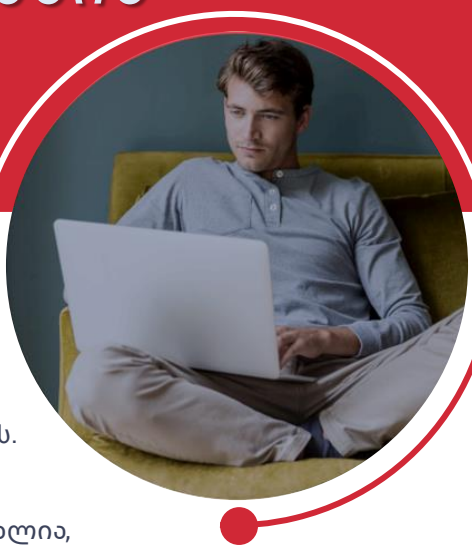
პაროლების ფსიქოლოგია: ონლაინქცევა, რომელიც საფრთხეს გვიქმნის



სულ უფრო მეტი ადამიანი მუშაობს და შოპინგობს ონლაინ და საკომუნიკაციოდაც ონლაინ არხებს იყენებს, რაც ჰაკერებს უადვილებს პირად ინფორმაციაზე წვდომას.

გამოკითხვის თანახმად, რომელშიც ავსტრალია, აშშ, ბრაზილია, გერმანია, დიდი ბრიტანეთი და სინგაპური მონაწილეობდნენ, მიუხედავად იმისა, რომ კიბერრისკების შესახებ იციან, მსოფლიოში უამრავი ადამიანი მაინც არ იცავს თავს. თქვენც ასე გაუფრთხილებლად იქცევით?

ტოპ-6 სარისკო ქცევა, რომელიც სამიზნედ გვაქცევს

1 ვიყენებთ ერთსა და იმავე პაროლს

თუ ჰაკერი ერთ ანგარიშს გატეხავს, ყველა დანარჩენი ანგარიშიც ადვილად ხელმისაწვდომი ხდება

91% 91%-მა იცის, რომ არ უნდა გამოიყენოს ერთი და იგივე პაროლი ან მისი ვარიაციები;

თუმცა...

66% 66% მაინც იმავეს აკეთებს!

2 გვინდა ვაკონტროლოთ

პაროლების განმეორებით გამოყენებით სიტუაციას კი არ ვაკონტროლებთ, არამედ ვრისკავთ. კითხვაზე, რატომ იყენებთ ერთი და იმავე პაროლს, ასე გვპასუხობდენ?

60% მეშინია, რომ login და პაროლი დამავიწყდება

52% მინდა ვიცოდე და ვაკონტროლო ჩემი ყველა პაროლი

3 ყურადღებას არ ვაქცევთ გატეხვის შემთხვევებს

თუ ბრენდი ან პლატფორმა, რომლითაც სარგებლობთ, გატეხეს, პაროლი უნდა შეცვალოთ.

52% იმის მიუხედავად, რომ მედიით გახმაურდა, რომ ბრენდი გატეხეს, 52%-ს არ შეუცვლია პაროლი ბოლო 12 თვეში

4 რისკს სათანადოდ არ ვაფასებთ

"მე არ ვარ სამიზნე!" ცდებით. შესაძლოა ჰაკერმა თქვენი საბანკო ბარათიდან მხოლოდ მცირე თანხა აგაწაპნოთ, თუმცა ათასობით მონაცემის შემთხვევაში, დიდი თანხა გამოდის.

41% 41% ფიქრობს, რომ მათი ანგარიშები ჰაკერისთვის არ იქნება საინტერესო

5 პროგნოზირებადი ვართ

ჰაკერებს არ გაუჭირდებათ მოიძიონ თქვენი პირადი ინფორმაცია ინტერნეტში ან სოციალური ქსელების მეშვეობით.

22% 22%-ს შეუძლია გამოიცნოს მეუღლის/პარტნიორის პაროლი

24% 24% პაროლად იყენებს სენტიმენტალურ ინფორმაციას

როგორია ძლიერი პაროლი?

ყველაზე დაცული პაროლი შეიცავს:

- **მინიმუმ 8** სიმბოლოს (რეკომენდებულია 12)
- მაღალი და დაბალი რეგისტრის ასოებს - **aA bB cC dD … zZ**
- ციფრებს - **1 2 3 4 5 6 7 8 9 0**
- დამატებით სიმბოლოებს - **! @ # $ % ^ & ***

პაროლის შერჩევის საიმედო ხერხი: **ფრაზა + თარიღი + სიმბოლო**
მაგ: Safety_First2021, SafestPasswordEver2030%

რამეს მაინც თუ ვაკეთებთ სწორად?

ვიყენებთ მრავალფაქტორულ ავთენტიფიკაციას!

54% იყენებს მრავალფაქტორულ ავთენტიფიკაციას პირადი ანგარიშებისთვის

მხოლოდ 37% იყენებს მრავალფაქტორულ ავთენტიფიკაციას სამსახურის ანგარიშებისთვის

ვენდობით ბიომეტრიას

65% ენდობა თითის ანაბეჭდებს და სახის ამომცნობ ტექნოლოგიებს ტრადიციული ტექსტური პაროლების ნაცვლად

რა არის მრავალფაქტორული ავთენტიფიკაცია?

ეს არის უსაფრთხოების გაძლიერებული დონე. მომხმარებლისა და პაროლის შეყვანის შემდეგ სისტემა ითხოვს დამატებით მონაცემს. (მაგ: ერთჯერადი სმს-კოდი ან თითის ანაბეჭდი.

ყველაზე მეტად ვუფრთხილდებით ფინანსურ და ელ.ფოსტის ანგარიშებს

69% 69% ძლიერ პაროლებს ქმნის ფინანსური ანგარიშებისთვის, 47% კი - ელ.ფოსტისთვის

62% 62% იყენებს მრავალფაქტორულ ავთენტიფიკაციას ფინანსურ ანგარიშებზე და 45% - ელ.ფოსტაზე

კიბერუსაფთხოებისთვის და საკუთრი თავის დასაცავად ბევრი რამ შეგვიძლია გავაკეთოთ. დამატებითი ინფორმაციისთვის გაეცანით www.staysafeonline.org