OUCH!

ამ გამოცემაში...

- ყალბი ონლაინ მაღაზიები
- თქვენი კომპიუტერი / მობილური მოწყობილობა
- თქვენი საკრედიტო ბარათი

ონლაინ შოპინგი - უსაფრთხოდ

მიმოხილვა

ახლოვდება სადღესასწაულო სეზონი და მალე მილიონობით ადამიანი მთელი მსოფლიოდან გადაწყვეტს საჩუქრების შეძენას.მრავალი ჩვენგანი აირჩევს ონლაინ შოპინგს, იმისათვის რომ იპოვოს საუკეთესო შემოთავაზებები და აირიდოს რიგში დგომა. სამწუხაროდ, ამ პერიოდს კიბერ კრიმინალებიც იყენებენ, რათა შექმნან ყალბი შოპინგის საიტები სადაც ითაღლითებენ და მოიპარავენ. ქვემოთ ჩვენ აგიხსნით ონლაინ შოპინგის რისკებს და ასევე იმას თუ როგორ მოიპოვოთ შესანიშნავი შეთავაზებები უსაფრთხოდ.

მოწვეული რედაქტორი

ლენი ზელსტერი (Lenny Zeltser) ქმნის უსაფრთხოების პროდუქტებს Minerva Labs-ში და ასწავლის მავნე პროგრამებთან ბრძოლას SANS Institute-ში. ლენი აქტიურია Twitter-ზე შემდეგი დასახელებით - **@lennyzeltser** და აქვს საკუთარი ბლოგი, მისამართზე **zeltser.com**.

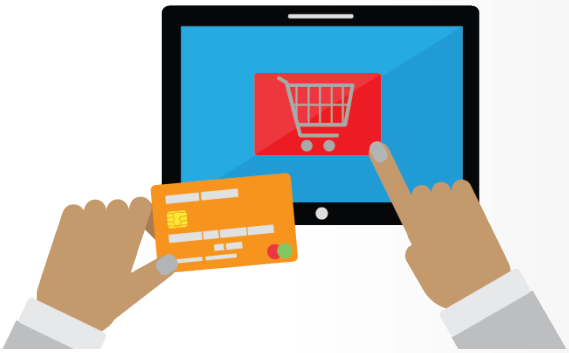
ყალბი ონლაინ მაღაზიები

მრავალ ლეგიტიმურ ონლაინ მაღაზიასთან ერთად, არსებობს კიბერ კრიმინალების მიერ შექმნილი ყალბი ვებ-საიტები. კრიმინალები ქმნიან ასეთ ყალბ ვებ-საიტებს ისე, რომ მაქსიმალურად მიამსგავსონ რეალურს ან იყენებენ კარგად ნაცნობი მაღაზიების სახელებს და ბრენდებს. შემდეგ ისინი იყენებენ ყალბ ვებსაიტებს იმ ხალხის მოსატყუებლად ვინც ეძებს საუკეთესო შეთავაზებებს. როდესაც თქვენ ინტერნეტით ეძებთ აბსოლიტურად დაბალ ფასებს, თქვენ შეიძლება აღმოჩნდეთ ერთერთ ასეთ ყალბ ვებსაიტზე. როდესაც ირჩევთ ვებსაიტს შენაძენის გასაკეთებლად, უფრთხილდით იმ საიტებს სადაც ფასები გაცილებით დაბალია ვიდრე ყველა შესაბამის მსგავს საიტზე ან საიტი გთავაზობთ ისეთ პროდუქტებს რაც ქვეყნის მასშტაბით არსად აღარაა გაყიდვაში. მათი პროდუქტები ასე იაფია იმის გამო, რომ თქვენს მიერ მიღებული პროდუქტი იქნება არალეგიტიმური, ყალბი, მოპარული, ან ზოგ შემთხვევაში საერთოდ ვერ მიიღებთ მას. დაიცავით თავი შემდეგი რჩევების გათვალისწინებით:

- შეძლებისდაგვარად შეიძინეთ იმ ვებსაიტებიდან რომელთაც უკვე იცნობთ, ენდობით და ადრე უკვე გამოგიყენებიათ.
- დარწმუნდით რომ ვებსაიტს აქვს ლეგიტიმური საფოსტო მისამართი და ტელეფონის ნომერი გაყიდვებისა და მხარდაჭერის თემებთან დაკავშირებით. თუ საიტი საეჭვოდ გამოიყურება, დარეკეთ და გაესაუბრეთ პიროვნებას. თუ თქვენ ვერ მოახერხებთ ვეინმესთან დალაპარაკებას, ეს შეიძლება გახდეს პირველი მიზეზი მაღაზიის სინამდვილეში ეჭვის შესატანად.
- დააკვირდით ისეთ შემოთავაზებებს რაც ძნელი დასაჯერებელია, ასევე გრამატიკას და მართლწერას.

ონლაინ შოპინგი - უსაფრთხოდ

- განსაკუთრებით დაუკვირდით ისეთ ვებსაიტებს რომლებიც თქვენთვის უკვე ნაცნობი საიტების ზუსტი ასლია, მაგრამ აქვს სხვა დომეინის სახელი ან მაღაზიის სახელი ოდნავ განსხვავებულია. მაგალითად, თქვენ შეიძლება ხშირად შოპინგობდეთ Amazon-ზე, რომლის მისამართია https://www.amazon.com. მაგრამ განსაკუთრებით უფრთხილდით საიტებს რომლებიც თავს ასაღებენ Amazon-ად, მაგალითად შემდეგი მისამართის გამოყენებით http://store-amazoncom.com
- საძიებო სისტემის გამოყენებით მოძებნეთ ონლაინ მაღაზიის სახელი და გაარკვიეთ რას ამბობენ სხვები ამ საიტის შესახებ. დაუკვირდით შემდეგ ფრაზებს “fraud”, “scam”, “never again” ან “fake.” ასეთი განხილვების არარსებობაც შეიძლება ნიშნავდეს იმას რომ საიტი ძალიან ახალია და ნაკლებად სანდო.
- სანამ რაიმეს შეიძენთ დარწმუნდით რომ თქვენი კავშირი ვებსაიტთან დაშიფრულია. ბევრი ბრაუზერი დაშიფრულ კავშირს ადასტურებს გასაღების, კლიტის ან სიტყვა HTTPS-ის მწვანედ გამოსახვით ვებსაიტის მისამართის წინ.



დაიცავით თავი ონლაინ, იშოპინგეთ მხოლოდ სანდო და მაღალი რეპუტაციის ვებ საიტებზე.

დაიმახსოვრეთ! მხოლოდ ის ფაქტი რომ საიტი გამოიყურება პროფესიონალურად არ ნიშნავს მის ლეგიტიმურობას. თუ თქვენთვის საიტი არაკომფორტულია და გაქვთ გარკვეული ეჭვები, არ გამოიყენოთ ის. გამოიყენეთ კარგად ნაცნობი ვებსაიტი რომელსაც ენდობით და სადაც ადრე უკვე გიშოპინგიათ. თქვენ შეიძლება იქ ვერ იპოვოთ საოცარი შემოთავაზება, მაგრამ მეტი შანსია მიიღოთ ლეგიტიმური პროდუქტი და თავიდან აირიდოთი თქვენი პერსონალური და ფინანსური ინფორმაციის მოპარვა.

თქვენი კომპიუტერი / მობილური მოწყობილობა

ლეგიტიმურ ვებსაიტებზე შოპინგთან ერთად, თქვენ უნდა დარწმუნდეთ რომ თქვენი კომპიუტერი ან მობილური მოწყობილობა უსაფრთხო და დაცულია. კიბერ კრიმინალები ეცდებიან დააინფიცირონ თქვენი მოწყობილობები იმისათვის რომ შეძლონ საბანკო ანგარიშების, საკრედიტო ბარათების ინფორმაციის და პაროლების მოპარვა. გაითვალისწინეთ შემდეგი რჩევები თქვენი მოწყობილობების დასაცავად:

- თუ სახლში გყავთ ბავშვები, განიხილეთ 2 მოწყობილობის ქონა, ერთი თქვენი ბავშვებისთვის და მეორე უფროსებისთვის. ბავშვები ინტერესიანები და ინტერაქტიულები არიან ტექნოლოგიების მიმართ, შედეგად მეტი შანსია დაინფიცირდეს მათი მოწყობილობა. სხვა კომპიუტერის ან ტაბლეტის გამოყენებით ონლაინ შოპინგის და საბანკო ტრანზაქციებისთვის, თქვენ შეამცირებთ დაინფიცირების შანსებს.
- ყოველთვის დააყენეთ ბოლო განახლებები (Updates) და გამოიყენეთ განახლებული ანტივირუსი. ეს ყველაფერი კიბერ კრიმინალებს გაურთულებს თქვენი მოწყობილობის დაინფიცირებას.

ონლაინ შოპინგი - უსაფრთხოდ

თქვენი საკრედიტო ბარათი

რეგულარულად განიხილეთ თქვენი საკრედიტო ბარათის ამონაწერი, იმისათვის რომ აღმოაჩინოთ საეჭვო გადარიცხვები, განსაკუთრებით მას შემდეგ რაც განახორციელეთ ონალინ შეძენა ან გამოიყენეთ ახალი ვებსაიტი. ზოგი საკრედიტო ბარათის პროვაიდერი გაძლევთ საშუალებას მიიღოთ ტრანზაქციების შესახებ ინფორმაცია სმს-ით ან ელექტრონული ფოსტით ყოველი გადახდისას ან როდესაც გადახდა სცდება განსაზღვრულ ოდენობას. ასევე შეგიძლიათ იქონიოთ ბარათი რომელსაც მხოლოდ ონალინ შოპინგისთვის გამოიყენებთ. თუ ამ ბარათის კომპრომეტირება მოხდება და მონაცემებს მოგპარავენ, შეძლებთ მის შეცვლას ახლით და შესაბამისად თქვენს არა ონლაინ გადასახადებს და ფინანსურ აქტივობას ეს არ შეეხება. თუ ფიქრობთ რომ თაღლითობის მსხვერპლი ხართ, დაუყოვნებლივ დაუკავშირდით საკრედიტო ბარათის გამცემ კომპანიას/ბანკს. ეცადეთ გამოიყენოთ საკრედიტო ბარათი ყველა ონლაინ შენაძენის გასაკეთებლად და თავიდან აირიდოთ სადებეტო ბარათების გამოყენება იქ სადაც შესაძლებელია. სადებეტო ბარათები იღებს თანხას პირდაპირ თქვენი საბანკო ანგარიშიდან, შესაბამისად გაცილებით ძნელი იქნება თანხის დაბრუნება თაღლითობის შემთხვევაში. ბოლო რჩევის სახით, გამოიყენეთ საკრედიტო ბარათები რომლებიც აგენერირებენ უნიკალურ ბარათის ნომერს ყოველი ონლაინ შეძენისას, ასევე სასაჩუქრე ბარათები, ან გამოიყენეთ ცნობილი საგადასახადო სერვისები, მაგალითად PayPal, რომლებიც არ გადასცემენ თქვენი საკრედიტო ბარათის ნომერს ვენდორებს (ონლაინ მაღაზიებს).

მეტის გაგება / დამატებითი ინფორმაცია

გამოიწერეთ ყოველთვიური OUCH! უსაფრთხოების ცნობიერების ამაღლების გამოცემა, ისარგებლეთ OUCH! არქივით, და შეიტყვეთ უფრო მეტი SANS-ის უსაფრთხოების ცნობიერების ამაღლების გადაწყვეტილებების შესახებ ჩვენს საიტზე securingthehuman.sans.org/ouch/archives.

რესურსები

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Four Steps to Staying Secure:	https://securingthehuman.sans.org/ouch/2016#october2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

სარედაქციო საბჭო: Walt Scrivens, Phil Hoffman, Bob Rudis, Cherul Conley
ტექსტი თარგმნა: გიორგი გურგენიძე