სპამი

სპამი (ინგლ. **Spam, Bulk** ან **Junk**) არის ელექტრონული წერილის ტიპი, რომელიც იგზავნება პიროვნების ან კომპანიის მიერ, მიმღების დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა. პიროვნებას, რომელიც მსგავს წერილებს გზავნის ეწოდება სპამერი. მათი ძირითადი მიზანია თავიანთი პროდუქტის პოპულარიზაცია.

<u>როგორ ხვდება ჩვენი იმეილი სპამერის ხელში</u> - სპამერისთვის ყველაზე რთულია იმ მისამართების ხელში ჩაგდება, რომელთაც უნდა გაუგზავნოს ესა თუ ის მეილი. რადგან აქ ლაპარაკია არა ერთ და ორ, არამედ ათასობით მეილზე. ამისთვის სპამერები რამოდენიმე ხერხს მიმართავენ:

- ცნობილი კომპანიის მომხმარებლების ბაზის გატეხვა.
- კომპანიის თანამშრომლისგან არაოფიციალური გზით მომხმარებლის მონაცემების შეძენა.
- სხვადასხვა ყველასათვის ნაცნობი და საზოგადო საიტებიდან მონაცემების ამოღება სპეციალური პროგრამებით. (მაგ: Harvester).

- კომპიუტერიდან რომელიც დაინფიცირებულია ტროიანით შესაძლებელია მოიპოვო ყველა მეილი, რომელზეც მოხდა მიმოწერა დაინფიცირებული კომპიუტერით.
- სპამერებს აქვთ გავრცელებული სახელების ბიბლიოთეკა, რომელსაც სხვადასხვა კომბინაციებით იყენებენ და იგებენ უამრავ მეილს.

<u>რა არის სპამი?</u> - სპამი არის ელექტრონული წერილის ტიპი, რომელიც მასობრივად და ანონიმურად იგზავნება მიმღების ელექტრონული ფოსტის მისამართზე, მის დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა და განკუთვნილია რაიმე მომსახურების ან საქონლის რეკლამირებისათვის (პოტენციის ასამაღლებელი აბების რეკლამა, ფიქტიური კომპანიებისგან საფონდო ბირჟებზე მომხიბვლელი გარიგებების შესახებ მოწვევები და უამრავი სხვა დამაინტრიგებელი წინადადება).

პიროვნებას, რომელიც მსგავს წერილებს აგზავნის ეწოდება სპამერი. გარდა რეკლამისა ბოროტმოქმედები სპამს იყენებენ ფიშინგური შეტევების განსახორციელებლად ან მავნე პროგრამების გასავრცელებლად. მიუხედავად იმისა, რომ ინტერნეტ მომხმარებლების უმეტესობამ იცის სპამის შესახებ და უარყოფითად

აფასებს მას, არის ასევე ბევრი ისეთი პიროვნება ვინც ხდება სპამის მსხვერპლი. მრავალ ქვეყანაში სპამირება ისჯება კანონით.

ყოველდღიურად მსოფლიოში მილიარდობით ელექტრონული წერილი იგზავნება და სტატისტიკურად ელექტრონული წერილების ტრაფიკის 80%-ზე მეტი არის სპამი! შესაბამისად ნორმალური წერილების რაოდენობა არის 20%-ზე ნაკლები.

<u>სპამის სახეობები</u> - ყველაზე გავრცელებული სპამის სახეობებია:

- ლეგალური პროდუქციის რეკლამა, რომლის ღირებულებაც დაბალია.
- არალეგალური პროდუქციის რეკლამა, რომელიც აკრძალულია კანონით.
- კონკურენტი პროდუქციის ანტირეკლამა.
- ფიშინგი, რომელიც ხდება სპამ მეილის მიღების შემდეგ.

<u>რა არის სპამ ბოტი?</u> - სპამ ბოტი არის სპეციალური პროგრამა, რომელიც აგროვებს ელ-ფოსტის მისამართებს ინტერნეტში. სპამ ბოტი ავტომატურად ათვალიერებს სხვადასხვა ვებ გვერდებს, ფორუმებს, ბლოგებს და ტექსტში ეძებს ელ-ფოსტის მისამართს, შემდგომ ნაპოვნი ელ-ფოსტის მისამართები ხვდება სპამერების წერილების მასობრივი დაგზავნის სიაში, რის საშუალებითაც ისინი აგზავნიან სპამს.

თუ თქვენ ღია ტექსტით რომელიმე ვებ გვერდზე გაქვთ განთავსებული ან

დაფიქსირებული თქვენი ელ-ფოსტის მისამართი, დაწრმუნებული იყავით რომ სპამ-ბოტი იპოვის მას, რის შემდგომაც მოგივათ აუარებელი სპამ წერილები, ამიტომ არ გამოაქვეყნოთ თქვენი ელ-ფოსტის მისამართი ვებ-გვერდზე ან ფორუმზე.

ვინაიდან სპამ ბოტი არის მავნე პროგრამა, მას აქვს ასევე სპამის დაგზავნის ფუნქციაც. მან შეიძლება თქვენი კომპიუტერის საშუალებით გააზვნოს ათასობით სპამ წერილი სხვადასხვა ელექტრონულ მისამართზე. მომხმარებლისთის სპამ ბოტის არსებობა მის კომპიუტერში არის ძალზედ სახიფათო, რადგან მისი კომპიუტერის IP მისამართიდან გაგზავნილი სპამი ადრე თუ გვიან მოხვდება რომელიმე შავ სიაში (სპამის ბლოკირების სიები, რომელიც საშუალებას აძლევს ადმინისტრატორებს დაბლოკონ წერილები იმ სისტემებიდან, რომლებსაც აქვთ სპამის დაგზავნის ისტორია), რის შემდგომ მას შეექმენა პრობლემა გააგზავნოს ჩვეულებილივი წერილები, ვინადან თუ მისი IP მისამართი დაფისქსირებულაი რომელიმე შავ სიაში, მიმღების სერვერი ავტომატურად დაბლოკავს მისგან მოსულ ნებისმიერ წერილს. ეს ძალზედ მნიშვენელოვანია ორგანიზაციებისათვოს რომელთაც აქვთ თავიანთი მეილ-სერვერი, რადგან თუნდაც ერთმა მომხმარებელმა შეიძლება შეუქმნას პრობლემა ყველა სხვა მომხმარებელს, რომელიც იყენებს სამსახურებრივ ელ-ფოსტას.

თქვენ შეგიძლიათ შეამოწმოთ თქვენი IP მისამართი შავ სიებში არსებობის შესახებ:

შეამოწმეთ: http://www.mxtoolbox.com/blacklists.aspx და http://www.dnsbl.info

OK - ნიშნავს რომ თქვენი IP მისამართი არის წესრიგში.
Listed - ნიშნავს რომ თქვენი IP მისამართი შეტანილია შესაბამის შავ სიაში.

ბრძოლა სპამთან - აშკარაა, რომ სპამს მოაქვს სერიოზული ეკონომიკური სარგებელი სპამის შემკვეთებისათვის. ამდენად ყველაზე საიმედო გზაა, რომ სპამით მოსულ

რეკლამაზე თქვა უარი და არ შეიძინო სპამით რეკლამირებული ნივთი. სპამისაგან 100% დაცვა არ არსებობს და მთლიანად სპამ წერილებისგან თავის არიდება რთულია, ვინაიდან სპამერებიც არ ჩამორჩებიან დაცვის სისტემებს და სულ ახალ მეთოდებს იგონებენ, რათა მათმა წერილებმა მიაღწიოს ადრესატამდე. ამისათვის თვითონ მომხმარებელმაც უნდა დაიცვას რამოდენიმე წესი რათა მისი ელქტრონული ფოსტის მისამართზე არათუ მომრავლდეს არამედ შემცირდეს სპამის რაოდენობა. გთხოვთ გაითვალისწინოთ შემდეგი რეკომენდაციები:

- **არ უპასუხოთ სპამ წერილებს** - ამით თქვენ ადასტურებთ რომ თქვენი ელ-ფოსტის მისამართი არის აქტიური და ამის შემდეგ უფრო მეტი არასასურველი წერილი მოგივათ.

- **არ გახსნათ სპამ წერილში მითითებული არცერთი ლინკი (ბმული) რა შინაარსისაც არ უნდა იყოს ის**, ლინკზე დაჭერით შესაძლოა გადახვიდეთ სახიფათო ვებ-გვერდზე.

- **არ გახსნათ სპამ წერილში თანდართული ფაილი (attachment)**, რადგან შეიძლება შეიცავდეს ვირუსს ან მავნე პროგრამას.

- **არ გამოაქვეყნოთ თქვენი ელ-ფოსტის მისამართი ვებ-გვერდზე ან ფორუმზე**, რადგან სპამ ბოტები ათვალიერებენ ვებ გვერდებს და ელ-ფოსტის მისამართის პოვნისას ავტომატურად შეაქვთ სპამ სიაში.

- **შექმენით დამატებითი ელ-ფოსტის მისამართი** - თუ თქვენ ხშირად რეგისტრირდებით სხვადასხვა ვებ გვერდზე, ონლაინ სერვისებზე ან რაიმეს ყიდულობთ ინტერნეტის მეშვეობით. ამისათვის შექმენით სხვა ელ-ფოსტის მისამართი(ები), ეს მოგცემთ საშუალებას თქვენს ძირითად მისამართზე ნაკლები ”ნაგავი” მოვიდეს.

- **არ გადაამისამართოთ უცნობი წერილები** - თუ თქვენ უცნობისაგან მოგივიდათ წერილი, სადაც გთხოვენ გაავრცელოთ რაიმე ინფორმაცია და გადაუგზავნოთ თქვენს მეგობრებს, არ გააგზავნოთ რადგან ამ გზით სპამერს შეუძლია უფრო მეტი ელ-ფოსტის მისამართის გაგება.

- **გამოიყენეთ თქვენი ელ-ფოსტის პროგრამის ფილტრი** (Outlook, Thunderbird, The Bat, Live Mail), თქვენი სურვილის მიხედვით შეგიძლია შექმნათ წესები (rule) სადაც მიუთითებთ რის მიხედვით (From, Subject, Text), დაიბლოკოს არასასურველი წერილები ან გადაამისამართოთ სხვა ყუთში.

- **გამოიყენეთ ანტივირუსი** - ბევრ თანამედროვე ანტივირუსულ პროგრამებს გააჩნია ანტი-სპამ ფუქნცია.