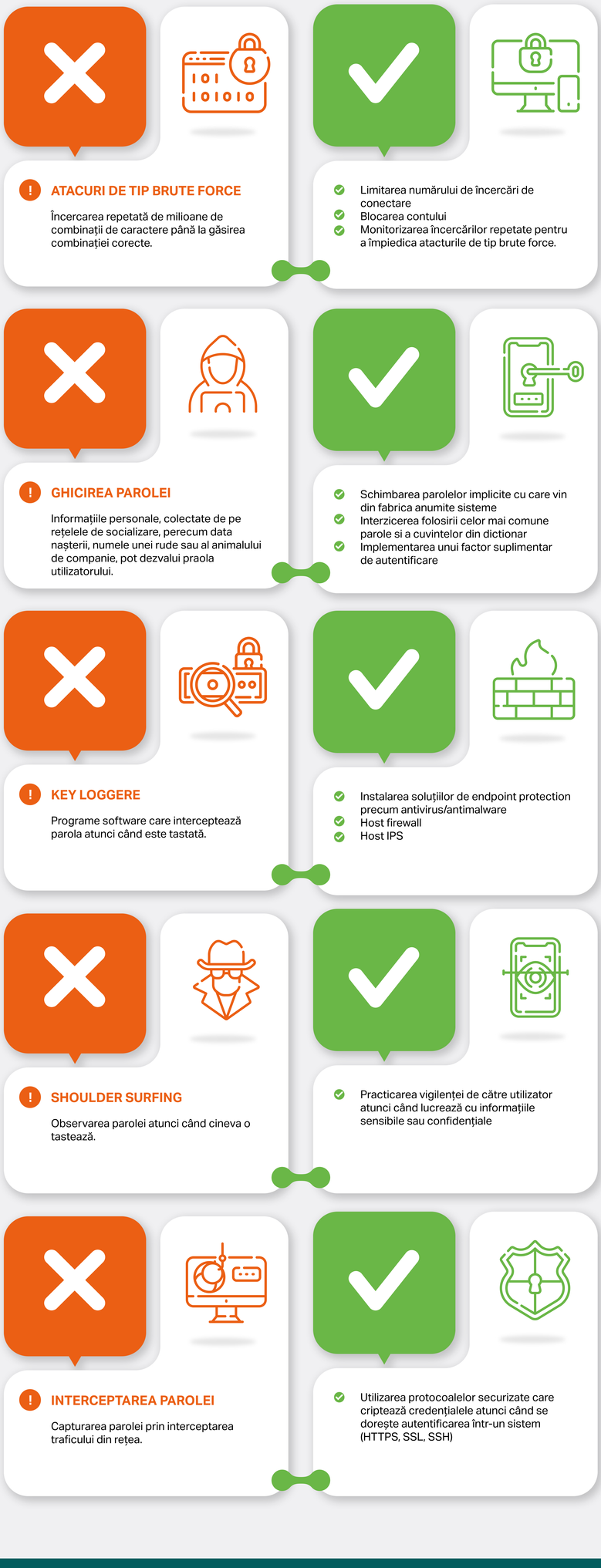
dendrio
Your journey. Upgraded.

SECURITATEA PAROLELOR

Atacatorii folosesc o varietate de unelte pentru a comprimite parolele, inclusiv software-uri disponibile gratuit pe Internet. Următoarele sfaturi sunt menite să ajute utilizatorii să securizeze modul în care sunt folosite parolele în organizație.

CUM SUNT COMPROMISE PAROLELE...	CUM LE PUTEM SECURIZA



ATACURI DE TIP BRUTE FORCE

Încercarea repetată de milioane de combinații de caractere până la găsirea combinației corecte.

- Limitarea numărului de încercări de conectare
- Blocarea contului
- Monitorizarea încercărilor repetate pentru a împiedica atacurile de tip brute force.

GHICIREA PAROLEI

Informațiile personale, colectate de pe rețelele de socializare, precum data nașterii, numele unei rude sau al animalului de companie, pot dezvalui praola utilizatorului.

- Schimbarea parolelor implicite cu care vin din fabrica anumite sisteme
- Interzicerea folosirii celor mai comune parole si a cuvintelor din dictionar
- Implementarea unui factor suplimentar de autentificare

KEY LOGGERE

Programe software care interceptează parola atunci când este tastată.

- Instalarea soluțiilor de endpoint protection precum antivirus/antimalware
- Host firewall
- Host IPS

SHOULDER SURFING

Observarea parolei atunci când cineva o tastează.

- Practicarea vigilenței de către utilizator atunci când lucrează cu informațiile sensibile sau confidențiale

INTERCEPTAREA PAROLEI

Capturarea parolei prin interceptarea traficului din rețea.

- Utilizarea protocoalelor securizate care criptează credențialele atunci când se dorește autentificarea într-un sistem (HTTPS, SSL, SSH)