ონლაინ შესყიდვა (online shopping) სულ უფრო პოპულარული ხდება და ყოველდღიურად იზრდება იმ მომხარებელთა რაოდენობა, რომლებიც არჩევანის მრავალფეროვნების, ფასის, ხარისხის, სიმარტივისა და სხვა მახასიათებლების გამო უპირატესობას **ონლაინ მაღაზიებს** ანიჭებენ. ონლაინ ვაჭრობას თან ახლავს ჩვენს პერსონალურ და ფინანსურ მონაცემთა დაცულობასთან დაკავშირებული რისკები. მათ თავიდან ასაცილებლად კონკრეტული წესები უნდა დავიცვათ.

ონლაინ შესყიდვისას რეკომენდებულია:

1. *ბოქლომის სიმბოლოიანი ვებგვერდის გამოყენება:*

- ონლაინ შესყიდვა ისეთი ვებგვერდიდან განახორციელეთ, რომელსაც მისამართის ველში თან ერთვის **ბოქლომის სიმბოლო,** რაც მიუთითებს ტრანზაქციების დაცულობაზე. ვებგვერდზე ბარათის მონაცემების შეყვანისას, ბოქლომის სიმბოლოსთან ერთად მისამართის პანელი უნდა იწყებოდეს HTTPS://-ის გამოსახულებით (ნაცვლად HTTP://-ისა), სადაც S-ი (secure) მიუთითებს ვებგვერდის უსაფრთხოებაზე.

2. *სანდო ვებგვერდების და მობილური აპლიკაციების (Mobile App) გამოყენება*

- ახალ ვებგვერდზე შესყიდვის განხორციელებამდე წინასწარ მოიძიეთ ინფორმაცია **ვებგვერდის და რეალიზატორის** შესახებ. გაეცანით სხვა მომხმარებელთა შეფასებას და გამოცდილებას.

- არ გახსნათ იმ ვებგვერდის ბმული, რომელიც ელექტრონული ფოსტის **ე.წ. საეჭვო გზავნილების (Spam-ის) საქაღალდეში** შემოვიდა რეკლამის სახით. ასეთი ვებგვერდიდან შესყიდვის განხორციელება საფრთხის შემცველია, რადგან შესაძლოა გახდეთ ე.წ „phishing“-ის (ინტერნეტ-თაღლითობის ფორმა, როდესაც ხდება პირადი დაცული ინფორმაციის მოპარვა) მსხვერპლი, რომელიც ყალბი ელექტრონული ფოსტის დაგზავნით ან ყალბ ვებგვერდზე თქვენი შეტყუებით თქვენი ანგარიშის, პაროლის, ფინანსური და სხვა პერსონალური მონაცემების მითვისებას ისახავს მიზნად. ზოგიერთი კომპანია საეჭვო შეტყობინებით (Spam) ახდენს აკრძალული პროდუქციის ან მომსახურების რეკლამირებას.

- იმ შემთხვევაში, თუ ონლაინ შესყიდვას ახორციელებთ მობილური ტელეფონით, მიზანშეწონილია გადმოწეროთ ის **აპლიკაცია (mobile apps),** რომელიც ამ მაღაზიის მიერ არის ატვირთული **აპლიკაციების მაღაზიაში (app stores).**

- ონლაინ მაღაზიის აპლიკაციები გადმოწერეთ მხოლოდ სანდო წყაროებიდან, როგორებიცაა **Apple App Store-ი ან Google Play.**
- რეკომენდებულია ონლაინ შესყიდვისათვის **სპეციალური ელექტრონული ფოსტის** შექმნა, რაც დაგეხმარებათ პოტენციურად ზიანის შემცველი ელექტრონული გზავნილებისა ან ყალბი შეტყობინებების კონტროლში.

3. უსაფრთხო ფულადი ანგარიშსწორების მეთოდების გამოყენება

- ინტერნეტში ფულადი ანგარიშსწორების მეთოდებს შორის ყველაზე უსაფრთხო არის **პლასტიკური ბარათით ანგარიშსწორება,** რადგან ის იძლევა თანხის დაბრუნების შესაძლებლობას ისეთ შემთხვევებში, როდესაც შესყიდული პროდუქცია არ იგზავნება დანიშნულების ადგილზე ან ადრესატს მიეწოდა არასწორი ნივთი. გამოიყენეთ საკრედიტო ბარათი მაშინაც კი, როდესაც ტრანზაქციას ახორციელებთ ისეთი ელექტრონულ საგადასახადო სისტემის საშუალებით, როგორიცაა **PayPal, Google Wallet, ან Apple Pay.**
- ინტერნეტ შესყიდვებისთვის სასურველია **სპეციალური საკრედიტო ბარათის** გამოყენება, რომელზეც მხოლოდ ლიმიტირებული თანხაა ხელმისაწვდომი. არსებობს ასევე **ბარათის დაზღვევის** შესაძლებლობაც.
- არასოდეს გასცეთ თქვენი **საკრედიტო ბარათის მონაცემები** ელექტრონული ფოსტის საშუალებით.
- გირჩევთ, არ ისარგებლოთ ისეთი ონლაინ მაღაზიებით, რომლებიც ითხოვენ **პასპორტისა და ბარათის ასლების** გაგზავნას.
- ხშირად შეამოწმეთ **საბანკო ანგარიშები** და დარწმუნდით, რომ ადგილი არ აქვს ისეთ დანახარჯებს და ტრანზაქციებს, რომელებიც თქვენ არ განგიხორციელებიათ. ასეთის აღმოჩენის შემთხვევაში დაუყოვნებლივ დაუკავშირდით თქვენს მომსახურე ბანკს.
- ონლაინ ვაჭრობისას ვებგვერდზე საბანკო ბარათის მონაცემების შეყვანისას არ არის სასურველი მონიშნოთ პუნქტი **"დაიმახსოვრე ჩემი ბარათი მომავალი შესყიდვებისთვის"** (remember my card).

4. პირადი კომპიუტერის და დაცული ინტერნეტ მომსახურების, მათ შორის უსადენო ინტერნეტ (Wi-Fi) სერვისების გამოყენება

- არ არის რეკომენდებული საჯარო **უსადენო ინტერნეტ ქსელის (Wi-Fi)** გამოყენებით თქვენ ანგარიშზე შესვლა და ტრანზაქციის განხორციელება.
- ონლაინ შესყიდვისას არ ისარგებლოთ **საერთო მოხმარების კომპიუტერით.** ამ შემთხვევაში სისტემა იმახსოვრებს თქვენ მიერ ინტერნეტში განხორციელებულ ქმედებებს და უცხო ადამიანის მიერ კომპიუტერის შემდგომი მოხმარება ქმნის თქვენ ანგარიშზე წვდომის საფრთხეს.
- გამოიყენეთ **დაცული ინტერნეტ მომსახურების სერვისები,** რადგან დაუცველი ინტერნეტ კავშირის შემთხვევაში, იქმნება თქვენ პერსონალური ინფორმაციაზე, მათ შორის საბანკო მონაცემებზე არასანქცირებული წვდომის რეალური საფრთხე.
- თუ მაინც მოხდა დაუცველი ქსელის მეშვეობით მომსახურების მიღება, რეკომენდირებულია თქვენი **ანგარიშების პაროლების შეცვლა.**
- სასურველია, მონაცემების დაცვის მიზნით მომხმარებელმა გამოიყენოს **უნიკალური და რთული, მრავალფეროვანი სიმბოლოების კომბინაციისგან შემდგარი პაროლი.** პაროლი უნდა იყოს 8-დან 12-მდე სიმბოლოსაგან შემდგარი წინადადება და უნდა შეიცავდეს ციფრებს, დიდ და პატარა ასოებს, რომ ვერ მოხდეს მისი ადვილად გამოცნობა და გატეხვა.
- მაღალი რისკის შემცველია **ერთი და იგივე პაროლის გამოყენება** სხვადასხვა ონლაინ მაღაზიებით სარგებლობისას. იმ შემთხვევაში, თუ ყველა ონლაინ მომსახურების მიღებისას გამოიყენება იდენტური მომხმარებლის სახელი და პაროლი, ერთ-ერთ ანგარიშზე უნებართვო წვდომის შემთხვევაში, მომხმარებლის სხვა ანგარიშებიც დგება საფრთხის ქვეშ.

5. პერსონალური მონაცემების მოცულობის კონტროლი

- ინტერნეტ შესყიდვისას ყურადღება გაამახვილეთ თუ რა სახის პერსონალურ ინფორმაციას ითხოვს ვებგვერდი ტრანზაქციის დასასრულებლად. როგორც წესი, ონლაინ მაღაზიას ვაჭრობის განსახორციელებლად არ სჭირდება ისეთი ინფორმაცია, როგორიცაა **თქვენი პირადი ნომერი, თუმცა ესაჭიროება მისამართი და საბანკო ბარათის რეკვიზიტები.**

- გაეცანით მაღაზიის მონაცემთა დამუშავების წესებს, რომელიც, როგორც წესი, მოცემულია კონფიდენციალობის პოლიტიკის დოკუმენტში **(Privacy Policy).**