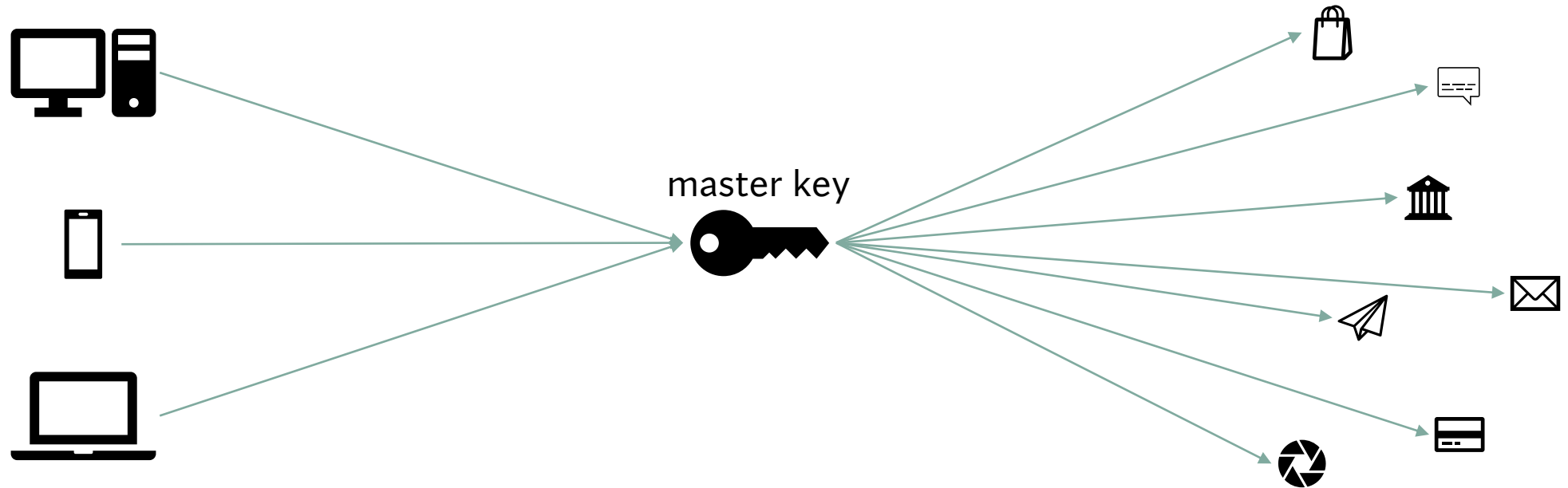


Suggerimenti Google



Suggerimenti Troy Hunt

PASSWORD MANAGER



VANTAGGI

RICORDARE UNA SOLA PASSWORD

GENERARE AUTOMATICAMENTE PASSWORD

PASSWORD SINCRONIZZATE CON TUTTI I DISPOSITIVI

AUTOCOMPILAZIONE DEI DATI DELL'ACCOUNT

PASSWORD AGGIORNATE AUTOMATICAMENTE

AGGIUNGERE INFORMAZIONI SULL'ACCOUNT

FILE DELLE PASSWORD CRIPTATO

KeePass XC



Password Manager Offline

<https://keepassxc.org/>

Google Password Manager



Password Manager Browser

<https://passwords.google.com/>

Bitwarden



Password Manager Online

<https://bitwarden.com/>

LIVELLO DI SICUREZZA

100%?

“L’unico vero sistema sicuro è un sistema spento,
chiuso in una gettata di cemento,
sigillato in una stanza rivestita di piombo
protetta da guardie armate.
Ma anche in questo caso ho i miei dubbi.”

« Prof. Eugene Howard Spafford (**Spaf**) »

AUTENTICAZIONE A DUE FATTORI (2FA)

MESSAGGIO TELEFONO	OTP inviato per SMS al numero di telefono specificato dall'utente in fase di registrazione
INDIRIZZO MAIL	OTP inviato per MAIL all'indirizzo specificato dall'utente in fase di registrazione
DISPOSITIVO HARDWARE	OTP generato tramite hardware specifico (esempio: https://www.yubico.com/)
APPLICAZIONE	OTP inviato tramite app installata sullo smartphone (esempio: https://getaegis.app/)