Recomandări pentru creare parole:

Conține între între 6 și 40 caractere;
Nu conține spațiu;
Conține cel puțin o literă majuscula A-Z;
Conține cel puțin o literă minusculă a-z;
Conține cel puțin o cifră 0-9;
Conține un caracter special din setul: - . , : ; [ ] { } _ + = @ # $ ^ * ? ! | ~

- 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.
- 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.
- 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.
- 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.
- 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.