ფიშინგი

ფიშინგი (ინგლისურად fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები, მაგალითად პაროლი, საკრედიტო ბარათის ან საბანკო ანაგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია.

ფიშინგისას შენიღბული ინტერნეტ კომუნიკაციის საშუალებით ხდება მომხმარებლის შესახებ ისეთი ინფორმაციის მოპოვება, როგორიცაა მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი. ეს მიიღწევა შემდეგი მეთოდებით: მასიური ელექტრონული წერილების დაგზავნით (წერილის ავტორებად იყენებენ ცნობილ ორგანიზაციებს და ბრენდებს), ასევე პირადული შეტყობინებებით სადაც იყენებენ ბანკის სახელს, მეილ სერვერების გამოყენებით და სოციალური ქსელების საშუალებებით. წერილში ხშირად არის ვებ გვერდის ბმული, რომლის ვიზუალური მხარე არ განსხვავდება ნამდვილისგან. შესაბამისად გაყალბებულ ვებ გვერდზე შეტანილი ინფორმაცია: მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი ავტომატურად ხვდება ეგრედ წოდებული "ფიშერი"-ს ხელში.

ფიშინგის ისტორია - პირველი სტატია ფიშინგზე და ფიშინგის განხორციელების მეთოდებზე 1996 წელს დეტალურად იქნა აღწერილი ხაკერულ ჟურნალში "2600: The Hacker Quarterly".

ახალი საფრთხეები - დღევანდელ დღეს ფიშინგი ცდება უბრალოდ ინტერნეტ-თაღლითობას, ყალბი ვებ-გვერდების არსებობა გახდა თაღლითობის მრავალი მიმართულებიდან ერთ-ერთი ყველაზე აქტუალური და საგანგაშო. წერილი რომელიც თითქოს ბანკიდან არის გამოგზავნილი შეიძლება მომხმარებელს მოუწოდებდეს მითითებულ ნომერზე სავალდებულოდ დაკავშირებისაკენ, რათა მოგვარებული იქნას მის საბანკო ანგარიშზე არსებული პრობლემა. ამ მეთოდს ეწოდება ვიშინგი "ViShing" (ხმოვანი ფიშინგი). აღნიშნულ ნომერზე დარეკვის შემდეგ მომხმარებელი ხვდება ავტო მოპასუხესთან, რომელიც სთხოვს ინფორმაციას სხვადასხვა პირად მონაცემებზე, მაგალითად პინ-კოდი, ანგარიშის ნომრები, პაროლები და ა.შ. ასევე "ვიშერი"-ბი თავადაც რეკავენ მსხვერპლთან და არწმუნებენ მათ, რომ ისინი ოფიცილური ორგანიზაციიდან არიან, რისთვისაც იყენებენ ყალბ სატელეფონო ნომრებს. საბოლოოდ კი მოიპოვებენ მომხმარებლის პირად ინფორმაციას.

აგრეთვე ძალიან პოპულარული ხდება SMS-ფიშინგი, ცნობილი როგორც სმიშინგი "SMiShing". თაღლითები თავის მსხვერპლს უგზავნიან SMS შეტყობინებას სადაც მოთავსებულია ფიშინგ საიტის ბმული. ბმულზე შესვლისთანავე მომხმარებელი ხდება ფიშერის მსხვერპლი და კარგავს პირად ინფორმაციას. SMS შეტყობინება

აგრეთვე შეიძლება მოუწოდებდეს მომხმარებელს მითითებულ ნომერზე დაუყონებლივ დაკავშირებას, რათა მისი პრობლემა იქნას გადაჭრილი.

ფიშინგ წერილი - ფიშინგ წერილი არის ელექტრონული ფოსტის მისამართზე მოსული ყალბი წერილი, რომელიც თითქოს გამოგზავნილია ბანკის, სერვის პროვაიდერის ან სხვა ცნობილი ბრენდ ორგანიზაციის მიერ, რომელთანაც მომხმარებელს აქვს შეხება, სადაც რაიმე მიზეზით სთხოვენ მას გაანახლოს თავისი პირადი მონაცემები მითითებული ბმულის საშუალებით. დასახელებული მიზეზი შეიძლება იყოს სხვადასხვაგვარი, მაგალითად ასეთი ყალბი წერილი შეიძლება იტყობინებოდეს, რომ მომხმარებლის ანგარიში იქნება შეჩერებული თუ არ მოხდა მისი პაროლის ან საკრედიტო ბარათის ინფორმაციის განახლება მოცემულ ვებ გევრდზე.

ფიშინგ წერილების დამახასიათებელი ნიშანია მაღალი ხარისხის გაყალბება. მაგალითად მიმღები იღებს წერილებს ბანკის ან სერვის პროვადერის ლოგოთი , რომელიც არის ორიგინალის ზუსტი ასლი. მომხმარებელი, რომელიც ვერ ხვდება ტყუილს გადადის არა ოფიციალურ ვებ გვერდზე არამედ ყალბზე, რომელიც ასევე ვიზუალურად ძალიან ჰგავს ცნობილი კომპანიის ვებ გვერდს მხოლოდ მისამართია განსხვავებული და ინფორმაციის შეგროვების შემდეგ შეიძლება მოხდეს მომხმარებლის გადამისამართება რეალურ ვებ-გვერდზე.

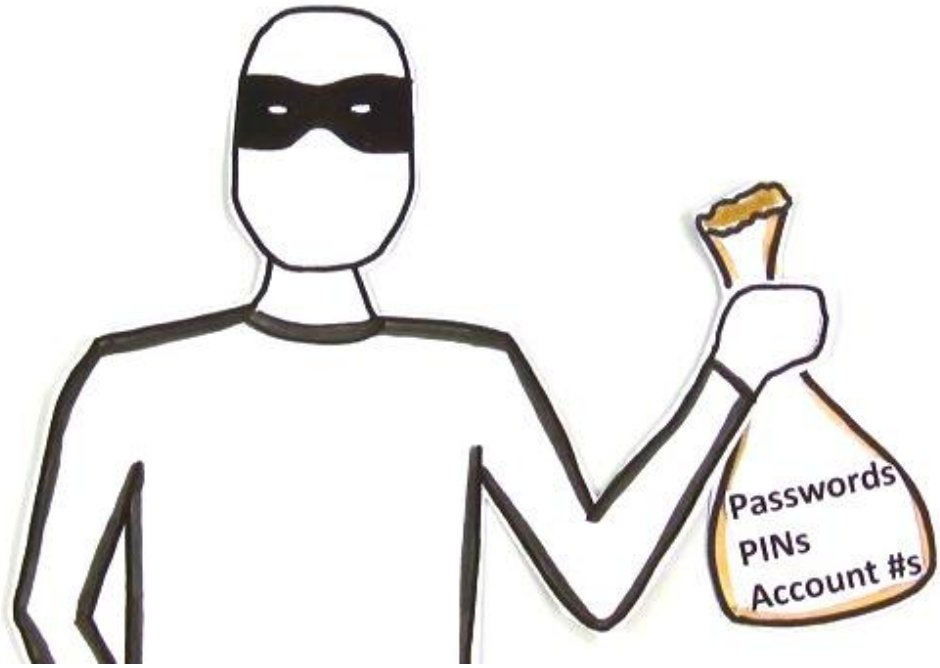
ფიშინგ ვებ გვერდი - როდესაც მომხმარებელი გადადის ყალბ ვებ გვერდზე და მითითებულ ველებში შეჰყავს თავისი მომხმარებლის სახელი, პაროლი და საბანკო რეკვიზიტები თაღლითებისთვის ხელმისაწვდომი ხდება მისი ელექტრონული ფოსტა ან თუნდაც ინტერნეტ ბანკინგის მონაცემები. აღსანიშნავია ისიც, რომ ყველა "ფიშერი" თავად არ იყენებს მოპოვებულ ინფორმაციას, ისინი ყიდიან სხვა პირებზე

რომლებსაც აქვთ კარგად შემუშავებული გეგმა თუ როგორ უნდა მოიპარონ ფული სხვისი ანგარიშებიდან.

როგორც წესი ფიშინგ ვებ გვერდი ფუნქციონირებს მხოლოდ რამდენიმე დღე (საშუალოდ 5-10), რადგან ანტი-ფიშინგ ფილტრები დროულად პოულობენ ახალ საშიშროებებს და ამის გამო ფიშერებს უწევთ სულ ახალ-ახალი ვებ გვერდების რეგისტრაცია ან არსებული სხვა ვებ გვერდების გატეხვა და მალულად ფიშერული საიტის განთავსება, მაგრამ ვებ გვერდების ვიზუალური მხარე მაინც უცვლელი რჩება და ძალიან ჰგავს კომპანიის რელურ ვებ-გვერდს.

<u>როგორ ხორციელდება ფიშინგი</u> - ფიშინგის ყველაზე ხშირ სამიზნეს წარმოადგენენ ბანკები, საფინანსო ორგანიზაციები, ელექტრონული აუქციონები და ინტერნეტ მაღაზიები. ვინაიდან თაღლითებს სურთ მოიპოვონ ინფორმაცია, რომელიც იძლევა ფულთან წვდომის საშუალებას. აგრეთვე პოპულარულია ელექტრნული ფოსტის მონაცემების მოპარვა, რათა შემდგომში გამოიყენონ სპამის და ვირუსების გასავრცელებლად.

ფიშერების კიდევ ერთი ხრიკი არის ბმულის URL მისამართები, რომელიც ძალიან ჰგავს ნამდვილი ვებ გევრდის სახელს და კარგი დაკვირვების გარეშე მომხმარებელმა შეიძლება ვერ შეამჩნიოს ასოების ცდომილება. ასევე ყალბი ვებ გვერდი შეიძლება იწყებოდეს IP მისამართით და გრძელდებოდეს ორგანიზაციის სახელით, ან მითითებული იყოს რაიმე სხვა ვებ გევრდი, რომელზეც მიბმულია სხვა ვებ გვერდის მისამართი.

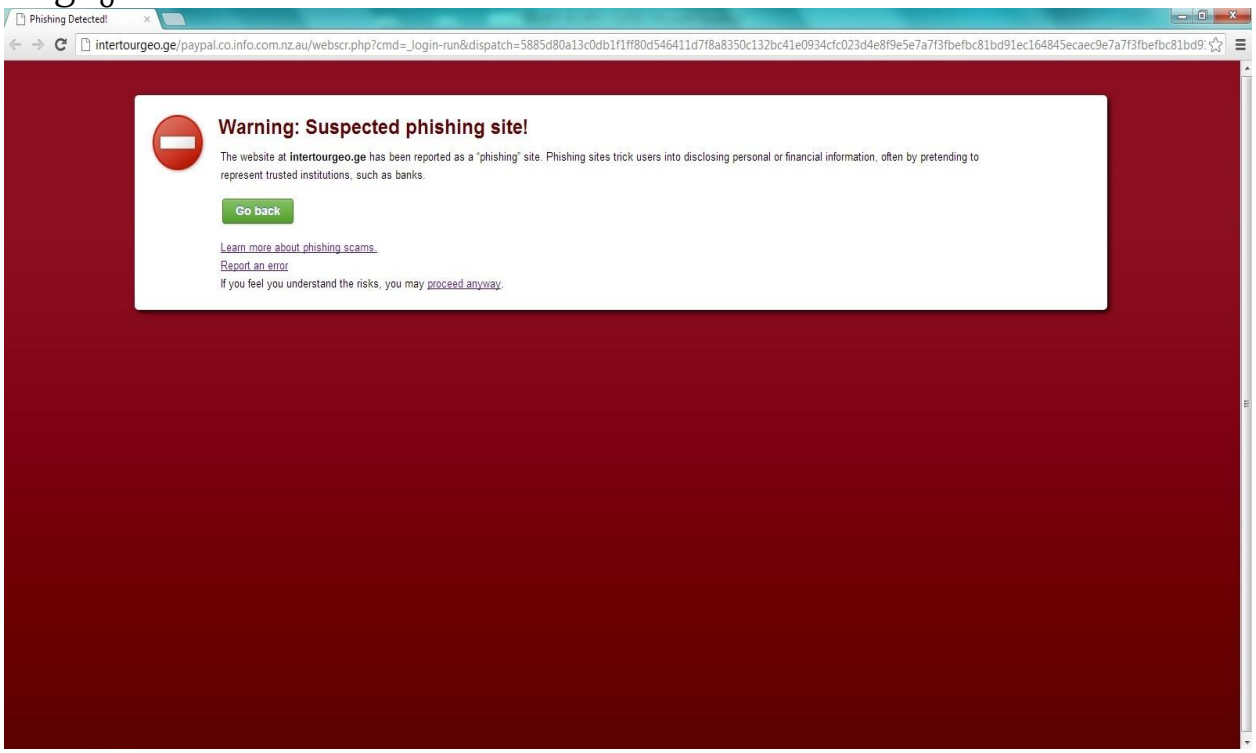


პირადი მონაცემების მოპარვა არ არის ერთადერთი საფრთხე რომელიც მომხმარებელს შეიძლება შეემთხვეს. ფიშინგური ვებ გვერდი შეიძლება ასევე შეიცავდეს მავნე ან შპიონურ პროგრამას, ასე რომ თუ თქვენ არ გაქვთ არანაირი ანგარიში, რომელითაც შეიძლება თაღლითები დააინტერესდნენ, ეს იმას არ ნიშნავს რომ თქვენ ხართ უსაფრთხოდ, რადგან ფიშინგური შეტევების წარმატება დაფუძნებულია მომხმარებელთა გაუთვითცნობიერებაზე ან უყურადღებობაზე.

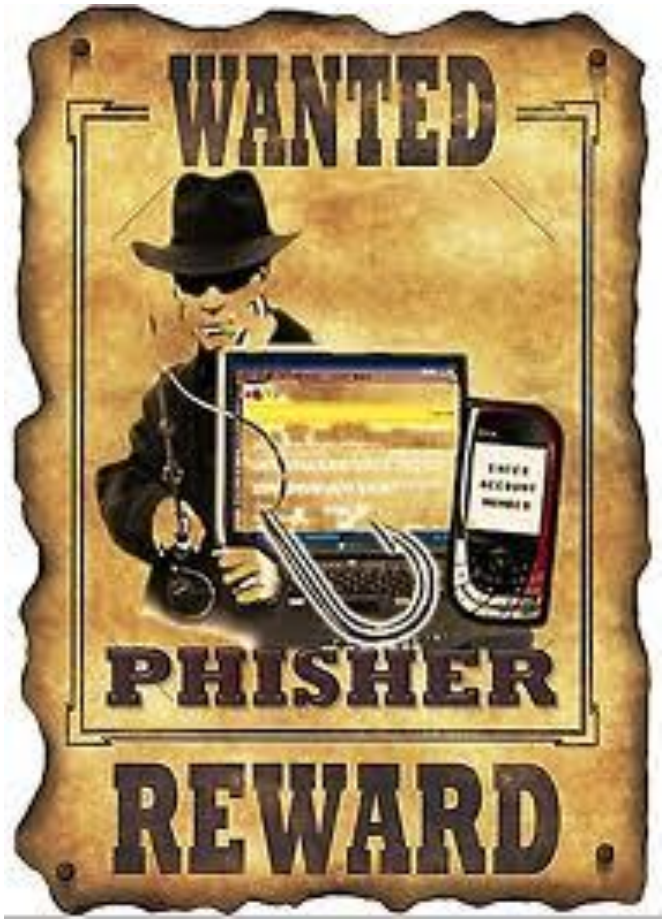
ფიშერები ხშირად იყენებენ გამოსახულებას ტექსტის ნაცვლად, რის შემდეგაც ანტიფიშინგის ფილტრებს ურთულდებათ მათი აღმოჩენა. მაგრამ სპეციალისტებმა შეიმუშავეს მეთოდი რომელიც მეილში მოსულ გამოსახულებას ადარებს ანტიფიშინგის ბაზას და ამის შემდეგ ბლოკავს მას თუ მეილში აღმოაჩენს ფიშინგის ელემენტებს.

<u>ინტერნეტ ბრაუზერები, რომლებიც იუწყებიან ფიშინგის საფრთხეს</u> - ძალიან მნიშვნელოვანი მიმართულება იყო ფიშინგ საიტების სიის შექმნა (ეგრეთ წოდებული ბლექლისტი), რომელსაც აქტიურად იყენებენ ისეთი ინტერნეტ ბრაუზერები როგორიცაა: Internet Explorer, Mozilla Firefox, Google Chrome, Safari და Opera.

2006 წელს შეიქმნა DNS სერვისების მეთოდი , რომლებიც ფილტრავენ ცნობილ ფიშინგ საიტებს, ეს მეთოდი მუშაობს ყველა ზემოთ ჩამოთვლის ინტერნეტ ბრაუზერში.



ფიშინგთან ბრძოლა - რამდენიმე წლის წინ ფიშინგთან საბრძოლველად შეიქმნა ანტი-ფიშინგის სამუშაო ჯგუფი (Anti-Phishing Working Group - APWG), სადაც გაერთიანებულები არიან ფიშინგის სამიზნე კომპანიები, ასევე უსაფრხოების პროგრამული უზრუნველყოფის მწარმოებლები და კიბერ დანაშაულთან მებრძოლი კომპანიები, ჯამში 2500 კომპანიაზე მეტი. APWG-ს წევრები ატყობინებენ ერთმანეთს ახალი ფიშერული შეტევების შესახებ და ერთად ზრუნავენ ამ საკითხთან დაკავშირებით საზოგადოების განათლებაზე.


WANTED
PHISHER
REWARD