Cum setez o parolă sigură si de ce?

Iulia Stratulat - 2021-08-06 - Cum rezolv...?

Parolele reprezintă unul dintre punctele slabe în securitatea unui cont, nu numai pentru cel al unui website sau al unei adrese de email, ci pentru orice cont securizat cu parolă.

Întotdeauna va exista o persoană rău intenționată care dorește să exploateze conturile slab securizate, de aceea este bine să utilizați parole sigure pentru securitate sporită.

De obicei, parolele sunt "sparte" pentru a fura datele sau software-ul folosit, pentru a modifica pagina (defacing) ori pentru a crea pagini de phishing.

Pentru a preveni problemele ce pot apărea ca urmare a utilizării unor parole nesigure, ROMARG recomandă folosirea unor parole cât mai sigure, care să nu fie știute de nimeni altcineva decât de către dumneavoastră, deținătorul contului.

În cele ce urmează vă vom oferi niște date după care vă puteți ghida pentru a crea parole sigure.

1. Utilizați câte o parolă pentru fiecare cont

Nu folosiți aceeași parolă pentru mai multe conturi. În cazul în care parola va fi "spartă", șansele de a compromite conturile mai departe vor crește exponențial.

De exemplu, vi se afla parola la contul de email, dacă folosiți aceeași parolă și pe pagina de administrare a site-ului, pagina dumneavoastră devine complet compromisă.

Având parola de la contul de email ar putea să vă compromită și contul de client și de aici lucrurile pot merge mai departe până la pierderea numelui de domeniu.

2. Folosiți o parolă sigură

O parolă poate fi spartă în mai multe moduri. De obicei se utilizează o metodă numită "brute force" - încercarea tuturor combinațiilor posibile de litere până este găsita cea corectă.

Dacă cererile de conectare vin de la o adresă IP, firewall-ul serverului le va bloca, dar uneori, în funcție de cât de iscusiți sunt cei care încearcă să vă spargă parola, cererile ar putea veni de la un număr foarte mare de adrese IP și astfel firewall-ul să nu le poată bloca.

Pentru a preveni acest tip de atac recomandăm următoarele în legătura cu parola folosită:

- **Folosiți o parolă lungă.** O parolă sigură ar trebui să nu fie mai scurtă de 8 caractere. Cu cât parolă este mai lunga, cu atât șansele de a fi spartă sunt mai mici deoarece orice caracter adăugat în plus crește exponențial numărul de combinații necesare pentru găsirea parolei prin brute force.
- **Nu utilizati doar cuvinte** și folosiți mereu o combinație de: caractere speciale (:"$%^#^), litere mici (dffsdfsf) și mari (GGSUAJB). Securitatea adițională adăugata este sporită foarte mult.
- **Nu folosiți cuvinte sau nume semnificative** pentru dumneavoastră. De exemplu, nu folosiți numele de domnișoara a mamei, zile de naștere, numele animalului avut în copilarie și așa mai departe.
- Dacă totuși doriți să aveți o parolă pe care să o țineți minte, **asigurați-vă că aceasta este formatată în așa fel încât sa fie foarte greu de ghicit**. Spre exemplu, luăm combinația "parolasigura", care se poate scrie in felul urmator: p@r07AS16urQ. Alăturarea de litere mari și mici plus simboluri și cifre utilizate in loc de litere o fac mult mai sigură deși aceasta este în mod normal o parolă cu o securitate minimă, am putea spune chiar inexistentă.

  Notă! Nu utilizati exemplul de mai sus ca parolă proprie!

Deoarece memorarea unor parole complexe este destul de complicată și notarea lor pe suport fizic sau logic nu este indicată, puteăi utiliza un manager de parole. Un astfel de manager de parole poate fi unul online sau unul local, pe calculatorul dumneavoastră.

3. Securitatea locală

- Atât setarea unei parole sigure, cât și păstrarea acesteia în mod corespunzător reprezintă procese foarte importante.

Asigurați-vă că **nu aveți parola scrisă undeva la vedere** deoarece o persoană cu intenții rele ar putea-o folosi în dezavantajul dumneavoastră.

- Asigurați-vă că **programul antivirus este menținut cu update-urile la zi** pentru a evita situațiile în care ați putea să fiți infestat cu un key logger (program ce salvează tot ce tastați) și astfel parola să fie obținută de o persoană rău intenționată.
- Încercați să **navigați pe pagini securizate prin HTTPS**, deoarece informația transmisă prin astfel de pagini este criptată iar în cazul în care trebuie să folosiți o rețea wireless nesecurizată de exemplu, informația transmisă va fi în siguranță.
- Mai este si problema site-urilor de phishing. Aceste pagini seamănă foarte bine cu pagina originala și astfel pot obține date de autentificare pentru diverse conturi. **Evitați să dați click pe link-uri din email-uri** care pot părea suspicioase, mai bine scrieți adresa în mod manual în browser.

Acestea sunt principalele metode de protejare a conturilor prin parole sigure.

În cazul în care aveti nevoie de asistență suplimentară, echipa ROMARG vă stă la dispoziție prin email la adresa support@romarg.com.