**ლექცია № 8 ვირუსები და მათთან ბრძოლა**

კომპიუტერული ვირუსების გამოჩენა 1980 წლიდან დაიწყო, როდესაც ისინი სწრა­ფად ვრცელდებოდნენ ინფიცირებული დისკეტების საშუალებით. ბოლო წლებში ისინი სულ უფრო მეტად მავნე და მომხმარებლისათვის შეუმჩნეველნი გახდნენ.

*ცოტა ისტორია.* პირველად ტერმინი ”კომპიუტერული ვირუსი” იხმარა ამერიკელმა მეცნიერმა **ფრედი კოენმა** (Fred Cohen) 1983 წელს, თუმცა ის პროგრამები, რომლებიც ამ ტერმინის განმარტების ქვეშ ექცეოდნენ, ადრეც არსებობდნენ. პირველ კომპიუტე­რულ ვირუ­სად ითვლება თამაში “Pervading Animal”, რომელიც 1960 წელს გამოჩნდა და არ იყო შექმნილი ვინმესთვის ზიანის მისაყენებლად, მაგრამ ვირუსის საბაზისო თვისებას ამჟღავნებდა - შეეძლო გამრავლება. ეს თვისება, (გამრავლება), ავტორის - **ჯონ ვოლ­კერის** მიერ არ იყო მიზანმიმართულად შექმნილი, ის წარმოადგენდა კო­დის შეცდო­მის შედეგს. კომპიუტერ Univac 1108 -სთვის შექმნილი თამაში Pervading Animal იძ­ლეოდა საშუალებას კითხვების მეშვეობით იმ ცხოველის სახელის გამოც­ნობისა, რო­მელიც წამყვანმა ჩაიფიქრა. შეცდომა იმაში მდგომარეობდა, რომ მოდი­ფიცირებული თამაში, როცა მასში დამატებითი კითხვების შეტანა ხდებოდა, ჩაიწე­რებოდა ძველის ადგილას და ამავე დროს კოპირდებოდა სხვა დირექტორიაში. შედე­გად, რამდენიმე ასეთი მოდიფიცირების შემდეგ დისკი გადაივსებოდა. რადგანაც Pervading Animal არ აყო წმინდა სახის ვირუსი, ის არ შეიცავდა თვითგავრცელების შესაძლებლობას, ის ვრცელდებოდა იმ მომხმარებლების მიერ, რომლებიც თავისი ნებით ჩაიწერდნენ ამ თამაშს თავის დისკეტაზე.

თავად იდეა თვითწარმოქმნადი პროგრამებისა ეკუთვნის კომპიუტერების ”მამას”, უნგრული წარმოშობის ამერიკელ მათემატიკოს **ჯონ ფონ ნეიმანს,** (John von Neu­mann), რომელმაც 1949 წელს ამ შესაძლებლობების შესახებ გამოაქვეყნა მონოგრაფია- ”თვითწარმოქმნადი ავტომატების თეორია”.

პირველი ვირუსი ქსელში 1975 წელს გამოჩნდა სახელწოდებით **Creeper,** რომელიც მოდემის საშუალებით ერთი კომპიუტერიდან მეორეში შეაღწევდა და ამ მეორე კომპიუტერის მონიტორზე გამოჩნდებოდა წარწერა ”I'M THE CREEPER: CATCH ME IF YOU CAN" **- მე კრიპერი ვარ: აბა დამიჭირე, თუ შეგიძლია. Creeper** მა წარმოქმნა პირველი ანტივირუსული პროგრამა **Reaper,** რომელიც ვრცელდებოდა ქსელში და თუ კი ის რომელიმე კომპიუტერში აღმოაჩენდა **Creeper** -ს, წაშლიდა მას.

ინტერნეტის, ელექტრონული ფოსტის და ძალიან პოპულარული Windows -ის წყა­ლობით ვირუსები მთელს ქვეყანაში წარმოუდგენელი სისწრაფით ვრცელდება. ექ­სპერტთა დაკვირვების მიხედვით, Malware -ს (ყველა სახის მავნებელი პროგრამის საყოველთაოდ მიღებული დასახელება) მოცულობის ზრდა წელიწადში 15%-ს აღე­მატება.

მართალია, ძირითად საფრთხეს მომხმარებლებს კომპიუტერული ვირუსები უქმნიან, არსებობს სხვადასხვა სახის მავნე პროგრამებიც.

განვმარტოთ მათი მუშაობის პრინციპები.

**ვირუსი** - ესაა პროგრამული კოდი, რომლის ტირაჟირებაც სხვა ობიექტში დამატების შედეგად ხდება. ეს პროცესი მიმდინარეობს შეუმჩნევლად, მომხმარებლის ნებარ­თვის გარეშე, ამგვარად, ვირუსს შეუძლია ფაილების, დოკუმენტების ან ფაილური და დისკური სტრუქტურების, როგორიცაა ჩასატვირთი სექტორი ან ფაილების განლაგების ცხრილი, ინფიცირება. ვირუსის გააქტიურება ხდება ინფიცირებული პროგრამის გაშვებისას. მათ შეუძლიათ მუდმივად იარსებონ მეხსიერებაში და მოახდინონ მომხმარებელთა ფაილების ინფიცირება ან საკუთარი ფაილების შექმნა, ასევე შეუძლიათ შეცვალონ მნიშვნელობები სისტემურ რეესტრში. ვირუსი, აუცილებელი არაა იყოს ცალკეული პროგრამა, და ყოველთვის არ წარმოადგენს დესტრუქციულს თავისი შინაარსით, ყველაფერი დამოკიდებულია მის ნაირსახეობაზე.

**Worm (ჭია)** \_ ესაა დამოუკიდებელი პროგრამა, რომელიც ერთი კომპიუტერიდან მეორეზე საკუთარი თავის კოპირების შედეგად ვრცელდება, როგორც წესი ლოკალური ქსელის ან საფოსტო გზავნილების საშუალებით. ეს პროგრამები ანადგურებენ მონაცემთა ფაილებს ან აწარმოებენ ერთობლივ შეტევას სხვა კომპიუტერის წინააღმდეგ. ყოველთვის არ არსებობს მკაფიო განსხვავება ვირუსებსა

და ჭიებს შორის.

**ტროას ცხენები ანუ ტროიანები** \_ პროგრამები, რომელთა გააქტიურებაც ხშირად მომხმარებლის თანხმობის შედეგად ხდება. ამ ერთი შეხედვით უწყინარ პროგრამებს შეუძლიათ შეცვალონ მომხმარებელთა პაროლები და მიმართვის უფლებები. ტროიანი შეიძლება აღმოჩნდეს კომპიუტერში საფოსტო გზავნილებიდან ან ვებ-საიტებიდან. მაგალითად, ჰაკერი რომელიმე საიტიდან ატყობინებს

მსხვერპლს, რომ ინტერნეტში შეიმჩნევა ძალიან ვერაგი ვირუსის ეპიდემია და სთავაზობს მიმართოს თავის ვითომც და ანტივირუსულ პროგრამას, საიდანაც რეალურად მოხდება მისი ინფიცირება. შერეული კოდები წარმოადგენენ ახალი კლასის დახვეწილ მავნე პროგრამებს, რომლებიც მოიცავენ ვირუსების, ჭიების და ტროიანების ყველა მახასიათებელს, რაც საშუალებას აძლევს ბოროტგანმზრახველს

აწარმოოს განსაკუთრებით ეფექტური შეტევა. ასეთი პროგრამების მიზანს წარმოადგენს ვებ-სერვერები და ქსელები, რაც მნიშვნელოვნად ამარლებს მათ აფრთხეს. და ბოლოს, არ შეიძლება არ აღვნიშნოთ \_ სპამი. ყველა, ვინც სარგებლობს ელექტრონული ფოსტით, ადრე თუ გვიან ღებულობს მოსაბეზრებელ სარეკლამო შეტყობინებებს ანუ სპამს. სპამი ნამდვილი უბედურებაა, რომელიც საფრთხეს უქმნის კომპიუტერის უსაფრთხოებას. იგი წარმოადგენს იდეალურ გარემოს სხადასხვა თაღლითებისათვის, რომლებიც ავრცელებენ საეჭვო მარკეტინგულ სქემებს. ამ კატეგორიის ზოგიერთი წერილი შეიცავს ვირუსებს და სხვა მავნე პროგრამებს. როგორც წესი, სპამერები ეძებენ მიამით მომხმარებლებს, რომლებიც მიიღებენ შეტყობინებას და მოახდენენ

მასზე რეაგირებას. ისინი მალავენ საკუთარ მისამართებს, ამიტომაც

შეუძლებელია მათი დასჯა.

არც თუ ისე მარტივი საქმეა ჩვეულებრივი წერილების განსხვავება სპამისაგან, თუმცა არსებობს მათთვის დამახასიათებელი თავისებურებები. კერძოდ, სპამერები იყენებენ ფიქტიურ მისამართებს (ველში From), უთითებენ უწყინარ ტექსტებს ველში Subject (მაგალითად, “თქვენ მიიღეთ ჩემი წერილი?” ან “ინფორმაცია, რომელიც თქვენ შეუკვეთეთ”), ცდილობენ ჩართონ წერილში მიმართვა

“ერთჟერად” ვებ-გვერდებზე, რომელიც ქრება მას შემდეგ, როდესაც ვინმე წამოეგება ანკესზე.

დაწვრილებით სპამერების ტექნოლოგიები აღწერილია ვებ-საითზე http://www.spamfaq.net/spamfighting.shtml

გთავაზობთ ზოგიერთი ანთვირუსული პროგრამის მოკლე დახასიათებას.

**Aladdin Knowledge Systems**

პროდუქტები: **eSafe Desctop, eSafe Enterprisees**

ეს პაკეტი აერთიანებს ანტივირუსულ ტექნოლოგიებს,

პერსონალურ ბრანდმაუერს, საფოსტო ფილტრს და სამუშაო მაგიდის

ბლოკირების უტილიტებს. შესაძლებელია 60-დღიანი დემო-ვერსიის

გადმოტვირთვა ვებ-საიტიდან: <http://www.aks.com/>

ინფორმაცია ვირუსების შესახებ:

<http://www.aks.com/home/csrt/valerts.asp>

**Central Command**

პროდუქტები: Vexira Antivirus (ვერსიები: Home, Small Business,

Enterprise, Government, Educational Edition).

ესაა გამოსაყენებლად მარტივი სკანერები, რომელთა საშუალებითაც შეგიძლიათ შეამოწმოთ ელექტრონული ფოსტა, ჩასატვირთი ფაილები და ქსელური დისკები. თითოეული პროდუქთისათვის არსებობს დემო-ვერსია.

ვებ-საიტი: http://www.centralcommand.com/

ინფორმაცია ვირუსების შესახებ:

http://www.centralcommand.com/recent\_threats.html

**Command Software Systems, Inc.**

პროდუქტები: Command AntiVirus, სახლის და კორპორატიული ვერსია.

ეს პროგრამა ამოწმებს 70 ტიპის (მათ შორის შეკუმშულ) ფაილებს, აუცილებლობის შემთხვევხაში ვებ-გვერდებსაც. ხელმისაწვდომია 30-დღიანი დემო-ვერსია ვებ-საიტზე:

<http://www.commandcom.com/>

ინფორმაცია ვირუსების სესახებ:

<http://www.commandcom.com/virus/index.cfm>

**Computer Associates International, Inc.**

პროდუქტები: eTrust EZ Armor, eTrust EZ Antivirus, eTrust EZ

Deskshield, eTrust EZ Firewall.

კომპანია CAI გვთავაზობს პროდუქტების ფართო სპექტრს,

როგორც სახლის, ისე მცირე ბიზნესისა და მსხვილი

კორპორაციებისათვის.

ვებ-საითი: <http://www.cai.com/> <http://www2.my-etrust.com/>

ინფორმაცია ვირუსების შესახებ:

http://www3.ca.com/virus

**ESET**

პროდუქტი: NOD32

პრგრაამას უზრუნველყოფს კომპიუტერის მუდმივ დაცვას, შეუძლია ინტეგრირება Windows Explorer-თან და საფოსტო კლიენტებთან. პაკეტი შეიცავს განახლების მრავალ ვარიანტს, რომელშიც გათვალისწინებულია ლოკალურ ქსელში მუშაობის თავისებურებები.

ვებ-საითი: <http://www.nod32.com/>

ინფორმაცია ვირუსების შესახებ:

http://www.nod32.com/aupport/pedia.htm

**F-Secure Corp.**

პროდუქტი: F-Secure Anti-Virus

კომპანის გვთავაზობს თავისი პროგრამის ათზე მეთ ვერსიას. მათ რიცხვში შედის პერსონალური და კორპორატიული პროგრამების ატზე მეტი ვერსია. პაკეტი თოთალ სუითე მოიცავს ბრანდმაუერისა და ანტივირუსის ფუნქციებს. ხელმისაწვდომია სადემონსტრაციო ვერსიები:

ვებ-საიტი: <http://www.f-secure.com/>

ინფორმაცია ვირუსების შესახებ:

http://www.f-secure.com/virus-info

**Grisoft,Inc.**

პროდუქტები: AVG Antivirus 6.0 (უფასოდ ვრცელდება ვერსიები Professional და Server)

კომპლექტში შედის ანტივირუსული სკანერი და ელექტრონული ფოსტის დაჩვის სისტემა ავტომათური განახლების ფუნქციებით. ხელმისაწვდომია 30-დღიანო დემო-ვერსია. ვებ-საიტი: http://www.grisoft.com/

ინფორმაცია ვირუსების შესახებ:

<http://www.grisoft.com/html/us_alert.php>

**კასპერსკის ლაბორატორია**

პროდუქტი: კასპერსკის ანტივირუსი.

პროგრამას შეუძლია ინტეგრირება Outloox Express-თან და MS

Office-ის პროდუქტებთან.

ვებ-საითი: http://www.kasperskylabs.com/

ინფორმაცია ვირუსების შესახებ:

<http://www.kasperskylabs.com/news.httnl?tnews=20140>

**Network Associates(McAfee)**

პროდუქტები: McAfee VirusScan, McAfee Clinic, McAfee

NetShield, McAfee WebShield, McAfee GroupShield.

სოლიდური ფირმა, გვთავაზობს ანტივირუსული პროგრამების ფართო არჩევანს სახლში მომუშავე მომხმარებლებისათვის, კერძო მეწარმეებისათვის და მსხვილი კორპორაციებისათვის. თითოეული პროდუქტისათვის ხელმისაწვდომია სადემონსტრაციო ვერსია.

ვებ-საიტი: <http://www.nai.com/> <http://www.mcafee.com/> <http://www.mcafeeb2b.com/>

ინფორმაცია ვირუსების შესახებ:

http://vil.nai.com/VIL/default.asp

**Norman ASA**

**Virus Control, Norman Personal Firewall, Norman Privacy.**

პროგრამული პაკეტი შედგება მოდულებისაგან, რომელიც შეიცავს რეზიდენტულ სკანერს, სკანერს ხელით შემოწმებისათვის, განახლების სისტემას და უტილიტების ნაკრებს. ადმინისტრატორს შეუძლია ააწყოს სისტემა ისეთი სახით, რომ კლიენტების პროგრამების განახლება მოხდეს ინტერნეტიდან. საიტზე მოთავსებულია 30-დღიანი დემო-ვერსია.

ვებ-საიტი: http://www.norman.com/

ინფორმაცია ვირუსების შესახებ:

<http://www.norman.com/virus_info/virus_descriptions.shtml>

**Panda Software**

პროდუქტი: Panda Antivirus

შემოტავაზებული პროგრამული კომპლექსი უძრუნველყოფს ლოკალური ქსელის (სერვერის და კლიენტ-კომპიუთერების) სრულ დაცვას. სახლში მომუშავე მომხმარებლებს შეუძლიათ შეიძინონ Titanium ან Platinum , რომელთა განახლებაც ხდება ყოველდრე და თავსებადია WindowsXP-სთან.

ვებ-საიტი: http://www.pandasoftware.com/

ინფორმაცია ვირუსების შესახებ: http://www.pandasoftware.com/

**Sophos**

პროდუქტი: Sophos Anti-Virus

პროგრამა დამუშავებულია სპეციალურად კორპორატიული ქსელებისათვის, ახორციელებს დისკების, შესრულებადი ფაილების, დოკუმენტების და ქსელური დისკების მონიტორინგს. ხელმისაწვდომია სასინჯი ვერსია

ვებ-საიტი: http://www.sophos.com/

ინფორმაცია ვირუსების სესახებ: <http://www.sophos.com/virusinfo>

**Symantec Corp.**

პროდუქტები: Norton Antivirus, Norton Internet Security

პროდუქტები განკუთვნილია, როგორც ცალკეულ მომხმარებლებისათვის, ისე ნებისმიერი ზომის ფირმებისათვის. Norton Internet Security-ის შემადგენლობაში შედის ბრანდმაუერი, ხოლო Norton Antivirus-ი კარგად ინტეგრირდება საფოსტო

პროგრამებტან და მუშაობს ლოკალურ ქსელში.

ვებ-საიტი: http://www.symantec.com/

ინფორმაცია ვირუსების შესახებ: http://www.sarc.com/

Malware – „მავნე პროგრამა“

მავნე, „მავნე“ პროგრამა - ეს არის კრებითი სახელწოდება ყველა ტიპის მავნე ფუნქციის მქონე პროგრამისთვის. განვმარტოთ, თუ რაში მდგომარეობს მისი არსი. მავნე ფუქნციების მქონე პროგრამა შეიცავს ვირუსებს, ე.წ. „Trojans“, „Worms“ და „Spyware“, თუმცა უნდა ითქვას, რომ მხოლოდ ამით არ შემოიფარგლება მისი მავნე ფუნქცია. მავნე ფუნქციის მქონე პროგრამის მიზანი უპირველეს ყოვლისა არის სისტემებში შეღწევა და ამდენად, იქ შენახული ინფორმაციის კრიმინალური, კომერციული ან გამანადგურებელი მიზნებისთვის გამოყენება. მიმოვიხილოთ მავნე ფუნქციის მატარებელი პროგრამის გავრცელების გზები, თუ როგორ უნდა იქნას იგი თავიდან აცილებული და როგორ უნდა მოიქცეთ, როდესაც გაქვთ ეჭვი, რომ თქვენი კომპიუტერი „დაინფიცირებულია“.  
  
მავნე ფუნქციის მქონე პროგრამა ხასიათდება საკმაოდ დიდი ცვალებადობით როგორც ფორმის, ასევე ფუნქციონალური თვალსაზრისით. ზოგიერთი ამ ტიპის პროგრამა გამოიყენება ისეთი ინფორმაციის „მოსაპარად“, როგორიცაა საკრედიტო ბარათის ნომრები, საიდენტიფიკაციო ან სხვა სენსიტიური ბიზნეს ინფორმაცია იმ კომპიუტერიდან, რომლის დაინფიცირებაც მოახდინა. სხვა ამ ტიპის პროგრამამ კი შესაძლოა ასე ვთქვათ „მიითვისოს“ თქვენი კომპიუტერი და გამოიყენოს იგი სხვა სისტემებზე თავდასხსმისათვის. მავნე ფუნქციის მატარებელი პროგრამა გამიზნულია საკმაოდ მძიმე შედეგების გამოსაწვევად, რაც გამოიხატება თქვენი კომპიუტერიდან ინფორმაციის განადგურებით ან ინფორმაციის მთლიანობის დაღვევით, მისი დამახინჯებით. აქედან გამომდინარე კი შეგვიძლია დანამდვილე­ბით ვთქვათ, რომ ასეთ შემთხვევაში პრევენცია ჯობია შედეგების გამოსწორებას, ამიტომაც, გაითვალისწინეთ თქვენს კომპიუტერზე ამგავრი „მავნე“ პროგრამის გავრცელების თავიდან არიდების გზები.  
  
**როგორ ვრცელდება „მავნე“, მავნე ფუნქციის მქონე პროგრამა?**  
  
კრიმინალები მუდმივად ავითარებენ ახალ და ინოვაციურ საშუალებებს, იმისათვის, რომ დააინფიცირონ თქვენი კომპიუტერი მავნე ფუნქციის მატარებელი პროგრამით საკუთარი მიზნების მისაღწევად. გთავაზობთ რამდენიმე საყოველთაოდ ცნობილ საშუალებეს, თუ როგორ ვრცელდება ამგვარი პროგრამა და იმ პრევენციულ მექანიზმებს, რომლებსაც თქვენ გამოიყენებთ მისი თავიდან არიდების მიზნით.  
  
**ელ-ფოსტა**  
  
ამგვარი „მავნე“ პროგრამები ხშირად ელ-ფოსტით თანდართულ ფაილშია წარ­მოდგენილი ან ავტომატურად ხდება მისი ჩამოტვირთვა და დაინსტალირება თქვენს კომპიუტერზე, როდესაც თქვენს ელ-ფოსტაში მოცემულ ბმულზე დააწკაპუნებთ.

· ყოველთვის ყურადღება მიაქციეთ ყველა იმ თანდართულ ფაილს, რაც ელ-ფოსტით მოგდით - თუნდაც იგი მეგობრისგან ან თანამშრომლისგან იყოს გამოგზავნილი. ყო­ველთვის განახორციელეთ ასეთი თანდართული ფაილების სკანირება მანამ, სანამ გახსნით.

· არასოდეს არ გახსნათ ფაილი ან არ დაწკაპუნოთ საეჭვო ან უცნობი გამომგზავნის ბმულზე.  
  
**ვებგვერდები**„მავნე“ პროგრამები შეიძლება უყურადღებობის გამო ჩამოიტვირთოს ვებგვერ­დებიდან, ან ავტომატურად მოხდეს მისი ჩამოტვირთვა თქვენს კომპიუტერზე რო­გორც კი შეხვალთ ამ მიზნით შექმნილ ვებგვერდზე (რაც თქვენ წინასწარ არ იცით ბუნებრივია).

· მიაქციეთ ყურადღება აპლიკაციების ჩამოტვირთვის მოთხოვნას ან „Add-Ons“-ის დაინსტალირების მოთხოვნას, როგორიცაა საეჭვო ActiveX კომპონენტები ან უჩვეულო, უცნაური „media players“.

· არასოდეს არ ჩამოტვირთოთ ან დააინსტალიროთ პროგრამები უცნობი ან არა­საიმედო ვებგვერდებიდან.  
  
**„მოციმციმე“ სარეკლამო ფანჯრები (Pop-Ups)**უნდა ვაღიაროთ, რომ სრულიად ახალი და ჭკვიანურად მოფიქრებული გავრცელე­ბის საშუალება გახლავთ „მოციმციმე“ სარეკლამო ფანჯრები, რომელთა ლეგალურო­ბაშიც ეჭვს ევრ შეიტანთ ერთი შეხედვით, რადგანაც ნამდვილად შეიცავენ სარეკლა­მო შეტყობინებებს.

· არასოდეს არ შეიძინოთ რაიმე პროგრამა ამგვარი მოულოდნელად გამოშუქებული შეტყობინებების ან ელ-ფოსტის მეშვეობით.

· განსაკუთრებით უფრთხილდით ისეთ თაღლითურ განცხადებას, რომელიც გარწმუნებთ, რომ განახორციელა თქვენი კომპიუტერის სკანირება და აღმოაჩინა „მავნე“ პროგრამა.  
  
**სოციალური ქსელების საიტები**გავრცელების კიდევ ერთი გზა გახლავთ სოციალური ქსელების საიტები, რომელთა დაინსტალირებაც ხდება საეჭვო, 3-ე მხარის მიერ შემოთავაზებული „Add-Ons“-ის აპლიკაციებით ან შეტყობინებებში მოსული ვებ-ბმულებზე დაწკაპუნებით. ასეთ შემთხვევაში, ამ საიტების გამოყენებისას უსაფრთხოების შესახებ მოსაზრებები აბსოლუტურად მცდარია, ასე, რომ იყავით ყურადღებით.

· დააინსტალირეთ 3-ე მხარის მიერ შემოთავაზებული მხოლოდ ის სოციალური ქსელების აპლიკაციები, რომლებიც საკმაოდ ცნობილი და სანდოა.

· არასოდეს დააწკაპუნოთ უცნობი ან საეჭვო გამომგზავნისგან მიღებულ შეტყობი­ნებებში მოცემულ ბმულებს, და ასევე იმ შეტყობინებებსაც, რომლებიც სანდო კონ­ტაქტებიდან არის გამომგზავნილი, თუმცა თქვენ ეჭვი გაქვთ და დარწმუნებული ხართ, რომ მძიმე შედეგებს გამოიწვევს.  
  
**პროგრამული უზრუნველყოფა**„მავნე“ ფუნქციის მატარებელი პროგრამა, რომელიც მოთავსებულია ლეგა­ლური სახისა და ფორმის მქონე პროგრამულ უზრუნველყოფაში - ეს გახლავთ ყვე­ლა­ზე ხშირად გამოყენებული გზა მისი გავრცელებისა. **„Peer to Peer“ (ერთრანგიანი?)** პროგ­რამული უზრუნველყოფა და კრეკირებული ან პირატული პროგრამული უზრუნ­ველყოფა (მაგალითად: „warez'“), ხშირად აადვილებს „მავნე“ ფუნქციის მატარე­ბული პროგრამების გავრცელებას.

· არასოდეს დააინსტალიროთ არაავტორიზებული, არალიცენზირებული ან ოფი­ციალურად დაუდასტურებელი პროგრამული უზრუნველყოფა თქვენს კომპიუტერ­ზე.

· ყოველთვის დაეჭვდით უფასო პროგრამული უზრუნველყოფის შემოთავაზებაში - აუცილებლად წაიკითხეთ და გაიაზრეთ ლიცენზირებისა და უსაფრთხოების პოლიტიკა მანამ, სანამ დააინსტალირებით პროგრამას.  
  
**კომპიუტერული მატარებლები (მედიები)**„მავნე“ პროგრამები შეიძლება ადვილად გავრცელდეს კომპიუტერული მატარებლე­ბის, როგორებიცაა DVD, CD, და USB ზიარი გამოყენებით.

· არასოდეს მიუერთოთ არასანდო და საეჭვო კომპიუტერული მედია-მატარებელი თქვენს კომპიუტერს.

· ყოველთვის განახორციელეთ ზიარ კომპიუტერულ მატარებელზე შენახული ფა­ილების სკანირება მანამ, სანამ გახსნით ან დააკოპირებთ მას.  
  
**მობილური მოწყობილობები**ცნობილია, რომ „მავნე“ პროგრამები ვრცელდება ასევე მობილური მოწყობილობების მეშვეობით, როგორიცაა მობილური ტელეფონები. რადგანც მოწყობილობები სულ უფრო ემსგავსებიან მინი კომპიუტერებს, მათზე ამგვარი მავნე პროგრამების გავრცე­ლების საფრთხე სულ უფრო გაიზრდება.

· არასოდეს დააინსტალიროთ შეუმოწმებელი ან არაოფიციალური პროგრამული უზრუნველყოფა თქვენს მობილურ მოწყობილობაზე.

· ყურადღებით იყავით და არ დათანხმდეთ თქვენი მოთხოვნის გარეშე, თვითნებუ­რად მოსულ ტექსტის შინაარსს ან სხვა შეტყობინებებს, რომლებიც გთხოვენ პროგ­რამული უზრუნველყოფის დაინსტალირებას ან ასევე გთავაზობენ უცნობ და საეჭვო ბმულებს.  
  
**რა ტიპის კონტროლების დანერგვა დამეხმარება „მავნე“ პროგრამის პრევენციაში?**„მავნე“ ფუნქციის მატარებელი პროგრამა არის საკმაოდ რეალური და ძლიერი საფ­რთხე ინფორმაციის უსაფრთხოების თვალსაზრისით. ამდენად, აუცილებელია არსე­ბობდეს სპეციფიკური უსაფრთხოების კონტროლები, რათა დაცულები ვიყოთ ამ საფრთხისგან. შემდეგი კონტროლების განხორციელება დაგეხმარებათ პრევენციაში.  
  
**გამოიყენეთ ანტი-ვირუსული პროგრამული უზრუნველყოფა**· დააინსტალირეთ კარგი, სანდო ანტი-ვირუსი და ანტი-ჯაშუშური პროგრამა (anti-spyware) და მოახდინეთ მისი აქტივაცია. არსებობს რამდენიმე საკმაოდ კარგი, სანდო უფასო პრევენციული პროგრამები, როგორებიცაა Microsoft Security Essentials, Comodo Anti-Virus და AVG Free, რომლებიც დაგიცავენ „მავნე“ პროგრამებისგან.

· პორგრამული უზრუნველყოფის კონფიგურაცია ააწყვეთ ისე, რომ მან შეასრულოს ყოველდღიური განახლებები, რათა შესაბამისად იქონიოთ უახლესი ვერსიები ვირუსებისგან თავდასაცავად.  
  
**განაახლეთ ყველა პროგრამული უზრუნველყოფა**· თქვენი ოპერაციული სისტემის კონფიგურირება ნიშნავს ყველა განახლების ავტო­მატურად ჩამოტვირთვასა და ინსტალირებას.

· რეგულარულად შეამოწმეთ თქვენს კომპიუტერზე არსებული ყველა სხვა პროგრა­მული უზრუნველყოფა არის თუ არა განახლებული უსაფრთხოების უახლესი ვერსი­ებით.  
  
**გამოიყნებეთ დამცავი ბარიერი - ბრანდმაუერი (Firewall)**· დააინსტალირეთ და გაააქტიურეთ თქვენს კომპიუტერზე პირადი დამცავი ბარიერი

· უზრუნველყავით, რომ დამცავი ბარიერი კონფიგურირებული იყოს იმგვარად, რომ დაბლოკოს ყველა არასასურველი შემომავალი ტრაფიკი.

· მარტივად არ დათანხმდეთ დაკავშირების ყველა მოთხოვნას - შეეცადეთ გაიგოთ, თუ რა ცდილობს დაგიკავშირდეთ დამცავი ბარიერის მეშვეობით და ეჭვის არსებობის შემთხვევაში არ დათანხმდეთ კავშირის მოთხოვნას.  
  
**არ გამოიყენოთ ადმინისტრატორის ანგარიში**· არასოდეს არ გამოიყენოთ ადმინისტრატორის მომხარებლის ანგარიში ყოველდღი­ურად კომპიუტერით სარგებლობისას, რადგანაც ეს ხელს ვერ შეუშლის malware -ს მოიპოვოს თქვენი კომპიუტერის ადმინისტრატორის უფლებები და ნებისმიერი პო­ტენციური დახმარების შეზღუდვით ზიანი გამოიწვიოს.

· Windows-ის სტანდარტულ მომხმარებლის ანგარიშს აქვს ლოკალური ადმინისტრა­ტორის უფლებები და არ უნდა იქნას გამოყენებული. ამის ნაცვლად, შექმენით ან გა­მოიყენეთ განსხვავებული მომხმარებლის ანგარიში, რომელსაც ექნება ძირითადი მომხმარებლის უფლებები.  
  
**პროფილაქტიკური სკანირება**· განახორიელეთ სკანირება ყველა ჩამოტვირთულ, კოპირებულ ფაილზე ან ელ-ფოს­ტით მოსულ თანმხლებ ფაილებზე მანამ, სანამ გახსნით ან გაუშვებთ მათ დასაინსტა­ლირებლად.

· რეგულარულად (სულ მცირე თვეში ერთხელ) შეასრულეთ თქვენი კომპიუტერის სკანირება ვირუსების ან სხვა მავნე პროგრამების აღმოსაჩენად.  
  
**გაააქტიურეთ „სპამის“ და „ფიშინგის“ ფილტრები**· დარწმუნდით, რომ აქტივირებული გაქვთ „სპამის“ და „ფიშინგის“ ფილტრები ელ-ფოსტისა და ინტერნეტ-ბრაუზერისთვის.

· წაშალეთ ყველა შემოსული სპამი. არასოდეს უპასუხოთ ან დააწკაპუნოთ საეჭვო „სპამის“ ან „ფიშინგის“ შემცველ მეილებს ან ბმულებს.  
  
**გაააქტიურეთ „მოციმციმე“ სარეკლამო ფანჯრების (Pop-Up) ბლოკირება**· დარწმუნდით, რომ გააქტიურებული გაქვთ თქვენი ინტერნეტ ბრაუზერისთვის „მოციმციმე“ სარეკლამო ფანჯრების ბლოკირება და გათიშეთ იგი მხოლოდ იმ საიტებისთვის, რომლებსაც კარგად იცნობთ და ენდობით.  
  
**დამეხამრეთ, მგონი ვირუსი მაქვს!**მუდმივად უნდა განახორციელოთ თქვენი კომპიუტერის მონიტორინგი უჩვეულო ან არასწორი მოქმედებებისთვის. თუკი ფიქრობთ, რომ თქვენი კომპიუტერი დაინფიცი­რებულია „მავნე“ პროგრამის ფუნქციით, მაშინ სასწრაფოდ რამე უნდა იღონოთ. უპირველეს ყოვლისა, არ განახორციელოთ რაიმე ისეთი ქმედება, რაც გამოიწვევს სენსიტიური ინფორმაციის გადაცემას (მაგალითად: ნივთების ან რაიმე სახის საქონ­ლის ონლაინ-ყიდვა ან ბანკინგი), შემდეგ კი მიჰყევით ქვემოთ მოცემულ ეტაპებს, განახორციელეთ „მავნე“ ფუნქციის მატარებელი პროგრამის იდენტიფიცირება.

განაახლეთ თქვენი ანტი-ვირუსი, ანტი-ჯაშუშური პროგრამა და ნებისმიერი სხვა რამ, რაც გეხმარებათ „მავნე“ ფუნქციის მატარებელი პროგრამის პრევენციაში, იქონიეთ განახლებების უახლესი ვერსიები.  
  
(შენიშვნა: ზოგიერთი „მავნე“ პროგრამა ხელსაც კი შეგიშლით და არ დაგაყენებინებთ ამ განახლებებს).  
  
გამორთეთ კომპიუტერი ინტერნეტიდან (მაგალითად: ქსელის კაბელი გამოაძრეთ ან გათიშეთ უსადენო ინტერნეტი) განახორციელეთ თქვენი კომპიუტერის სკანირება ჩამოტვირთული ანტივირუსის, ანტი-ჯაშუშური პროგრამის გამოყენებით თუკი აღმოჩენილი იქნა „მავნე“ პროგრამა, წაშალეთ ან გაასუფთავეთ ყველა საეჭვო ფაილი გადატვირთეთ კომიუტერი.  
  
გაუშვით ხელმეორე სკანირება, რათა გარანტირენული იყოს, რომ არ დარჩა აღმოუ­ჩენელი დანარჩენი ვირუსები.  
  
როგორც კი დარწმუნდებით, რომ კომპიუტერი სუფთაა, შეგიძლიათ ისევ ჩართოთ იგი ინტერნეტში.  
  
დაიცავით აქ შემოთავაზებული დაცვის მექანიზმები, რათა გარანტირებული იყოთ, რომ არ გახდებით „მავნე“ ფუნქციის მატარებელი პროგრამის მსხვერპლი.

სახლის უკაბელო ინტერნეტ ქსელის უსაფრთხოება

როდესაც გადიხართ სახლიდან, თქვენ ხომ არ ტოვებთ სახლის კარებს ფართოდ გა­ღებულს? პირიქით თქვენ აუცილებლად მიხურავთ და საიმედოდ ჩაკეტავთ მას. იგივე პრინციპის გატარებაა საჭირო სახლის უკაბელო ქსელთან მიმართებაში. თუ ქსელი დაუცველია, მაშინ შესაძლებელი ხდება მისი გამოყენება სხვადასხვა მიზნით. აქ მოცემულია რამდენიმე რჩევა, თუ როგორ უნდა გახადოთ დაცული საკუთარი უკაბელო ინტერნეტ ქსელი, სახლის პირობებში.  
  
არაავტორიზებულმა პიროვნებებმა შეიძლება მოიპოვონ წვდომა თქვენს სახლის უკაბელო ქსელში, თუ არ მიიღებთ განსაზღვრულ ზომებს ქსელის დასაცავად. უსაფ­რთხოების არ არსებობის შემთხვევაში მნიშვნელოვანი პერსონალური მონაცემები დაუცველია, ისინი ხელმისაწვდომი ხდება სხვა პიროვნებისათვის. ამას შეიძლება მოჰყვეს თქვენი პერსონალური მონაცემების უნებართვოდ გამოყენება (Identity Ste­aling). ასევე შეიძლება თქვენი ინტერნეტ კავშირი გამოიყენონ არალეგალური ქმედებების ჩასადენად, რაზეც პასუხისმგებლობა ეკისრება მფლობელს.  
  
**როუტერის დაკონფიგურირება:**იმისათვის რომ თქვენი „სახლის უკაბელო ინტერნეტი“ უსაფრთხო გახადოთ, ქსე­ლური მოწყობილობა როუტერი, უნდა იყოს შესაბამისად კონფიგურირებული. ჩვე­ულებრივ, როუტერი რომელიც მოწოდებულია ინტერნეტ პროვაიდერისაგან ან პირ­დაპირ მწარმოებლისაგან, აკმაყოფილებს მინიმალური უსაფრთხოების დონეს. ასეთი მდგომარეობა მისაღებია ინტერნეტ პროვაიდერებისათვის. იმ შემთხვევაში თუ თქვენ შეგექმნებათ რაიმე პრობლემა და დახმარებისთვის მიმართავთ პროვაიდერს, მათ გაუადვილდებათ თქვენთვის დახმარების აღმოჩნა და როუტერის გამართვა. მაგრამ ეს ასევე ნიშნავს, რომ თქვენი სახლის უკაბელო ქსელი დაუცველია.  
  
სანამ შეცვლით როუტერის კონფიგურაციის პარამეტრებს ყოველთვის თან იქონიეთ როუტერის ინსტრუქცია. როდესაც ცვლით პარამეტრებს ყოველთვის დაუკავშირ­დით როუტერს სადენის გამოყენებით, რადგან თუ ცვლილებებს აკეთებთ უკაბელო ქსელის გამოყენებით, შესაძლებელია კონფიგურირების პროცესში დაიკარგოს კავშირი, გაითიშოს ქსელი. ამ შემთხვევაში შესაძლებელია გამოიყენოთ ფურცლის კლიპერი, რომელიც როუტერის უკან არსებულ Reset-Button-ით კონფიგურაციას დააბრუნებს „ქარხნულ“ საწყის პარამეტრებზე.  
  
**უსაფრთხოების მინიმალური მოთხოვნები:**სახლის უკაბელო ქსელის მინიმალური უსაფრთხოებისათვის აუცილებელი პირობები.  
  
**დაშიფრეთ თქვენი ქსელი - ‘WPA' (და არა ‘WEP')**- დაშიფრვის გამოყენებით თქვენ ქსელში მიმოქცევადი ინფორმაცია, გაუგებარი და არაწაკითხვადი სახითაა მათთვის, ვინც ცდილობს მოიპოვოს არაავტორიზებული წვდომა.  
  
- დარწმუნდით რომ გამოყენებული დაშიფრვის სტანდარტი არის WPA-AES ან WPA2 და არჩეულია მინიმუმ 8 სიმბოლოს შემცველი პაროლი. (სასურველია არ გამოიყე­ნოთ სიტყვა ლეკსიკონიდან, სახელები ან თარიღები)  
  
- არასოდეს გამოიყენოთ WEP დაშიფრვის სტანდარტი, უკიდურესი აუცილებლობის შემთხვევების გარდა, იმიტომ რომ ეს სტანდარტი დაუცველია. WEP სტანდარტი ავ­ტომატურად გააქტიურებულია და გამოიყენება ინტერნეტ პროვაიდერების მიერ მოწოდებულ როუტერებში, ამიტომ საჭიროა მისი შეცვლა უფრო მეტად უსაფრთხო სტანდარტით.  
  
**შეცვალეთ თქვენი ქსელის სახელი - (Network Name)**

- უკაბელო ქსელს სტანდარტულად სახელი ენიჭება ინტერნეტ პროვაიდერი კომპანიის (მაგ: Silknet, Caucasus, Maximal) ან როუტერის მწარმოებელი ფირმის მიხედვით (Cisco, Linksys).  
  
- ამ ინფორმაციის გამოყენებით შეიძლება გარკვევა, თუ რომელი როუტერი გამოიყენება და როგორია მისი სტანდარტული კონფიგურაცია. ამ ეტპაზე ქსელი ხდება უფრო მარტივი სამიზნე არაავტორიზებული პერსონებისათვის.  
  
- ქსელის სახელი ხშირად მიმართებაშია როუტერის SSID სახელთან. საჭიროა ამ პარამეტრის შეცვლა რაიმე გაურკვეველი და მნიშვნელობის არმქონე სახელით.  
  
**შეცვალეთ როუტერთან წვდომის სტანდარტული წესები**- როუტერებზე ავტომატურად დაყენებულია მომხმარებლის სტანდარტული სახელი და პაროლი, მაგ: username: *admin* password: *admin*- ამ პარამეტრების შეუცვლელი სახით დატოვება სახიფათოა, რადგან ნებისმიერ პირს ვისაც ექნება წვდომა თქვენს ქსელთან, შეეძლება შეცვალოს როუტერის კონფიგურაცია.  
  
- შეცვალეთ სტანდარტული სახელი და პაროლი. სასურველია პაროლი იყოს მინიმ 8 სიმბოლოს შემცველი და შედგებოდეს ციფრების, დიდი და პატარა ინგლისური ასოების კომბინაციისაგან.  
  
**უსაფრთხოების რეკომენდირებული მოთხოვნები:**შემდეგი რჩევები, თქვენს სახლის უკაბელო ქსელს დამატებით უსაფრთხოებას შესძენს:  
  
**განათავსეთ როუტერი ცენტრალურ პოზიციაზე**- როუტერიდან უკაბელო სიგნალი ვრცელდება რადიალურად  
  
- თუ უკაბელო როუტერი განთავსებულია გარე კედელთან ახლოს, მაშინ შესაძლებელია სიგ­ნალი ფარავდეს შენობის გარე პერიმეტრს, რაც აადვილებს ქსელზე წვდომას და შეტევის გან­ხორციელებას.  
  
- შეძლებისდაგვარად განათავსეთ როუტერი შენობის ცენტრალურ, შუა ნაწილში. ასეთ შემ­თხვევაში მთლიანად დაიფარება შენობის შიდა პერიმეტრი და სიგნალი ნაკლებად იქნება ხელმისაწვდომი გარედან.  
  
**გათიშეთ ინტერნეტი როდესაც ტოვებთ სახლს**- თუ აპირებთ დატოვოთ სახლი გარკვეული დროით, მაშინ უსაფრთხოების მიზნით სასურ­ველია ინტერნეტი გათიშული დატოვოთ  
  
- ამით თქვენ თავიდან აიცილებთ თქვენს ქსელში უცხო პირის შემოჭრას, რადგან თუ თქვენ ჩართულს დატოვებდით ინტერნეტ ქსელს, მაშინ თქვენს არყოფნაში, ვერ შეამჩნევდით საეჭ­ვო აქტივობას. ასევე დაზოგავთ ენერგიას!  
  
- ბევრ როუტერს აქვს ჩასართავი ღილაკი მოწყობილობის უკანა მხარეს. დაბრუნების შემდეგ ჩართეთ როუტერი. დაახლოებით 5 წუთში ინტერნეტ ქსელი ჩაირთვება და განაგრძობთ მის გამოყენებას.  
  
**გააუქმეთ ქსელის სახელის მაუწყებლობის ფუნქცია**- ქსელის სახელი (ან SSID) ჩვეულებრივ სტანდარტულად გადაიცემა. როდესაც თქვენ ამოწ­მებთ ხელმისაწვდომ ქსელებს, მაშინ ხედავთ როგორც საკუთარ ასევე სხვა ქსელებს (არსებო­ბის შემთხვევაში), რადგან ისინი მაუწყებლობენ საკუთარ ქსელის სახელს.  
  
- ღიად ქსელის სახელის მაუწყებლობის დროს, თქვენი ქსელი ხდება სამიზნე შემტევი პერ­სონებისთვის.  
  
- გააქტიურეთ ‘Disable SSID broadcast' , რათა თავიდან აიცილოთ თქვენი ქსელის გამოჩენა სხვა კომპიუტერების „ხელმისაწვდომ ქსელთა სიაში.“  
  
**გამოიყენეთ უკაბელო ქსელის ნაცვლად, საკაბელო**- რათქმაუნდა ვერავინ გამოიყენებს თქვენს უკაბელო ქსელს, თუ თქვენ თავად არ გამოიყე­ნებთ მას, პირველ რიგში! თუ თქვენი კოპმიუტერი განთავსებულია როუტერთან ახლოს, და არ არის კოპმიუტერის სხვადასხვა ადგილზე გადაადგილების აუცილებლობა, მაშინ დაუკავშირდით როუტერს კაბელის საშუალებით.  
  
- გამოიყენეთ პირდაპირი კაბელი როუტერთან დასაკავშირებლად და დროებით გათიშეთ როუტერის Wireless ფუნქცია. მეტ უსაფრთხოებასთან ერთად თქვენი კავშირი უფრო სწრაფი გახდება.  
  
**გაფილტრეთ MAC\* მისამართის მიხედვით**- ყველა კოპმიუტერის ქსელის ბარათს აქვს უნიკალური იდენტიფიკატორი - Mac მისმართი.  
  
- თუ თქვენ დაუშვებთ მხოლოდ კონკრეტულ MAC მისამართის მქონე კოპმიუტერებს თქვენს ქსელში, ამით დამატებით უსაფრთხეობას შესძენთ ქსელს და თქვენს ინფორმაციას.  
  
- გააქტიურეთ ფუნქცია 'Filter by Mac adress', და სათითაოდ დაამატეთ ის Mac მისამართები, რომელთაც აძლევთ ქსელის გამოყენების უფლებას.  
  
**გათიშეთ DHCP\* სერვისი**- სტანდარტულად, როდესაც თქვენ უკავშირდებით უკაბელო ქსელს, როუტერის DHCP სერ­ვისი თქვენს კოპმიუტერს გამოუყოფს უნიკალურ IP მისამართს. ამ მისამართის მიხედვით ხდება თქვენი იდენტიფიცირება ქსელში.  
  
- IP მისამართის ავტომატურად მინიჭების სერვისის გათიშვით, თქვენი ქსელის უფრო მეტად დაცული გახდება. არაავტორიზებული კოპმიუტერები ვერ მიიღებენ IP მისამართს ავტომა­ტურ რეჟიმში.  
  
- სერვისის გათიშვის შემდეგ, ხელით მიანიჭეთ ყოველ დაშვებულ კოპმიუტერს IP მისამარ­თი.  
  
DHCP – Dynamic Host Control Protocol   
MAC – Media Access Control   
IP – Internet Protocol  
  
Windows ოპერაციული სისტემაში თქვენ შეგიძლიათ ნახოთ თქვენი MAC მისამართი შემდეგნაირად:  
  
Start -> Command Prompt.  
  
აკრიფეთ ipconfig /all  
  
12 ციფრიანი კოდი - “Physical Adress”-ის გასწვრივ არის Mac მისამართი.  
  
ციფრები - “IP Adress” - თქვენი კომპიუტერისთვის მინიჭებული IP მისამართი.  
  
ციფრები - „Default Gateway” - თქვენი როუტერის IP მისამართი

ფიშინგი

***ფიშინგი*** *(ინგლისურად phishing:fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზითმომხმარებელს 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 სმს-ფიშინგი, ცნობილი როგორც სმიშინგი "SMiShing". თაღლითები თავის მსხვერპლს უგზავნიან სმს შეტყობინებას სადაც მოთავსებულია ფიშინგ საიტის ბმული. ბმულზე შესვლისთანავე მომხმარებელი ხდება ფიშერის მსხვერპლი და კარგავს პირად ინფორმაციას. სმს შეტყობინება აგ­რეთვე შეიძლება მოუწოდებდეს მომხმარებელს მითითებულ ნომერზე დაუყოვ­ნებლივ დაკავშირებას, რათა მისი პრობლემა იქნას გადაჭრილი.   
 **ფიშინგ წერილი** - ფიშინგ წერილი არის ელექტრონული ფოსტის მისამართზე მოსუ­ლი ყალბი წერილი, რომელიც თითქოს გამოგზავნილია ბანკის, სერვისის 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 რამოდნიმე 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.  
 **როგორ ხoრციელდება ფიშინგი -** 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.  
  
ფიშირების 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 ჯაშუშურ 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 გაუთვითცნობიერებულობაზე 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.  
 **ინტერნეტ ბრაუზერები, რომლებიც იუწყებიან ფიშინგის საფრთხეს** - ძალიან მნიშ­ვნე­ლოვანი მიმართულება იყო ფიშინგ საიტების სიის შექმნა (ეგრედ წოდებული ბლექლისტი), რომელსაც აქტიურად იყენებენ ისეთი ინტერნეტ ბრაუზერები, როგო­რიცაა: Internet Explorer, Mozilla Firefox, Google Chrome, Safari და Opera. 2006 წელს შეიქმნა DNS სერვისების მეთოდი , რომლიც ფილტრავს ცნობილ ფიშინგ საიტებს. ეს მეთოდი მუშაობს ყველა ზემოთ ჩამოთვლილ ინტერნეტ ბრაუზერში.  
 **ფიშინგთან ბრძოლა** - რამდენიმე წლის წინ ფიშინგთან საბრძოლველად შეიქმნა ანტი - ფიშინგის სამუშაო ჯგუფი (Anti-Phishing Working Group - APWG), რომელშიც გაერ­თიანებულები არიან ფიშინგის სამიზნე კოპმანიები, 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.

 ბოტნეტი

მოდით, სანამ ბოტნეტის განხილვას დავიწყებდეთ, შესავალი გავაკეთოთ და გან­ვსაზღვროთ ზოგადად რას ნიშნავს ბოტი და რა მიზნებისთვის გამოიყენება. ბოტი შემოკლებული ვარიანტია სიტყვისა რობოტი და ჩვენს შემთხვევაში იგი წარმოად­გენს მავნე პროგრამას, რომელიც ინსტალირდება მსხვერპლის კომპიუტერში და გარკვეული ადამიანის, ან ადამიანების ეგრეთ წოდებული BOT MASTER-ის მიერ კონტროლირდება. ბოტებს ხშირად იყენებენ სხვადასხვა მავნე ქმედებების ჩასადე­ნად, მაგალითად DDoS შეტევების განსახორციელებლად და Spam-ის გასაგზავნად. მოდით სანამ ბოტების განხილვაზე გადავიდოდეთ, განვიხილოთ რას ნიშნავს DDoS შეტევა.  
  
DDoS - გახლავთ შემოკლებული ფორმა Distributed Denial of Service-ის, რაც ნიშნავს სერვერის ან რაიმე სერვისის მიერ უარის თქმას მომსახურებაზე. DDoS ის შემთხვე­ვაში ძირითადად შეტევა ხორციელდება ბევრი დავირუსებული კომპიუტერის მეშვეობით, ანუ ეგრეთწოდებული ზომბირებული კომპიუტერების ჯგუფიდან, რომლებიც ერთდროულად ახორციენებენ შეტევას. როგორც ზემოთ ვახსენეთ, ეს მეთოდი გამოიყენება სერვერის ან რაიმე სერვისის ფუნქციის შეფერხებისთვის, გათიშვისთვის.  
  
DDoS შეტევის შემთხვევაში სხვადასხვა IP მისამართებიდან ერთდროულად ხდება ბევრი დავირუსებული კომპიუტერიდან დიდი ინფორმაციის გაგზავნა მსხვერპლის მისამართით. მსგავსი შეტევის აღმოჩენა დიდ სირთულეს არ წარმოადგენს, მაგრამ შეტევის შეჩერება და მასზე რეაგირება ძალზედ რთულია. როდესაც მსგავსი შეტევა ერთი IP მისამართიდან ხდება, ის ძალზედ მარტივად იბლოკება Firewall-ის საშუალებით.  
  
ზოგადად მრავალი სახეობის ბოტი არსებობს, რომლებიც ერთმანეთისგან დანიშნულებით და ფუნქციით განსხვავდებიან. მაგალითად:  
  
· V0idBot

· z3r0xb0t

· Hunter Bot

· Ago bot

· RX-Bot  
  
ჩამოთვლილი ბოტების უმრავლესობა ტრადიციულად IRC (Internet Realay Chat) პრო­ტოკოლზეა ბაზირებული, რომელიც ბოტის ადმინისტრირებას და მართვას ძალზე მარტივს ხდის. უნდა აღვნიშნოთ, რომ IRC(Internet Relay Chat) წარმოადგენს პროტო­კოლს, რომელიც ჩათისთვის გამოიყენება. აგრეთვე ხშირად გვხვდება ეგრეთწოდებუ­ლი Web Based - ვებ საიტებზე ბაზირებული ბოტნეტები.  
  
ახლა გადავიდეთ კონკრეტულად ბოტნეტზე და განვიხილოთ თუ რას წარმოადგენს იგი.ბოტნეტი, იგივე ზომბების არმია, წარმოადგენს ზემოდ მოყვანილ ბოტების ორ­განიზებულ ჯგუფს, რომელიც ერთი ან რამოდენიმე ადამიანის მიერ კონტროლირ­დება. ბოტნეტის მფლობელი ცდილობს მაქსიმალურად გაავრცელოს ბოტი, რათა უფრო მძლავრი გახდეს მისი რესურსი.  
  
გასავრცელებლად მრავალი ხერხი გამოიყენება, სპამი IRC სერვერებზე და იმეილზე. ხშირად ბოტები P2P(Peer To Peer) ქსელების საშუალებით ვრცელდება, P2P ქსელი ძი­რითადად ფაილების გასაცვლელად გამოიყენება. აგრეთვე ბოტები ხშირად ვრცელ­დებიან ეგრეთწოდებული „Warez” საიტების საშუალებით.  
  
ბოლო პერიოდში ბოტნეტის მასშტაბური გავრცელებიდან გამომდინარე, ძალიან დი­დია იმის შანსი, რომ თქვენი პერსონალური კომპიუტერი ბოტნეტის ნაწილი იყოს. იმისათვის რომ ბოტნეტის მსხვერპლი არ გახდეთ, უნდა გეყენოთ ანტივირუსი, მუდ­მივად უნდა განაახლოთ თქვენი ოპერაციული სისტემა, გააკეთოთ ეგრეთწოდებული აფდეითები, ანუ მუდმივად უნდა იზრუნოთ თქვენი პერსონალური კომპიუტერის უსაფრთხოებაზე.

ელექტრონული ფოსტა და უსაფრთხოება

ელექტრონული ფოსტა დღეისათვის კომუნიკაციის ერთ-ერთ ყველაზე პოპულარულ მეთოდს წარმოადგენს. ის გამოიყენება, როგორც ბიზნეს-ურთიერთობებისთვის, ასე­ვე მეგობრებთან და ოჯახის წევრებთან კომუნიკაციისთვის. იმდენად,რამდენადაც ელექტრონული ფოსტა ინტერნეტ-ტექნოლოგიებს ეფუძნება, მისი გამოყენება დაკავ­შირებულია ისეთ საფრთეებთან, როგორიცაა **მავნე კოდი და ფიშინგი**(ინტერნეტ-თაღლითობის სახეობა, რომელიც მიზნად ისახავს პირადი მონაცემების ხელში ჩაგ­დებას).  
  
განვსაზღვროთ ელექტრონულიო ფოსტის უსაფრთხოების რამდენიმე მახასიათე­ბელი და გავეცნოთ იმ გამოცდილებას, რომელიც შეიძლება გამოყენებული იქნას ელექტრონული ფოსტით უსაფრთხო სარგებლობისთვის.  
  
***ელექტრონული ფოსტის უსაფრთხოების ზოგადი მახასიათებლები*ელექტრონული ფოსტა არ არის უსაფრთხო**· ელექტრონულ ფოსტა არ უნდა განვიხილოთ, როგორც კომუნიკაციის უსაფრთხო საშუალება, რადგან უმეტეს შემთხვევაში ეს ასე არ არის. ელ-ფოსტის წერილები იგ­ზავნება ინტერნეტის საშუალებით და გზად ბევრს სამარშრუტიზაციო სერვერს გაივ­ლის.  
  
· იმის მიუხედავად, დაშიფრული გაქვთ თუ არა გზავნილი, მისი წაკითხვა შესაძ­ლებელია მესამე პირის მიერ, რომელიც მოახერხებს გზავნილის ხელში ჩაგდებას, ხოლო დაშიფრვა 100%-იან გარანტიას არ იძლევა.  
  
**ელექტრონული მიმოწევა იურიდიულ ნორმებს ექვემდებარება**· ელექტრონული ფოსტა, ერთი შეხედვით კომუნიკაციის არაკონტროლირებადი სა­შუალებაა, მაგრამ მომხმარებელმა უნდა იცოდეს, რომ ელექტრონული გზავნილები შეიძლება ისევე დაექვემდებაროს იურიდიულ ნორმებს, როგორც ჩვეულებრივი წე­რილები და ისინი გამოყენებული იქნან სამხილის ან ნივთმტიცების სახით.  
  
· კარგად დაფიქრდით, რას აგზავნით ელექტრონული ფოსტის საშუალებით და წერი­ლი გულდასმით წაიკითხეთ, სანამ გაგზავნის ღილაკს დააჭერთ.  
  
**გაგზავნილ წერილს უკან ვეღარ დააბრუნებ**· გაგზავნილი ელექტრონული წერილის უკან გამოხმობა შეუძლებელია. მიუხედავად იმისა, რომ ელექტრონული ფოსტის ზოგიერთ პროგრამულ უზრუნველყოფას წერი­ლის უკან დაბრუნების ( “recall”) ფუნქცია აქვს, დარწმუნებული ვერ ვიქნებით, რომ გაგზავნილი წერილი არავის წაუკითხავს, ამასთან ელექტრონული ფოსტა ბევრ სერ­ვერს გაივლის დანიშნულების ადგილამდე და ყველგან თავის კვალს ტოვებს.  
  
· ყოველთვის ორჯერ გადაამოწმეთ წერილის მიმღებთა სია და გზავნილის შინაარსი გაგზავნამდე. თავი შეიკავეთ სამსახურთან დაკავშირებული ელექტრონული ფოსტის გაგზავნისგან მაშინ, როდესაც გაბრაზებული ხართ ან ალკოჰოლის ზემოქმედების ქვეშ იმყოფებით.  
  
**მოერიდეთ თაღლით მგზავნელებს**

· არაკეთილსინდისიერი მგზავნელების მხრიდან ძალიან ადვილია ისეთი წერილის გაგზავნა, რომელიც ერთი შეხედვით რეალური მისამართიდან მოსულს ჰგავს. ეს მეთოდი ყველაზე ხშირად გამოიყენება მავნე კოდის გავრცელებისას ან ფიშინგის დროს.  
  
· არ გახსნათ საეჭვო ელექტრონულ გზავნილზე მიბმული ფაილები და ბმულები, იმ შემთხვევაშიც კი, თუ იცნობთ მის გამომგზავნს და ენდობით მას. მცირე ეჭვის გაჩე­ნის შემთხვევაშიც ტელეფონით ან სხვა საშუალებებით დაუკავშირდით გამომგზავნს, რათა დაადგინოთ გზავნილი მართლა მისგან არის თუ არა. ასეთი გაუგებრობის თა­ვიდან აცილების კარგი საშალებაა **ელექტრონული ხელმოწერა**.  
  
***ელექტრონული ფოსტის უსაფრთხოების ზომები*რა წესებია შემოღებული თქვენს ორგანიზაციაში**· თქვენს ორგანიზაციაში შეიძლება დამტკიცებული იყოს „მისაღები გამოყენების პოლიტიკა “ეელქტრონული ფოსტით სარგებლობისთვის, რომელსაც უნდა იცნობ­დეთ და მისდევდეთ;  
  
· ეს პოლიტიკა შემოღებულია, იმისთვის, რომ დაცული იყოთ თქვენ და თქვენი კომ­პიუტერი. ეს პოლიტიკა, როგორც წესი მოიცავს სამსახურებრივი ელექტრონული ფოსტის გამოყენების წესებს, ინფორმაციის ტიპებს, რომელთა გაგზავნა დასაშვებია ელ.ფოსტის საშუალებით და ელექტრონული ფოსტით კომუნიკაციის მონიტორინგის შესაძლებლობას თქვენი ორგანიზაციის მხრიდან.  
  
**დაშიფრეთ მნიშვნელოვანი გზავნილები**· დაუშიფრავად გაგზავნილი ელექტრონული წერილი ღია ბარათივითაა, ის შეიძ­ლება წაიკითხოს **ნებისმიერმა** იმ გზაზე, რასაც წერილი ადრესატამდე გაივლის. და­შიფრული ელექტრონული გზავნილი კონვერტში ჩადებულ წერილს ჰგავს.  
  
· მნიშვნელოვანი ინფორმაციის შემცველი ელ. ფოსტის გაგზავნისას აუცილებლად გამოიყენეთ დაშიფრვის მეთოდები, ამისთვის ყველაზე ხშირად გამოიყენება **PGP** და **S/MIME** მეთოდები. თუ ვერ ახერხებთ მნიშვნელოვანი წერილის დაშიფრვას, მაშინ მისი შიგთავსი მოათავსეთ ფაილში, დაშიფრეთ ფაილი, მიაბით წერილს და ისე გაგ­ზავნეთ.  
  
**დიდი სიფრთხილით გადაამოწმეთ მისამართები, სადაც ელექტრონულ წერილს აგ­ზავნით**· ძალიან ხშირია ელექტრონული ფოსტის შეცდომით გადაგზავნის შემთხვევები, განსაკუთრებით მაშინ, თუ იყენებთ ფუნქციას „უპასუხე ყველას“ (Replay to All). ელექტრონული წერილი მხოლოდ იმათ უნდა გაეგზავნოს, ვისთვისაც მისი შინაარსი აქტუალურია.  
  
· კარგად დაფიქრთით წერილის შნაარსზე და ორჯერ გადაამოწმეთ მიმღებთა სია, სანამ გაგზავნის ღილაკს დააჭერთ.  
  
**მუდმივად განაახლეთ პროგრამული უზრუნველყოფა**· მავნე კოდმა ან ჰაკერებმა შეიძლება ისარგებლონ პროგრამული უზრუნველყოფის სუსტი მხარეებით თქვენს კომპიუტერში შემოსაღწევად და მნიშვნელოვან ინფორ­მაციაზე წვდომისათვის;  
  
· იზრუნეთ, რომ თქვენს კომპიუტერზე დაინსტალირებული ყველა პროგრამული უზრუნველყოფა, ელექტრონული ფოსტის კლიენტის ჩათვლით ინფორმაციული უსაფრთხოების კუთხით ბოლო ვერსიებით და პაჩებით იყოს განახლებული;

**გამოიყენეთ ინფორმაციული უსაფრთხოების პროგრამული უზრუნველყოფა**· ელექტრონული ფოსტა მავნე კოდის გავრცელების და ფიშინგური შეტევების ყვე­ლაზე გავრცელებული მეთოდია. უნდა გამოვიყენოთ ინფორმაციული უსაფრთხო­ების სპეციალური პროგრამული უზრუნველყოფები, რომელიც ამ ტიპის საფრთხე­ების პრევენციისა და მათგან დაცვისთვის გამოიყენება.  
  
· დარწმუნდით, რომ თქვენს კომპიუტერს აქვს ბოლო ვერსიით განახლებული მავნე კოდისგან დამცავი პროგრამული უზრუნველყოფა, უსაფრთხოდ კონფიგურირებუ­ლი ფაირვოლი და სპამის გააქტიურებული ფილტრი.  
  
**არ დააკლიკოთ ბმულებზე**· საფრთხილო გზავნილები ხშირად მოიცავს ინტერნეტ ბმულებს (URL), რომლებიც გვამისამართებენ მავნე კოდის შემცველ ვებ-გვერდებზე. მხოლოდ ბმულზე დაკლი­კებითაც კი შეიძლება კომპიუტერის დაინფიცირება.  
  
· ყოველთვის სიფრთხილით მოეკიდეთ ნებისმიერი სახის ბმულს და არასდროს და­აკლიკოთ ბმულებზე, რომელსაც შეიცავს გზავნილები უცნობი ან საეჭვო მისამართე­ბიდან;  
  
**არ გახსნათ მიმაგრებული ფაილები**· საფრთხილო გზავნილები ხშირად შეიცავს მიმაგრებულ ფაილებს, რომლებიც შეიძ­ლება მავნე კოდით იყოს დაინფიცირებული. ასეთი კოდი შეიძლება **ნებისმიერი ტი­პის ფაილში** იყოს დამალული, PDF და ZIP ფაილების ჩათვლით.  
  
· არასდროს გახსნათ მიმაგრებული ფაილები, რომლებიც მოსულია უცნობი ან საეჭვო მისამართებიდან, დარწმუნებული იყავით, რომ მიმაგრებული ფაილი ყოველთვის შემოწმებულია მავნე კოდის არსებობაზე.  
  
**ისარგებლეთ ვებ-ფოსტის (https) მხოლოდ უსაფრთხო სერვისებით**· იმ შემთხვევაში თუ ვებ-ფოსტის სერვისით სარგებლობთ, შეამოწმეთ რამდენად უს­აფრთხოა სისტემაში შესვლა (მომხმარებლის სახელით და პაროლით), სულ მცირე იმ დონეზე მაინც, ამ სერვისის ვებ-მისამართი შეიცავს თუ არა “https://”-ს (სადაც“s” აღ­ნიშნავს უსაფრთხოს - „Secure”).  
  
· იდეალურ შემთხვევაში, სრული ონლაინ სესია (ანუ ყველა კომუნიკაცია თქვენს კომპიუტერსა და ონლაინ ექაუნთს შორის) უნდა იყოს უსაფრთხო. ასეთი სერვისი მაგალითს წარმოადგენს Gmail, თუმცა ამ შემთხვევაშიც Gmail Setting-ში უნდ ამოხდეს ამ მოთხოვნის აქტივაცია.  
  
**გამორთეთ შიგთავსის ავტომატური ჩამოტვირთვის ფუნქცია**· სურათებისა დ ასხვა დინამიური შიგთავსის ავტომატური ჩამოტვირთვა შეიძლება ძალიან მოსახერხებელი და ლამაზი იყოს, მაგრამ ამასთანავე მათთან ერთად შეიძლე­ბა ჩამოიტვირთოს მავნე კოდი, ან არაკეთილსინდისიერ მგზავნელებს მიუვიდეს ინ­ფორმაცია, რომ თქვენი აქაუნთი აქტიურია.  
  
· სულ მცირე, აუცილებელია გამორთოთ შიგთავსის ავტომატური ჩამოტვირთვის ფუნქცია, მანამ, სანამ არ დარწმუნდებით, რომ გამომგზავნის მისამართი სანდოა. დაც­ვის უფრო მაღალ დონეს წარმოადგენს ყველა სახის დინამიური შიგთავსის დაბ­ლოკვა და წერილის მხოლოდ ტექსტის სახით გამოყვანის ფუნქციის გააქტიურება.

**გამორთეთ წინასწარი დათვალიერების პანელი**· ელექტრონული ფოსტის ბევრ პროგრამას აქვს „წინასწარი დათვალიერების პანე­ლის“ ფუნქცია, რომელიც ელექტრონული წერილის შეიგთავსს გვაჩვენებენ, რაც თვი­სობრივად იგივეა, რაც გზავნილის გახსნა, შესაბამისად ამ დროს შეიძლება მოხდეს მავნე კოდით დაინფიცირება.  
  
· ელექტრონული ფოსტის დიდი ნაწილი შეიძლება წინასწარვე იყოს იდენტიფიცირე­ბული, როგორც სპამი, ფიშინგი ან მავნე კოდის შემცველი და გაუხსნელად წაიშალოს. წინასწარი დათვალიერების პანელის ფინქციის გამორთვით თავიდან ავიდირებთ ასეთი წერილების გახსნას.  
  
**გამოიყენეთ ძლიერი და უნიკალური პაროლები**· პაროლი საშუალებას გვაძლევს დავიცვათ ჩვენი ელექტრონული ფოსტა შემოტევისა და არასანქცირებული წვდომისგან. შესაბამისად, რამდენიმე ინტერნეტ აქაუნთზე ერ­თი დ აიმავე პაროლის გამოყენება ყველა ამ აქაუნთზე წვდომის შესაძლებლობას იძ­ლევა, იმ შემთხვევაში, თუ ერთი მაინც გატყდა.  
  
· გამოიყენეთ პაროლი, რომელიც შეიცავს არანაკლებ 8 სიმბოლოს, მათ შორის და­ბალი და მაღალი რეგისტრის სიმბოლოებს, რიცხვებს და სპეციალურ სიმბოლოებს. პაროლი ხშირად ცვალეთ და სხვა აქაუნტზე არ გამოიყენოთ.  
  
**არ დაგავიწყდეთ სისტემიდან გამოსვლა (Log Out)**· ზიარი კომპიუტერიდან (მაგ. ინტერნეტ კაფეში) ვებ-ფოსტის გამოყენების ყველაზე ტიპიური შეცდომაა სისტემიდან გამოსვლის დავიწყება. ეს საშუალებას მისცემს მომ­ხმარებელს, რომელიც ამავე კომპიუტერთან მუშაობს, უპრობლემოდ დაათვალიეროს ვებ-ფოსტის აქაუნთი.  
  
**წაშალეთ ან დააარქივეთ ძველი ელექტრონული წერილები**· თუ ელექტრონული ფოსტის ერთ აქაუნთს დიდი ხნის განმავლობაში ხმარობთ, დი­დი შანსია, რომ მასზე დაგროვილია დიდი რაოდენობით მნიშვნელოვანი ინფორმა­ცია თქვენს შესახებ და თქვენი ორგანიზაციის შესახებ. ამის გამო მუდმივად იზრდე­ბა მნიშნელოვან ინფორაციაზე არასანქცირებული წვდომის რისკი;  
  
· ნუ შეინახავთ ელექტრონულ წერილებს წლების მანძილზე. წაშალეთ ან უსაფრთ­ხოდ დააარქივეთ ყველა ის წერილი, რომელიც აღარ გჭირდებათ.