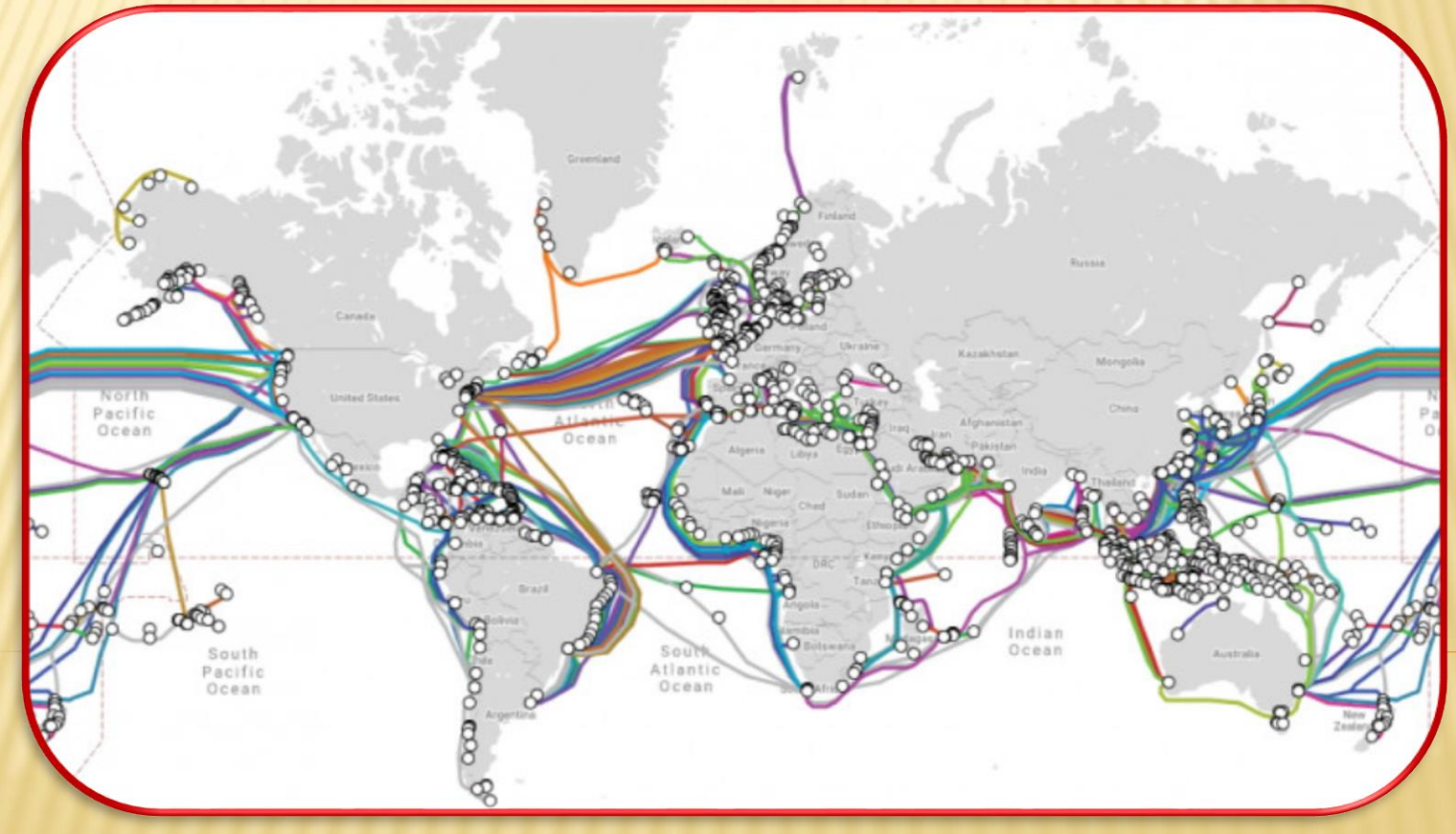
თემა 3.
ინტერნეტი. ვირუსები და მათთან ბრძოლა



ინტერნეტი (Internet) არის "მსოფლიო-ქსელი", ერთმანეთზე მიერთებული კომპიუტერების საჯაროდ ხელმისაწვდომი ქსელი. ინტერნეტს, ზოგჯერ ეძახიან, უბრალოდ "ქსელს“ (The Net), ანუ ქსელთა ქსელს, სადაც მომხმარებლებს, თუ მათ აქვთ უფლებები, შეუძლიათ ნებისმიერი კომპიუტერიდან მიიღონ ინფორმაცია. ინტერნეტი აღნიშნავს გლობალურ კომპიუტერულ ქსელს, რომელიც ეფუძნება IP პროტოკოლს და პაკეტთა მარშრუტიზაციას. ინტერნეტი ქმნის გლობალურ საინფორმაციო სივრცეს და წარმოადგენს მსოფლიო ქსელის საფუძველს.

ვინ შექმნა ის?

ვები, როგორც ჩვენ მას ვუწოდებთ, გამოიგონა ტიმ ბერნეს-ლიმ, რომელიც მუშაობდა CERN-ის ლაბორატორიაში. მის ნამუშევარს საფუძვლად ედო პოპულარული თეორია ჰიპერტექსტული გზავნილის (HTML) შესახებ. ნებისმიერ პერსონალურ კომპიუტერში ჩატვირთულ Windows გააჩნია ჰიპერტექსტის მარტივი ვერსია.

2004 წელს ბრიტანეთში დასახელდა ყველაზე დიდებული ინგლისელი. ეს იყო ბერნეს ლი, რომელმაც შექმნა "**World Wide Web**" – ი მსოფლიო ქსელი.

მალე ის გახდა ბრიტანეთის იმპერიის ორდენის მფლობელი, უფრო მარტივად რომ ავხსნა რაინდის წოდება მიიღო.

IP (Internet Protocol - ქსელთაშორისი ოქმი) მარშრუტიზაცია ქსელური ოქმი, საფუძველი **TCP/IP** ოქმების სტეკი.

IP ოქმი (RFC 791) გამოიყენება ქსელის ერთი ჰოსტიდან მეორეზე მონაცემთა არასანდო (პაკეტებად დაყოფილად) გადასაცემად. ეს ნიშნავს, რომ ამ ოქმის დონეზე მონაცემთა დანიშნულებამდე უცვლელად მისვლის გარანტია არ არსებობს. პაკეტები შეიძლება თავდაპირველი თანმიმდევრობით არ მივიდნენ, დაზიანდნენ ან საერთოდ დაიკარგონ. საიმედოობის გარანტიას იძლევა ისეთი სატრანსპორტო ოქმი, როგორიცაა **TCP (Transmission Control Protocol)**, რომელიც **IP**-ს ტრანსპორტად იყენებს.

ინტერნეტში გამოიყენება მეოთხე ვერსიის **IP**, რომელიც ასევე ცნობილია როგორც **IPv4**. ამ ვერსიის **IP** ოქმში, ქსელში არსებულ ყოველ წერტილს მიენიჭება **IP** მისამართი, რომელიც ოთხი ოქტეტისგან შედგება. ამგვარად ქვექსელებში კომპიუტერები ერთიანდებიან მისამართის საერთო პირველი ბიტებით. ამ პირველ ბიტებს ასევე ეწოდება ქვექსელის ნიღაბი.

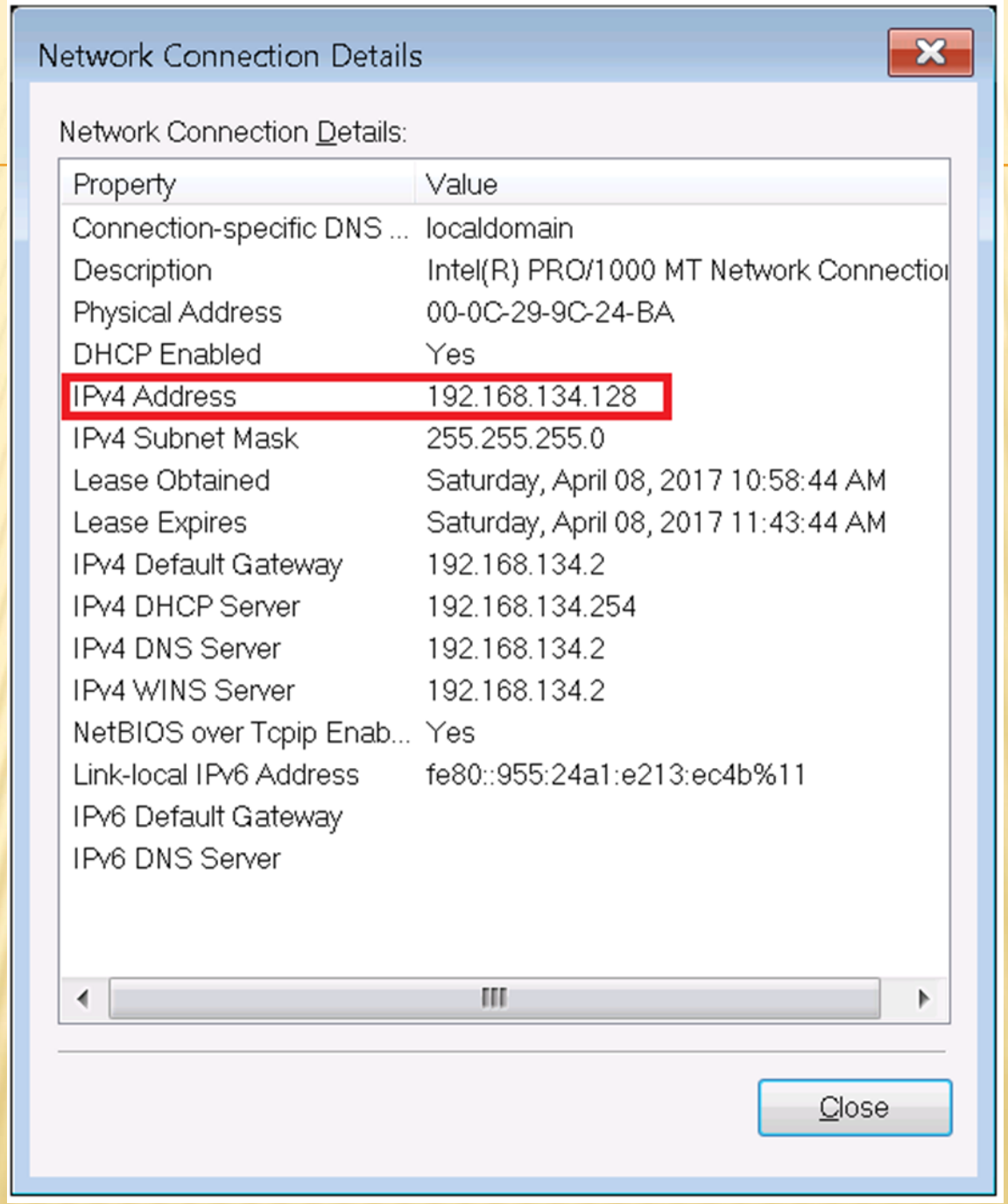
კვანძს (**Host**) ქსელში (მათ შორის ინტერნეტის ქსელში) იდენტიფიცირებისათვის უნდა ჰქონდეს შემდეგი ლოგიკური მისამართები:

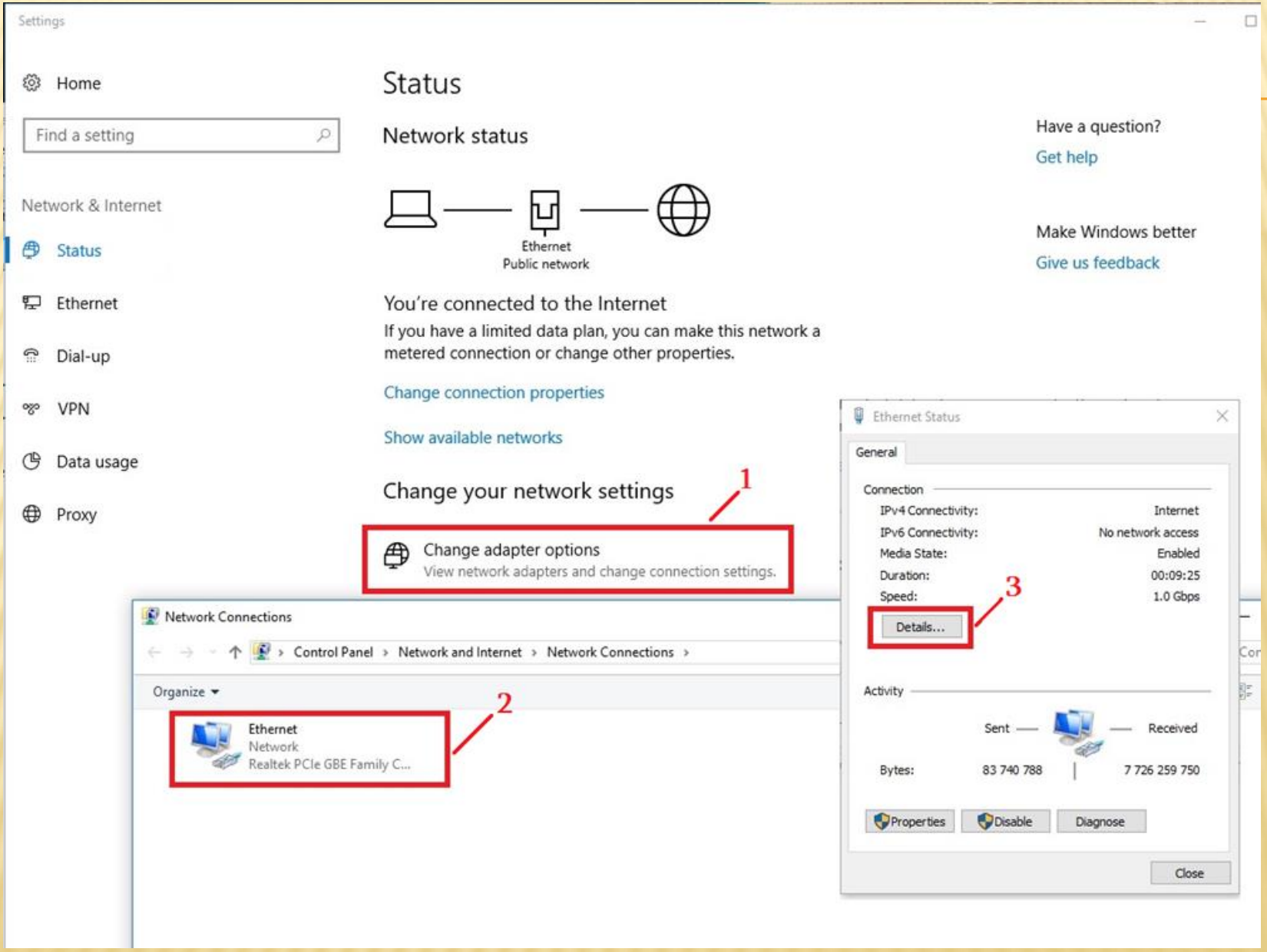
IP address - აი-პი მისამართი, უშუალოდ კვანძის უნიკალური მისამართი;

Subnet mask - ქვექსელის ნიღაბი, განსაზღვრავს ქსელის ზომას;

Default Gateway – ”შლუზი” (კარიბჭე სხვა ქსელებში), იმ მოწყობილობის მისამართი, რომელიც მოცემულ ქსელს (რომელშიც კონკრეტული კვანძია ჩართული) აკავშირებს სხვა ქსელებთან (ჩვეულებრივ ასეთი მოწყობილობაა მარშრუტიზატორი (**Router**);

Domain Name System Server Address - დომენური სახელების სისტემის სერვერის მისამართი.


Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DNS ...
localdomain
Description
Intel(R) PRO/1000 MT Network Connectio
Physical Address
00-0C-29-9C-24-BA
DHCP Enabled
Yes
IPv4 Address
192.168.134.128
IPv4 Subnet Mask
255.255.255.0
Lease Obtained
Saturday, April 08, 2017 10:58:44 AM
Lease Expires
Saturday, April 08, 2017 11:43:44 AM
IPv4 Default Gateway
192.168.134.2
IPv4 DHCP Server
192.168.134.254
IPv4 DNS Server
192.168.134.2
IPv4 WINS Server
192.168.134.2
NetBIOS over Tcpip Enab...
Yes
Link-local IPv6 Address
fe80::955:24a1:e213:ec4b%11
IPv6 Default Gateway
IPv6 DNS Server
Close


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Data usage
Proxy
Status
Network status
Ethernet
Public network
You're connected to the Internet
If you have a limited data plan, you can make this network a metered connection or change other properties.
Change connection properties
Show available networks
Change your network settings
1
Change adapter options
View network adapters and change connection settings.
Have a question?
Get help
Make Windows better
Give us feedback
Network Connections
Control Panel › Network and Internet › Network Connections ›
Organize
2
Ethernet
Network
Realtek PCIe GBE Family C...
Ethernet Status
General
Connection
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:09:25
Speed: 1.0 Gbps
3
Details...
Activity
Sent
Received
Bytes: 83 740 788 7 726 259 750
Properties
Disable
Diagnose
Close

არსებობს **IP**-მისამართების მინიჭების ორი ხერხი:

- სტატიკური **IP**-დამისამართება. ამ შემთხვევაში ქსელის ყოველი კომპიუტერისათვის **IP**-მისამართის, ქვექსელის ნიღბისა და **TCP/IP** პროტოკოლის სხვა პარამეტრების შეყვანა ხდება ხელით.
- დინამიკური **IP**-დამისამართება. ქსელში ჩართვისას კომპიუტერი ავტომატურად იღებს **TCP/IP** პარამეტრებს. ამისათვის ქსელის ერთ-ერთმა კომპიუტერმა უნდა შეასრულოს **DHCP**-სერვერის ფუნქცია, ე.ი. „დაურიგოს“ **IP**-მისამართები ყველა ხელახლა მიერთებულ კომპიუტერს.

ლოკალური ქსელების დიაპაზონები

მომხმარებლის კომპიუტერის ინტერნეტში ჩართვის შემდეგ, IP მისამართი კომპიუტერს პროვაიდერის მიერ ენიჭება. ხოლო ლოკალური ქსელებისთვის გამოყოფილია IP მისამართთა შემდეგი დიაპაზონები:

192.168.0.1 — 192.168.255.254

172.16.0.1 — 172.31.255.254

10.0.0.1 — 10.255.255.254

კომპიუტერებს ასეთი მისამართებით ინტერნეტთან წვდომა შეუძლიათ პროქსი სერვერების ან NAT-ის მეშვეობით.

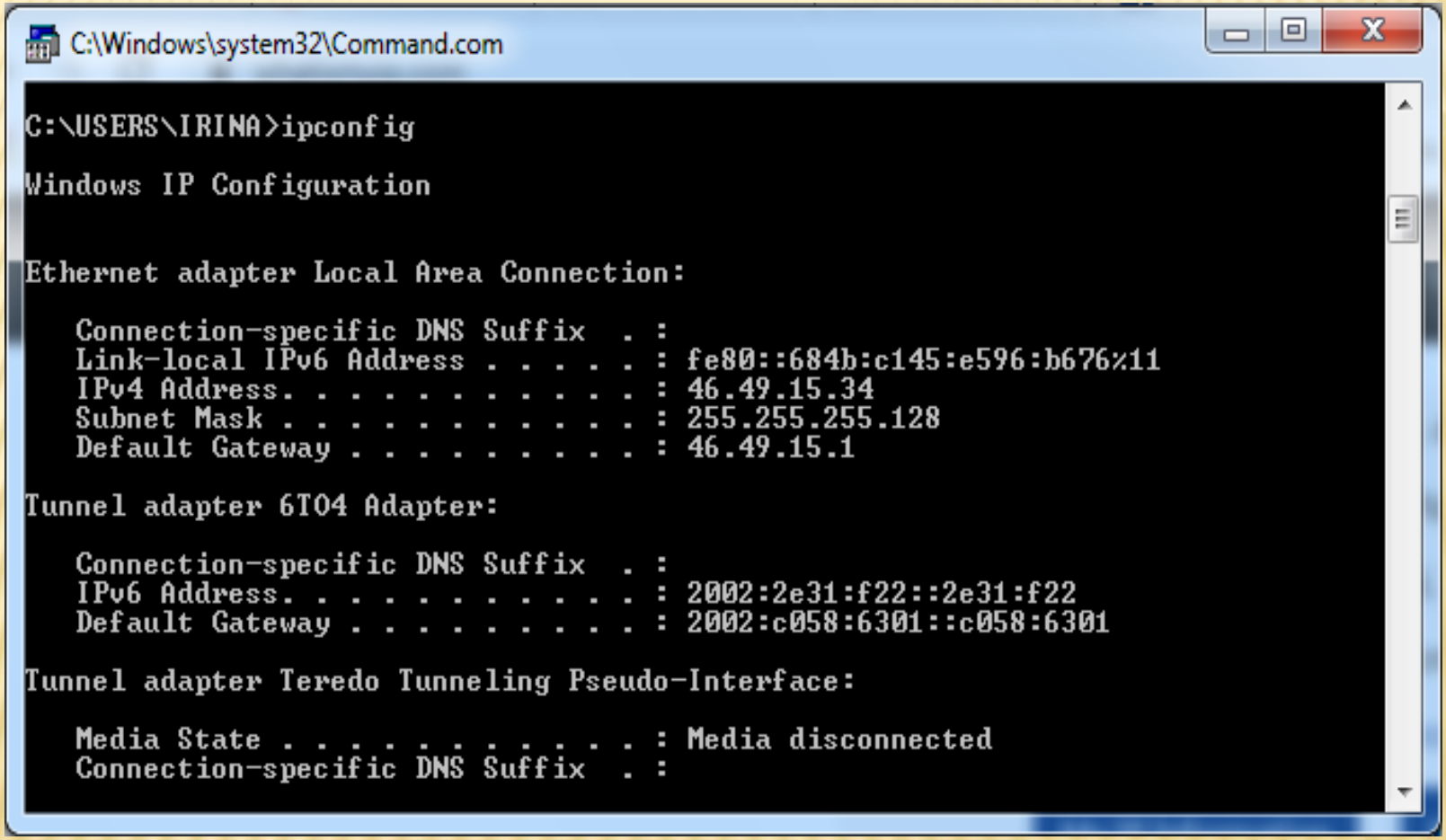
http://whatismyip.com/ , http://ip4.me

https://www.iplocation.net/

https://ipinfo.info/html/ip_checker.php

- Click Start
- Click All Apps expand the Accessories menu
- In the Accessories menu, Right Click Command Prompt and choose Run as Administrator
- Type ipconfig hit enter

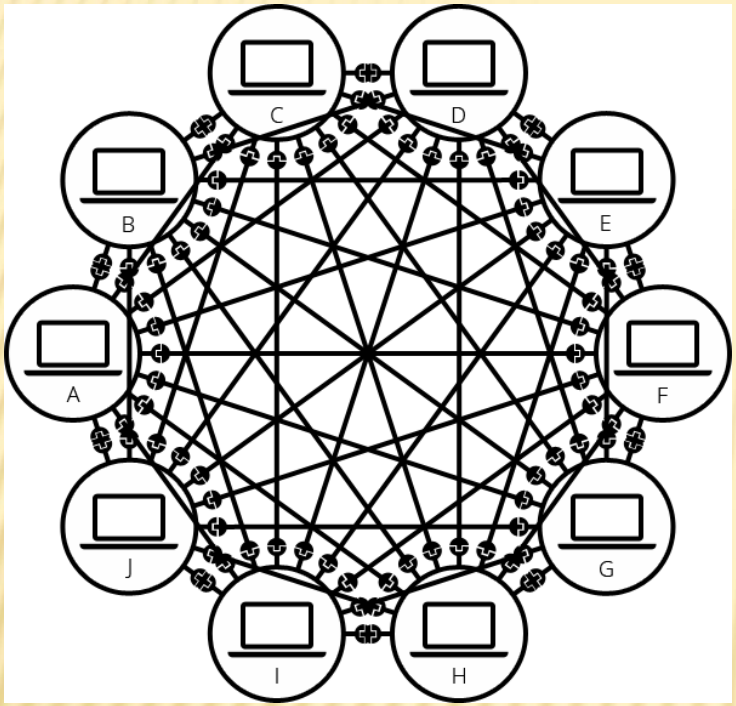
https://www.site24x7.com/ping-test.html


C:\Windows\system32\Command.com
C:\USERS\IRINA>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::684b:c145:e596:b676%11
IPv4 Address. . . . . : 46.49.15.34
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 46.49.15.1
Tunnel adapter 6TO4 Adapter:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2002:2e31:f22::2e31:f22
Default Gateway . . . . . : 2002:c058:6301::c058:6301
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

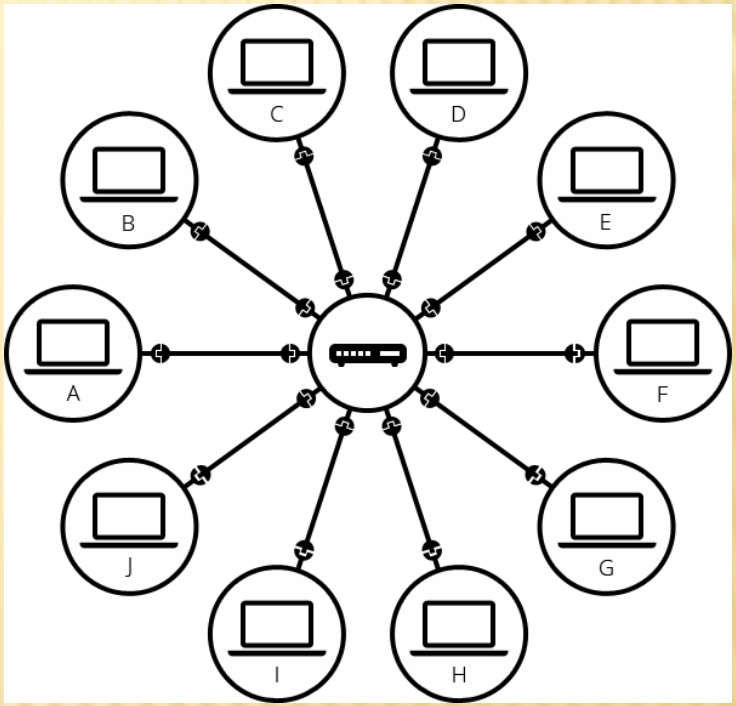
ლოკალური ქსელის ტოპოლოგიები - ლოკალური ქსელის არქიტექტურა

სალტური ტოპოლოგია (**BUS**)

სალტე არის უმარტივესი ფიზიკური ტოპოლოგია. ის შედგება მხოლოდ ერთი კაბელისაგან, რომელიც უერთდება ყველა კომპიუტერს.



ბადისებრი ტოპოლოგია (**MESH**)



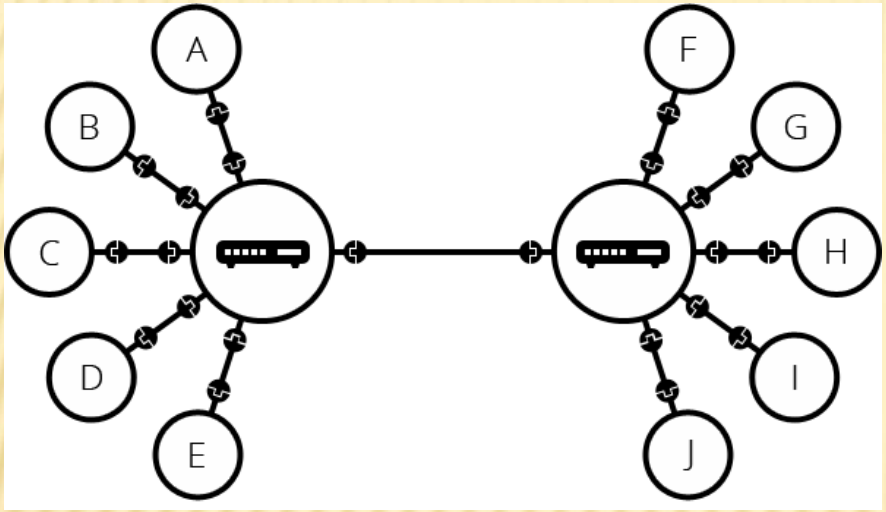
ვარსკვლავური ტოპოლოგია (**STAR**)

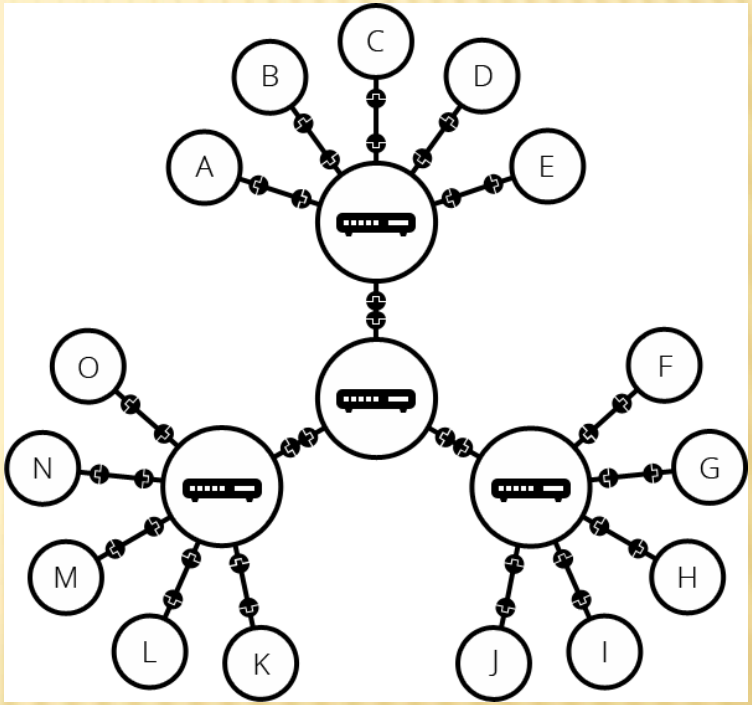
წრიული ტოპოლოგია (**RING**)

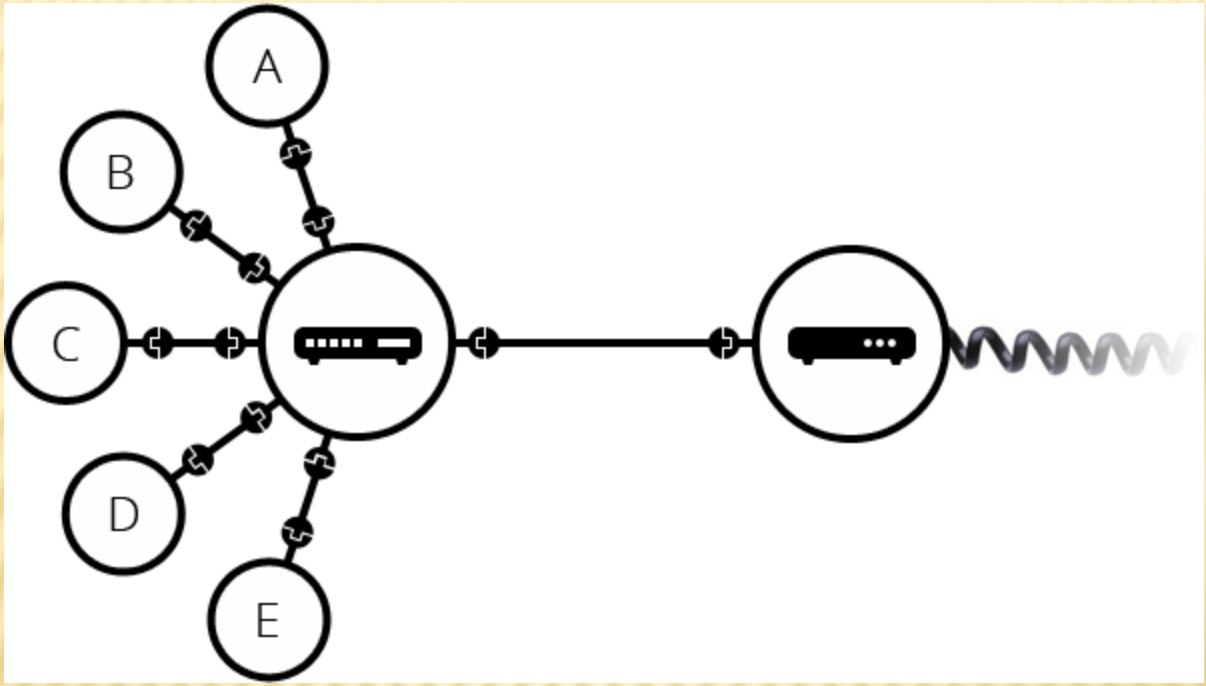
ჰიბრიდული ტოპოლოგია (**Hybrid**)

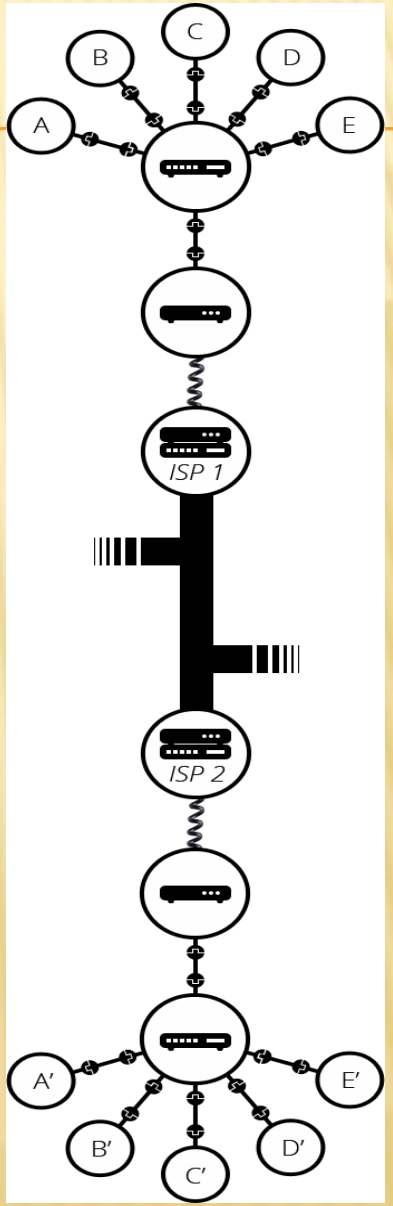
ვარსკვლავური ფიზიკური ტოპოლოგია აკავშირებს თითოეულ ქსელურ მოწყობილობას ცენტრალურ მოწყობილობასთან, რომელსაც ჰქვია ჰაბი (**HUB**). ახალი სამუშაო მანქანების დამატება მასში ძალიან ადვილია, ხოლო თუ რომელიმე სამუშაო მანქანა გამოვა მწყობრიდან, არც ეს შეუშლის ხელს სხვა მანქანების მუშაობას, თუმცა როგორც, ალბათ, მიხვდით, თუ ცენტრალური მოწყობილობა დაზიანდა, მთელი ქსელი შეწყვეტს მუშაობას.

ჰიბრიდული ტოპოლოგია მოიცავს ერთმანეთში შერეულ სხვადასხვა ტოპოლოგიებს. ამის ჩვენება სურათით შეუძლებელია, რადგანაც ძალიან ბევრი ვარიანტი არსებობს. დღესდღეობით, ფაქტიურად, ყველა ქსელი შერეულია და სხვადასხვაგვარი. ჰიბრიდული ტოპოლოგია შეიძლება სხვა დანარჩენ ტოპოლოგიებზე ძვირიანი იყოს, მაგრამ მას ყოველი მათგანიდან საუკეთესო თვისებები აქვს აღებული.


A
B
C
D
E
F
G
H
I
J


C
B
D
A
E
O
F
N
G
M
H
L
K
J
I


A
B
C
D
E


A
B
C
D
E
ISP 1
ISP 2
A′
B′
C′
D′
E′

როგორც აღვნიშნეთ, ინტერნეტის სიგნალი ვრცელდება კომპიუტერული ქსელების საშუალებით. ქსელური მოწყობილობები უკავშირდებიან ერთმანეთს სხვადასხვა ტიპის საშუალებებით:

- სპილენძის კაბელებით - მოწყობილობებს შორის მონაცემთა გადასაცემად იყენებს დენის სიგნალს;

- ოპტიკურ-ბოჭკოვანი კაბელებით - იყენებს შუშას და პლასტმასის სადენს, ე.წ. ბოჭკოვანს, რათა გადასცეს სინათლის სხივის იმპულსების მეშვეობით ინფორმაცია;

- უკაბელო კავშირი - იყენებს რადიო სიგნალებს, ინფრაწითელ ტექნოლოგიას (ლაზერებს), ან სატელიტურ კავშირებს. **Wi-Fi (ინგლ. wireless fidelity)** - ლოკალურ ქსელში უმავთულო კავშირის დამყარების საშუალება.

კომპიუტერებს შორის როლების განაწილების თვალსაზრისით ქსელები არსებობენ ერთრანგიანი, სადაც ყველა კომპიუტერი თანასწორუფლებიანია, და კლიენტ-სერვერული.

ინფორმაციის გადაცემის სიჩქარის მიხედვით ქსელები შეიძლება დავყოთ დაბალი (10 მბიტ/წმ-დე), საშუალო (100 მბიტ/წმ-დე), და მაღალი სიჩქარის ქსელებად (100 მბიტ/წმ-ზე მეტი).

მოდემი

კონცენტრატორი

კომუტატორი

მარშრუტიზატორი

უკაბელო წვდომის წერტილი

მრავალფუნქციური მოწყობილობები

მოდემი (Modem) - ელექტრონული მოწყობილობაა, რომელიც სატელეფონო ხაზებში, ანალოგური სიგნალის მეშვეობით გადასცემს ინფორმაციას კომპიუტერებს შორის.

კონცენტრატორი (Hub) - უზრუნველყოფს ერთ ქსელში რამოდენიმე კომპიუტერის ჩართვას (პორტების რაოდენობის მიხედვით) შემოსულ პაკეტებს უგზავნის ყველა კომპიუტერს, მიუხედავად იმისა, არის თუ არა მისთვის განკუთვნილი. ამის გამო ხდება ქსელში მოძრაობის, იგივე ტრაფიკის (Trafic), გადატვირთვა. ჰაბს შეიძლება ჰქონდეს 6, 12 და მეტი RJ 45 პორტი.

კომუტატორი (Switch) - უზრუნველყოფს ერთ ქსელში რამოდენიმე კომპიუტერის ჩართვას (პორტების რაოდენობის მიხედვით). ჰაბისაგან განსხვავებით სვიჩი მონაცემებს უგზავნის იმ კომპიუტერს, რომლისთვისაცაა განკუთვნილი.

მარშრუტიზატორი (Router) გამოიყენება სხვადასხვა ქსელების ერთმანეთთან დასაკავშირებლად, განსაზღვრავს მარშრუტს დაშორებულ ქსელებში ინფორმაციის გადაცემისას.

უკაბელო წვდომის წერტილი (Wireless Access Point) - გამოიყენება რადიოტალღური სიგნალებით საკომუნიკაციოდ.


მოდემი / როუტერი
WIFI მოწყობილობები
კაბელით მიერთებული მოწყობილობები


CN-C5E CN-C5ECHD


CN-C6 CN-C6CHD


FP-2WHT FP-1WHT


FP-BLANK-WHT SMB-BB1G-WHT


SMB-4WHT-C SMB-1WHT-C SMB-2WHT-C


PP-K12M PP-C5E PP-C6-24C PP-C6-48C


PP-K24 PP-K48

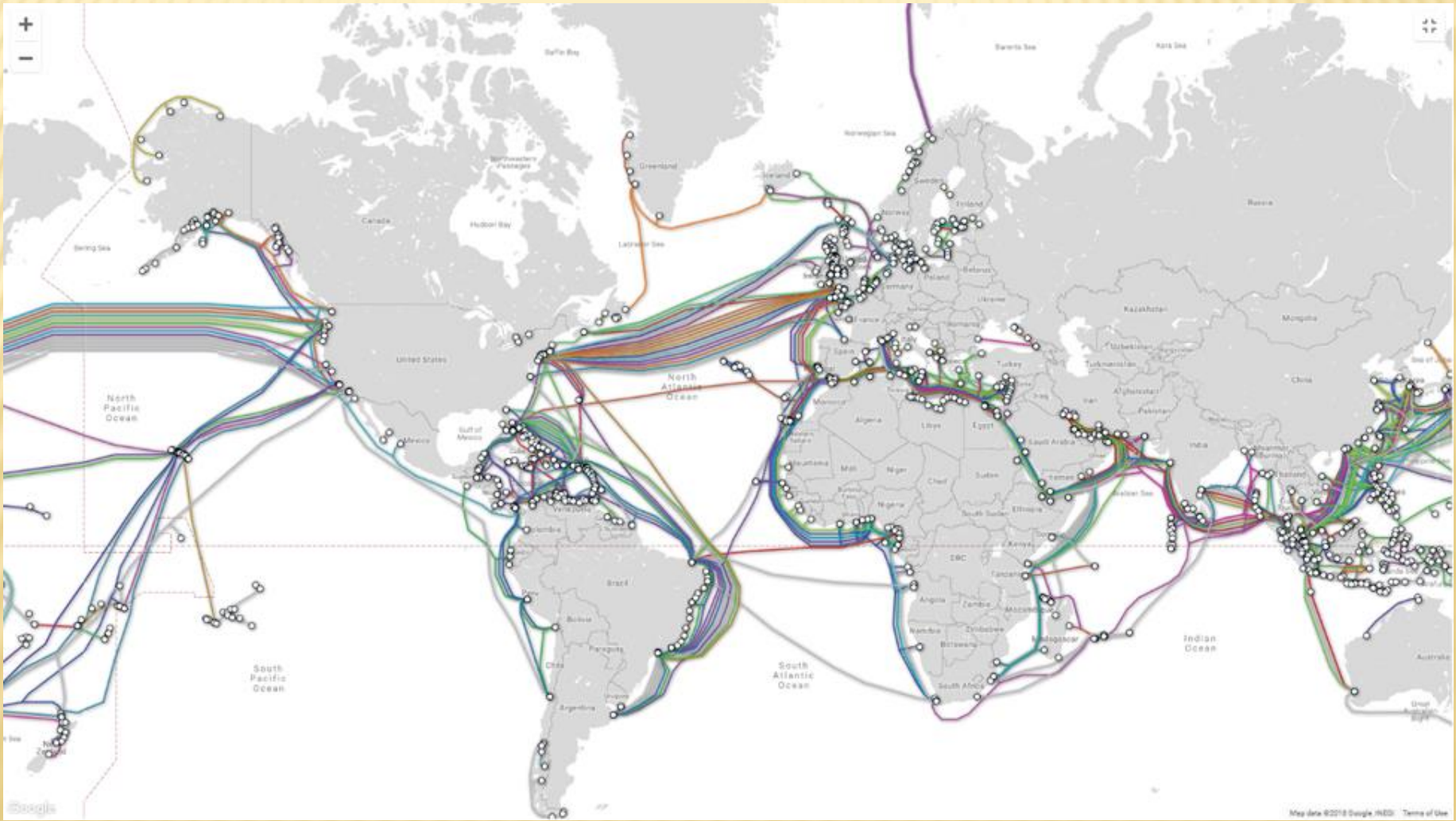

TO-CRIMP-90-RPT TO-CRIMP-RPT


N-10111 N-11111 Standard N-10111 N-11111 Patch

https://www.submarinecablemap.com/

ინტერნეტ კავშირის მხოლოდ 1% ხორციელდება სატელიტით,

დანარჩენი 99% კი წყალქვეშა კაბელებით ოკეანეების ფსკერზე.



Caucasus Cable System

RFS: 2008 November
Cable Length: 1,200 km
Owners: Caucasus Online
URL: http://www.co.ge/en/
Landing Points
Balchik, Bulgaria
Poti, Georgia
12.6 Tbps
http://blackseacable.com/

Diamond Link Global

RFS: 2020 Q1
Cable Length: 1,208 km
Owners: Diamond Link Global
URL: n.a.
Landing Points
Constanta, Romania
Poti, Georgia
129Tbps

Georgia-Russia

RFS: 2000 December
Cable Length: 433 km
Owners: Rostelecom, FOPTNET, DanTelco
URL: http://www.georgia-russia.com
Landing Points
Novorossiysk, Russia
Poti, Georgia
Sochi, Russia

ინტერნეტ-ბრაუზერი (ასევე ვებ ბრაუზერი ან უბრალოდ ბრაუზერი) წარმოადგენს პროგრამას, ტექნიკურად „HTTP კლიენტს“, რომელიც მომხმარებელს საშუალებას აძლევს „HTML დოკუმენტების“ ინფორმაციის ჩვენებას, ვებ-სერვერიდან ან ფაილური სისტემიდან. დღეისთვის მრავალი ინტერნეტ-ბრაუზერი არსებობს, მათ შორის პერსონალური კომპიუტერებისთვის ყველაზე პოპულარულია: **Google Chrome, Microsoft Edge (Internet Explorer), Google Chrome, Opera, Safari, Mozilla Firefox.**

ვებგვერდი - საიტის შემადგენელი ნაწილია. იგი წარმოადგენს ინფორმაციის წყაროს და შეიცავს ჰიპერტექსტებს, რომელთა საშუალებითაც ხდება სხვადასხვა დოკუმენტის მოძიება და კავშირი. ყველაზე ხშირად საიტი დაწერილია HTML ან XHTML ვებ პროგრამირების ენაზე და ხელმისაწვდომია ვებბრაუზერის საშუალებით.

https://www.sportuni.edu.ge

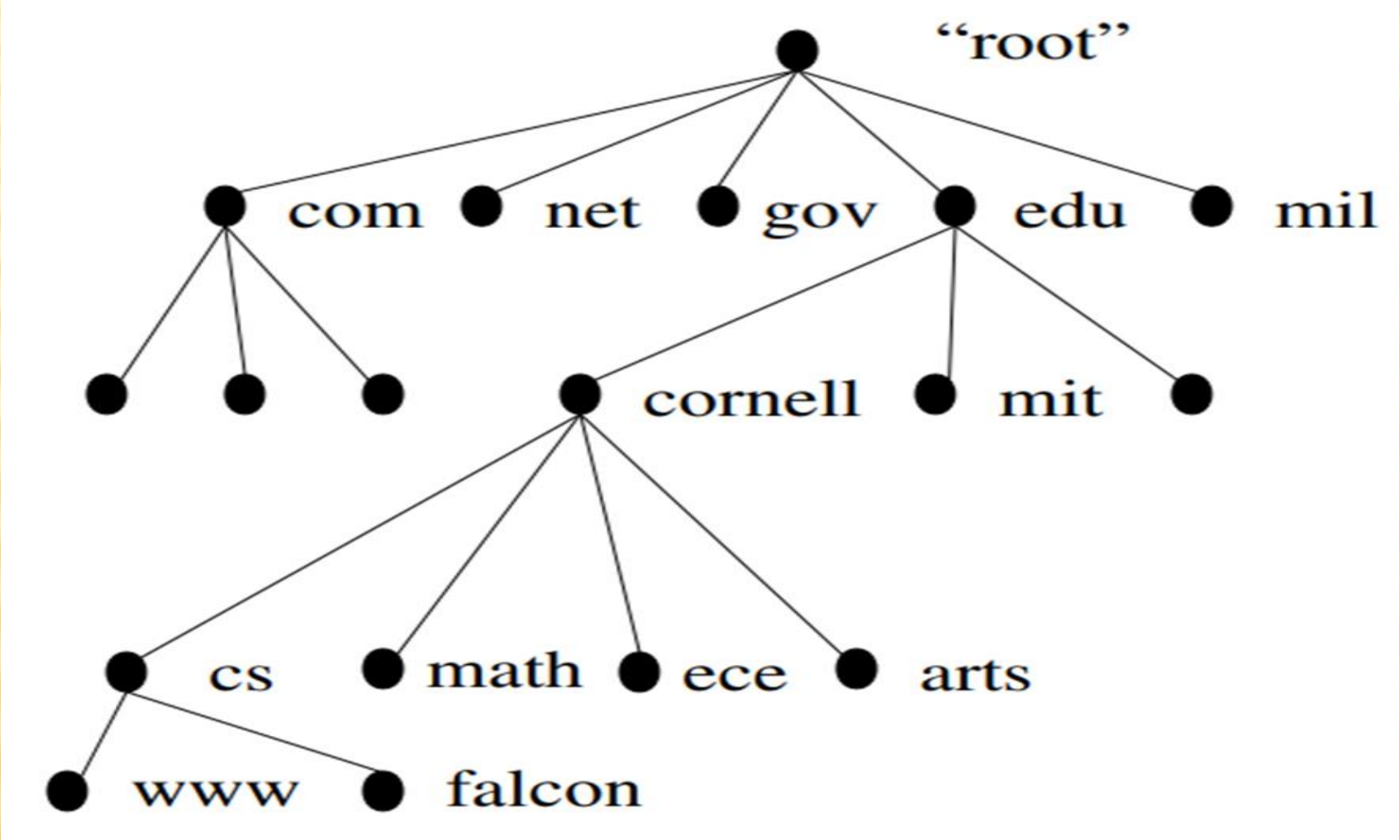
https://www.youtube.com/watch?v=0jRX0xq24AU

https://www.frop.com.au/apples/royal-gala/

- **ge** - საქართველო, **uk** - დიდი ბრიტანეთი და სხვა
- **edu** - საგანმანათლებლო
- **gov** - სამთავრობო ორგანიზაციები
- **mil** - სამხედრო ორგანიზაციები
- **com** - კომერციული ორგანიზაციები
- **org** - არაკომერციული და არასამთავრობო ორგანიზაციები
- **net** - ქსელური კომპანიები
- **HTTP** - ჰიპერტექსტის გადაცემის განაწესი

- **Electronic mail (E- mail** - ელექტრონული ფოსტა
- **Usenet** - ტელეკონფერენციათა სისტემა
- **FTP (File transfer protocol)** - ფაილების შენახვისა და გადაგზავნის სისტემა

Cornell University Website Domain Structure



ვებგვერდზე შესაძლებელია განთავსებული იყოს სხვადასხვა სახის ინფორმაცია: ტექსტი, სურათები, ვიდეოები, მედია ფაილები და ა.შ. ასევე სხვადასხვა სახის სკრიპტები (ჯავასკრიპტი, VB სკრიპტი და ა.შ). როგორც წესი, ვებგვერდზე ასევე განთავსებული სხვა ვებგვერდების მისამართები (ბმულები).

ყველაზე ხშირად ვებგვერდი გვხვდება შემდეგი გაფართოებით **.html** ან **.htm**.

ელექტრონული ფოსტა (e-mail) — კომპიუტერულ ქსელში წერილების მიღებისა და გაგზავნის ტექნოლოგია. წერილების გაგზავნა ხდება **Simple Mail Transfer Protocol**-ის საშუალებით. დღეისათვის, ეს სისტემა ფართოდ გამოიყენება სპამერების მიერ რომელიც თვითნებურად აგზავნინებს არასაჭირო წერილებს, რომელთაც სპამი ეწოდება, თუმცა არსებობს სპეცილური სისტემები, რომელიც ბლოკავს მსგავსი წერილების უმეტესობას.

ელექტრონული ფოსტის შექმნის თარიღად შეიძლება დავასახელოთ **1965** წელი, როდესაც მასაჩუსეტსის ტექნოლოგიური ინსტიტუტის თანამშრომლებმა, ნოელ მორისმა და ტომ ბან ბლეკმა დაწერეს პროგრამა **MAIL**, ოპერაციული სისტემა **CTSS**-ისთვის (**Compatible Time-Sharing System**). იგი მუშაობდა კომპიუტერზე **IBM 7090/7094.**

- ეს სისტემა თანდათან განვითარდა, მრავალმომხმარებლიანი ლოკალური სისტემის განვითარებასთან ერთად. მომხმარებლებს პროგრამა **mail**-ის გამოყენებით შეეძლოთ ერთმანეთისთვის წერილების გაგზავნა.
- შემდეგი ნაბიჯი იყო წერილების გაგზავნა ერთი კომპიუტერიდან-მეორეზე. ამისათვის გამოიყენებოდა კომპიუტერის სახელი და მომხმარებლის სახელი ამ კომპიუტერზე. მისამართი იწერებოდა შემდეგი სახით: **foo!joe** (მომხმარებლის სახელი იყო **joe**, კომპიუტერის კი **foo**). **UUCP** მისამართის გამოყენების შემთხვევაში, მისამართში ემატებოდა წერილის მარშრუტიც, რომელიც ადრესატამდე მისვლამდე რამდენიმე შუალედურ კომპიუტერს გაივლიდა, მაგალითად **gate1!gate2!foo!joe** (ამ წერილის მიმღები იყო **joe**, წერილი გაივლიდა **gate1**, **gate2** კომპიუტერებს და ბოლოს მოხვდებოდა **foo** კომპიუტერში).
- ასეთი მისამართების სუსტი მხარე იყო ის, რომ გამგზავნს უნდა სცოდნოდა სრული მარშრუტი, რომელიც წერილს უნდა გაევლო მიმღებამდე.

გლობალური დომენური სახელების სისტემის (**DNS**) შექმნის შემდეგ ადრესატის მისამართად შესაძლებელი გახდა დომენური სახელის გამოყენება, მაგალითად **user@example.com** - მომხმარებელი **user**, კომპიუტერზე **example.com.**

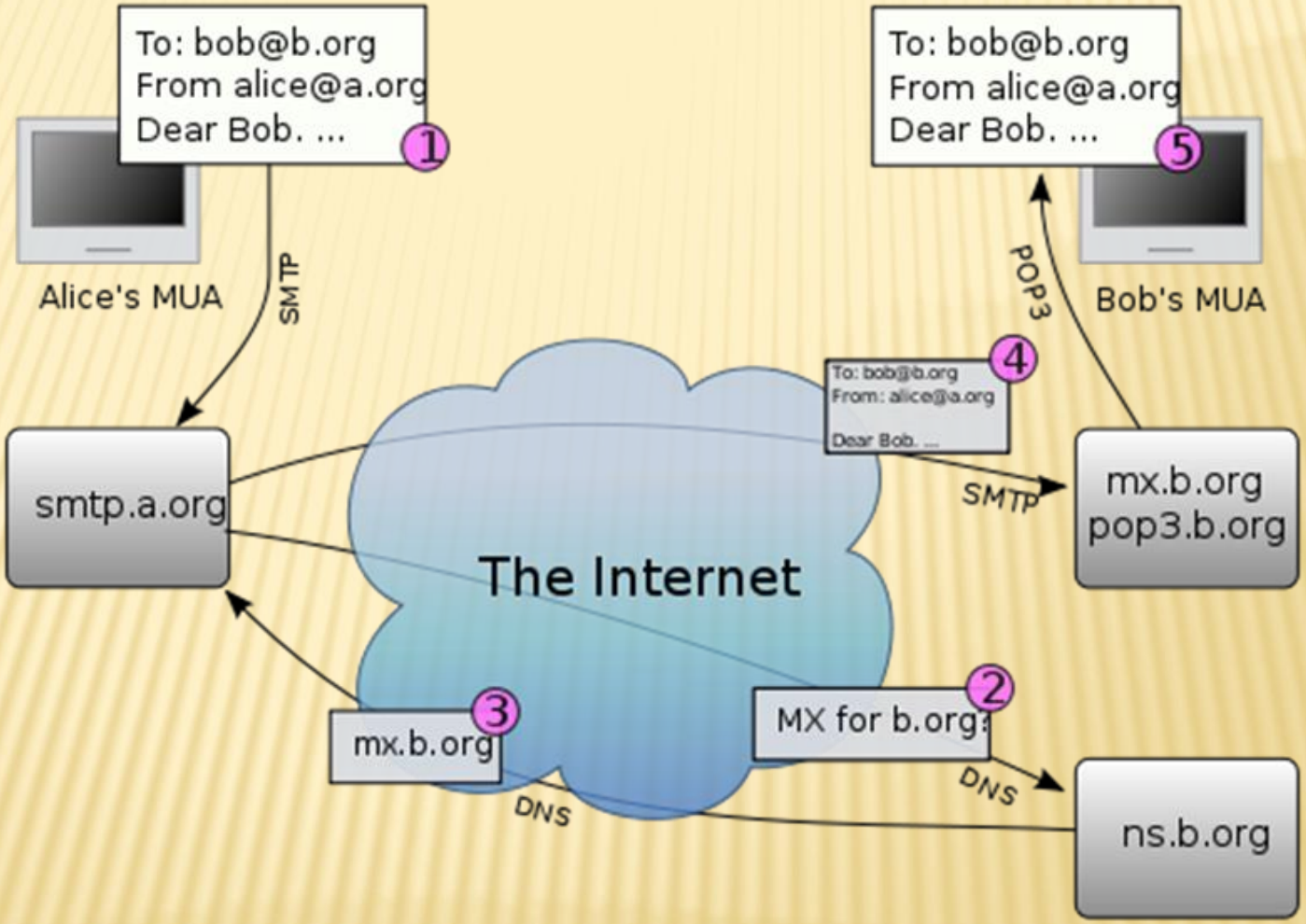
ამან საჭირო გახადა უკვე დანერგილი ცნებების შეცვლა. ფოსტისთვის დაიწყეს გამოყოფილი სერვერების გამოყენება. ახლა, წერილი პირდაპირ აღარ ხვდებოდა ადრესატის კომპიუტერში, არამედ იგი თავსდებოდა სერვერში და მიმღები სერვერიდან იღებდა თავის წერილებს **POP3, IMAP და RCP** პროტოკოლების საშუალებით.

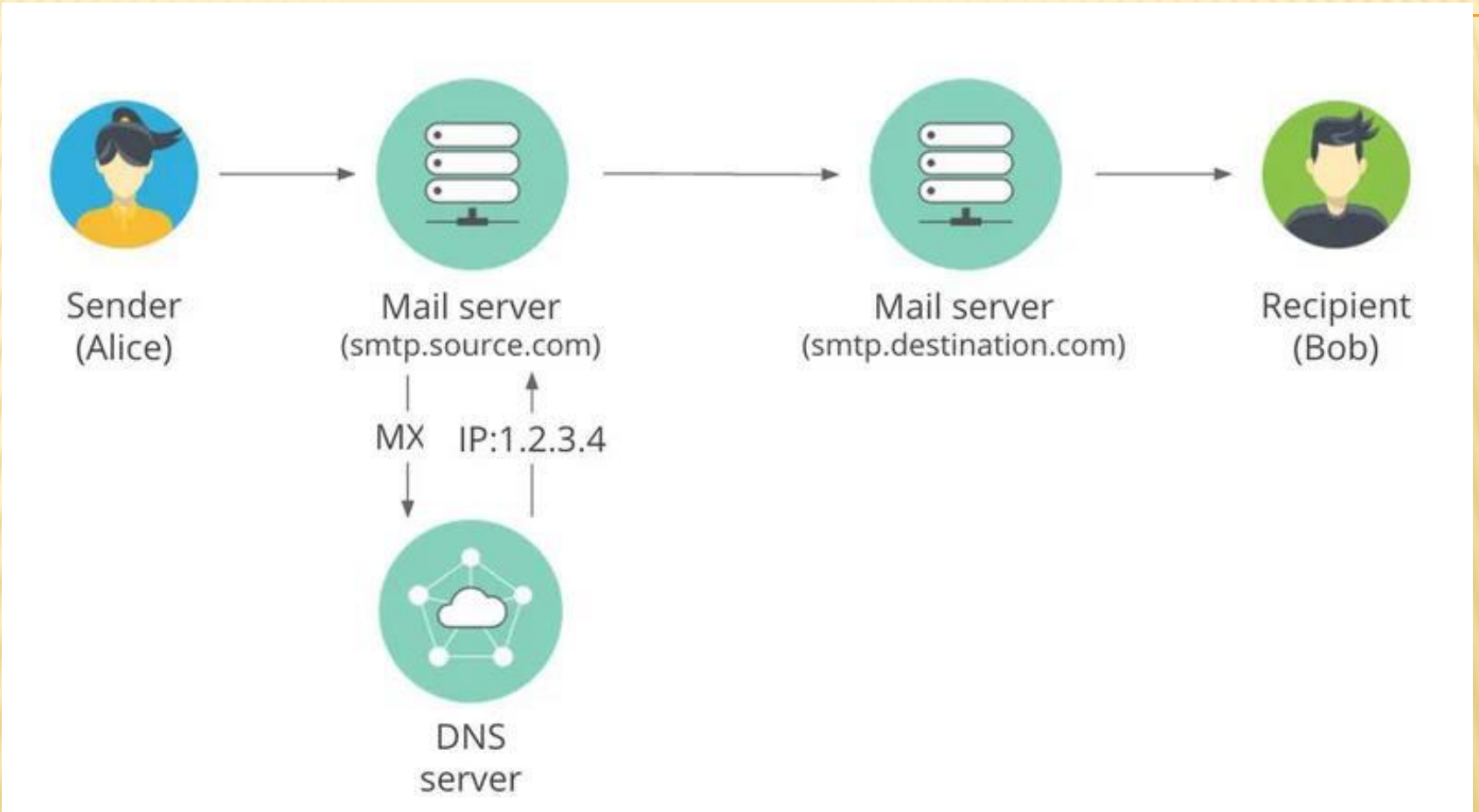
დღეისათვის დომენური სახელი აღარ გამოიყენება კონკრეტული კომპიუტერის მისამართად, იგი მხოლოდ საფოსტო დომენად იქცა და მასზე სხვადასხვა სერვერი შეიძლება იყოს პასუხისმგებელი.

მაგალითი

მოცემულ სურათზე მარტივად არის ნაჩვენები ელექტრონული ფოსტის გაგზავნისა და მიღების პრინციპი, როდესაც **Alice** თავისი ელექტრონული ფოსტის კლიენტი პროგრამის საშუალებით უგზავნის წერილს **Bob**-ს.

- მისი **(Alice)** ელექტრონული ფოსტის კლიენტი პროგრამა აფორმატებს წერილს შესაბამის ელექტრონული ფოსტის ფორმატში და **Simple Mail Transfer** პროტოკოლის **(SMTP)** საშუალებით უგზავნის ამ წერილს ლოკალურ საფოსტო სერვერს, რომელსაც აკონტროლებს მისი ინტერნეტ პროვაიდერი **(ISP)**. ამ შემთხვევაში **smtp.a.org** არის **Alice**-ს ინტერნეტ პროვაიდერის მისამართი.
- საფოსტო სერვერი ეძებს **SMTP** პროტოკოლში მითითებულ ელექტრონული ფოსტის მისამართს, ამ შემთხვევაში **bob@b.org**. @ ნიშნის მარცხენა ნაწილი არის მიმღების მომხმარებლის სახელი, მარჯვენა ნაწილი კი დომენური სახელი. გამგზავნი საფოსტო სერვერი ეძებს ამ მისამართს დომენური სახელების სისტემაში და პოულობს მიმღების სერვერს, რომელიც იღებს წერილს გამგზავნი სერვერიდან.
- **b.org** დომენის **DNS** სერვერი, **ns.b.org**, პასუხობს **MX** ჩანაწერით. ამ შემთხვევაში **mx.b.org** არის **Bob**-ის ინტერნეტ პროვაიდერის სერვერი.
- **smtp.a.org** უგზავნის წერილს **mx.b.org**-ს, **SMTP** პროტოკოლის საშუალებით, რომელიც ხვდება **Bob**-ის საფოსტო ყუთში.
- **Bob** იღებს ამ წერილს **POP3** პროტოკოლის საშუალებით.


To: bob@b.org
From alice@a.org
Dear Bob. ...
1
Alice's MUA
SMTP
smtp.a.org
The Internet
3
mx.b.org
DNS
MX for b.org?
2
DNS
ns.b.org
To: bob@b.org
From: alice@a.org
Dear Bob. ...
4
SMTP
mx.b.org
pop3.b.org
POP3
To: bob@b.org
From alice@a.org
Dear Bob. ...
5
Bob's MUA

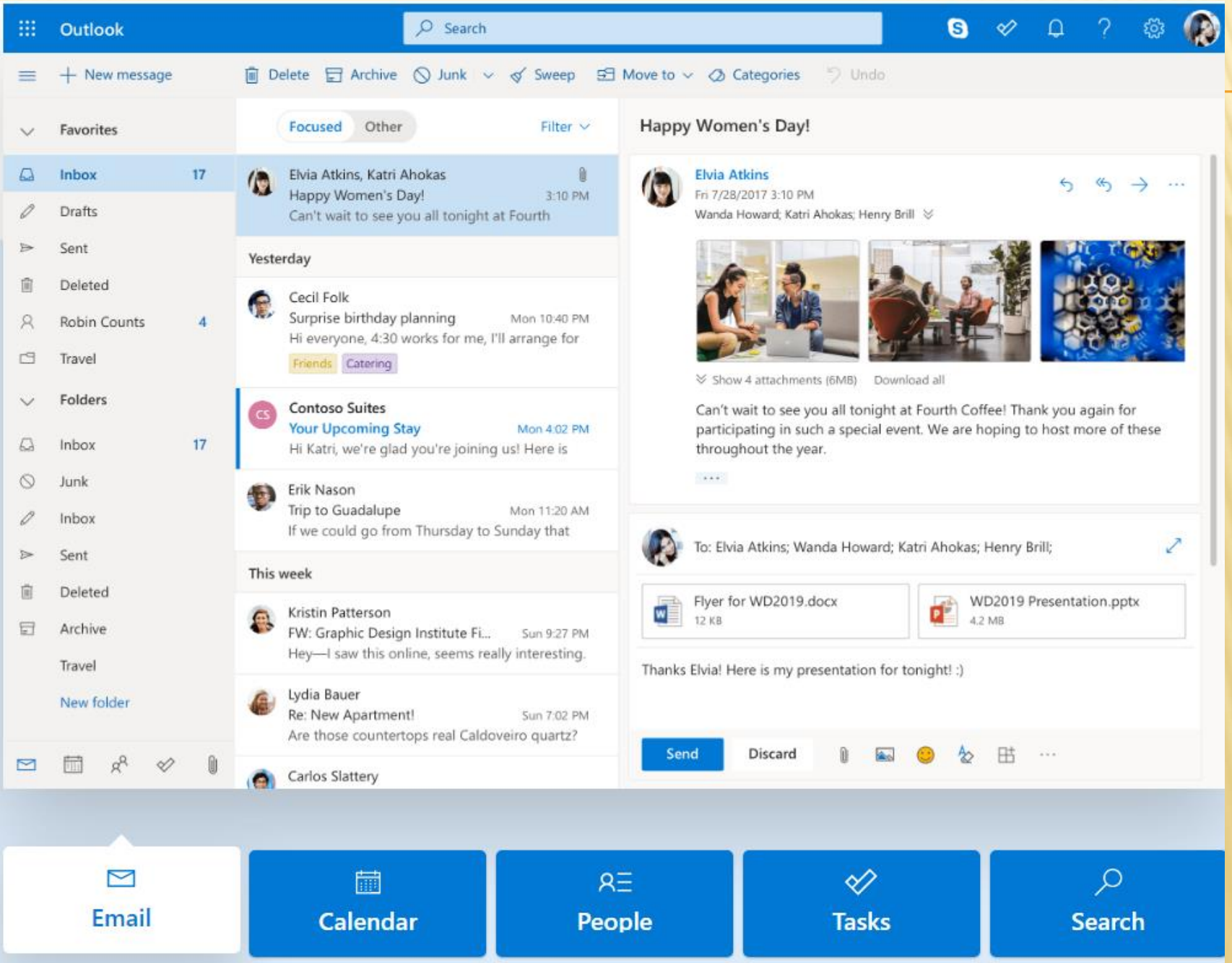


ელექტრონული წერილის გადაგზავნის პროცესი

ცნობილი საფოსტო სერვერები: Gmail Yahoo! Mail Hotmail Mail.Ru

Microsoft Outlook (OS X-ისთვის არის ცალკე სხვა პროგრამა - Microsoft Outlook for Mac, რომელსაც ადრე ერქვა Microsoft Entourage) არის პერსონალური ინფორმაციის მენეჯერი და e-mail კომუნიკაციის პროგრამა. Windows Messaging, Microsoft Mail, and Schedule-ში ის შედიოდა Office 97-დან მოყოლებული დღემდე და შეიცავს e-mail კლიენტს, კალენდარს, ამოცანათა მენეჯერს და მისამართების წიგნს. Mac OS-ზე ვინდოუსმა Outlook-ის შედარებით განსხვავებული ვერსია გამოუშვა 1990 წელს, მასში შეგვეძლო გვესარგებლა Microsoft Exchange Server-ით. Office 2001-ში მან წარმოადგინა ალტერნატიული აპლიკაცია, ოდნავ განსხვავებული ცვლილებებით და ეწოდა Microsoft Entourage. Office 2011-ში ეს ყველაფერი ჩაშენებულია

https://outlook.live.com/owa/



ყველაფერი კომპიუტერული ვირუსების შესახებ

შეერთებული შტატების კონტროლის პალატის მასალებში განხილულია კიბერსაფრთხეების სახეობები. კერძოდ:

1. მონაცემთა მთლიანობა - კიბერშეტევის დროს შეიძლება გამოყენებული იყოს ჰაკერული მეთოდები, რომლის მიზანია მონაცემთა მთლიანობის განადგურება ან მათი დამახინჯება და ცვლილებების შეტანა;
2. დაშვება - სისტემაზე განხორციელებული კიბერშეტევის შედეგად სისტემის ლეგიტიმურ მომხმარებებლს ექმნება ისეთი პირობები, რომ მომხმარებელს არ შეუძლია სისტემაში შესვლა ან ასეთი დაშვება არის გართულებული;
3. კონფიდენციალობა - კიბერშეტევის მიზანი შეიძლება იყოს კონფიდენციალური ინფორმაციის წყაროები და ეს ძირითადად ხორციელდება შემდგომში დანაშაულის ჩადენის მიზნით.

მავნე პროგრამა არის ნებისმიერი პროგრამა, რომელიც განკუთვნილია კომპიუტერის რესურსებზე ან ინფორმაციაზე არასანქციერებული წვდომის მოსაპოვებლად. ნებისმიერი პროგრამა, რომელიც მფლობელის გაცნობიერებული ნებართვის გარეშე ახორციელებს კომპიუტერში ცვლილებას და მოაქვს პირდაპირი ან არაპირდაპირი ზიანი შეიძლება ჩაითვალოს მავნე პროგრამად. მავნე ფუნქციების მქონე პროგრამები შეიძლება დაჯგუფდეს ვირუსებად, ტროას ცხენებად, ჭიებად, რეკლამების გამომტან, გამომძალველ, თაღლითურ და ჯაშუშურ პროგრამებად.

კომპიუტერული ვირუსი წარმოადგენს კომპიუტერულ პროგრამას, რომელიც სხვა პროგრამებისგან იმით განსხვავდება, რომ შეუძლია გამრავლდეს (ამებას მსგავსად) და დააზიანოს კომპიუტერის პროგრამული (ზოგჯერ აპარატურულიც) უზრუნველყოფა.

კითხვები (FAQ):

1. როგორ ვრცელდებიან ვირუსები?

პასუხი: ვირუსები ვრცელდებიან ინტერნეტით. მაგალითად ვებსაიტებზე შესვლისას, მესენჯერების გამოყენებისას, რაიმე პროგრამის გადმოწერისას, ელფოსტის მიღებისას და ა.შ აგრეთვე ინფორმაციის მატარებელი მოწყობილობებით : ვინჩესტერი, მობილური, ფლეშ დრაივი, ფლოპი დისკეტა და CD/DVD ...

2. რა ტიპის ვირუსები არსებობს ?

პასუხი: არსებობს ძალიან ბევრი სახეობის ვირუსი, რომელთა ჩამოთვლაც შორს წაგვიყვანს.

შემოვიფარგლოთ მაგალითებით. ვირუსები, რომლებიც ვრცელდებიან მესენჯერების საშუალებით, ელფოსტის ვირუსები, ტროიანული ვირუსები, რომლებიც თქვენს კომპიუტერში არსებულ ინფორმაციას თავის ავტორს უგზავნიან, ეს შეიძლება იყოს ელფოსტის პაროლები, ბანკის ანგარიშები, თქვენი ინტიმური მიმოწერა და ა.შ.

კომპიუტერული ვირუსი რამოდენიმე კატეგორიად იყოფა. მათგან ყველაზე პოპულარულები კი არიან:

ჩვეულებრივი ვირუსი – კომპიუტერის მუშაობის მოდიფიკაცია, მრავლდება თავისით, სჭრიდება პროგრამა, რომელზეც მიმაგრდება.

Worm (ვორმი, ჭიაყელა) – ჩვეულებრივი ვირუსისაგან იმით განსხვავდება, რომ არ სჭირდება ჰოსტ პროგრამა.

Roorkit – მალავს ზიანის მომტანი პროგრამის პროცესს, პრივილეგირებული წვდომა აქვს კომპიუტერთან.

Trojan Horse (ტროას ცხენი) – პროგრამა, რომელიც ირწმუნება, რომ გააკეთებს ერთს და სინამდვილეში აკეთებს მეორეს. ქმნის უკანა კარებს, რომელიც ჰაკერს საშუალებას აძლევს წვდომა ჰქონდეს მსხვერპლის კომპიუტერის სისტემასთან.

Spyware (შპიონი) – პროგრამა, რომელიც დაინსტალირების შემდეგ მალულად აგროვებს ინფორმაციას მომხმარებლის კომპიუტერიდან.

Adware (სარეკლამო) – პროგრამული პაკეტი, რომელიც არალეგალურ რეკლამებს აწარმოებს.

Spam (სპამი) - წარმოიდგინეთ შემდეგი ფაქტი: მსოფლიოში წამში სამი მილიონი ელექტრონული წერილი იგზავნება და აქედან 91% სპამია. ამ კატეგორიის ზოგიერთი წერილი შეიცავს ვირუსებს და სხვა მავნე პროგრამებს.

Phishing (პიშინგი) - ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა. პიშინგის საშუალებით ხდება ისეთი ინფორმაციის მოპოვება როგორიცაა მომხმარებლის სახელი, პაროლი, საბანკო ბარათის ან საკრედიტო ანგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია.

Malicious Botnet (მავნე ბოტნეტი) - კომპიუტერების ჯგუფი, რომელიც იმართება ერთი ან რამდენიმე ადამიანისგან, რომლებიც აწყობენ DDoS შეტევებს.

გამომძალველი პროგრამები - ასეთი პროგრამის არსი იმაში მდებარეობს, რომ კომპიუტერში მოხვედრის შემდეგ ის თანმიმდევრობით მიყვება ყველა ფაილს, შიფრავს მას და დაშიფრვის დასრულების შემდეგ გამოდის შეტყობინება, რომ ინფორმაციის აღსადგენად საჭიროა კონკრეტული თანხა გადარიცხული იყოს მითითებულ ანგარიშზე .

10 ყველაზე სახიფათო კომპიუტერული ვირუსი

(http://www.geobazari.com/2012/07/25/computer-viruses/):

1. Storm Worm
2. Leap-A/Oompa-A
3. Sasser და Netsky
4. MyDoom
5. SQL Slammer/Sapphire
6. Nimda
7. Code Red და Code Red II
8. Klez Virus
9. ILOVEYOU
10. Melissa

3. რა შეიძლება გახდეს ვირუსის ,,აკიდების '' მიზეზი?

პასუხი:

1. დაკრეკილი ვინდოუსი.
2. დაკრეკილი პროგრამული უზრუნველყოფა.
3. პორნო კონტენტის შემცველი საიტების თვალიერება.
4. ვარეზები, კრეკების და სერიულების საიტები.
5. სისტემის განახლებების გათიშვა.
6. მოძველებული პროგრამული უზრუნველყოფა.
7. ანტივირუსის და ბრანდმაუერის უქონლობა კომპიუტერში.
8. სხვისი მოტანილი ინფორმაციის შემცველი მოწყობილობის მიერთება.
9. ოპერაციული სისტემის არასწორი კონფიგურაცია.
10. ხვრელები პროგრამულ და ზოგჯერ აპარატურულ უზრუნველყოფაში.

და ა.შ.

4. როგორ გავიგო რომ ვირუსი მყავს?

პასუხი: თუ სისტემა ჭედავს, თუ ქსელში ზედმეტი ტრაფიკი გადის და ახლობლები გეუბნებიან რომ თქვენი ელფოსტით უცნაურ წერილებს იღებენ, ესეიგი ვირუსი გყავთ.
თუმცა ამის გაგება ანტივირუსითაც შეიძლება, თუ რა თქმა უნდა დაინსტალირებული გაქვთ კომპიუტერში.

5. რა არის ანტივირუსი?

პასუხი: ანტივირუსი წარმოდგენს კომპიუტერულ პროგრამას, რომლის ძირითადი ფუნქციაა ვირუსების პოვნა, აღმოჩენა და მოსპობა.

6. როგორ პოულობენ ანტივირუსები ვირუსებს?

პასუხი: ძირითადად 2 მეთოდით.

ა) ანტივირუსი ასკანერებს კომპიუტერში არსებულ ფაილებს საკუთარ ბაზებში არსებული მონაცემების მიხედვით.

ბ) იყენებს ინტელექტუალურ (ევრისტიკულ) მეთოდს, ამ დროს შეიძლება ისეთი ვირუსების აღმოჩენა, რომელთა სიგნატურები (ვირუსების მონაცემები) მის ბაზაში ჯერ არაა.

7. ვინ აწარმოებს ანტივირუსებს და რომელია ყველაზე კარგი?

პასუხი: არსებობს ბევრი კომპანია, რომელით ამ საქმიანობას ეწევა,მაგალითად

ESET, LLC http://www.eset.com/

ALWIL Software http://www.avast.com/

Avira http://www.free-av.com/

Kaspersky Lab http://www.kaspersky.com/

რაც შეეხება მათ შორის საუკეთესოს, ეს უკვე სხვა საკითხია. უნდა გაითვალისწინოთ ფაქტი, ვერცერთი ანტივირუსი ვერ დაიცავს თქვენს კომპიუტერს 100%-ით.

8. რა უნდა ვქნათ თუ კომპიუტერი დავირუსდა?

პასუხი: ა) ვაყენებთ ანტივირუსს (თუ აქამდე არ გვქონდა) და ვასკანერებთ მისი საშუალებით.

ბ) გამორთეთ კომპიუტერი და დაელოდეთ კომპეტენტურ ახლობელს. როცა კომპიუტერი გამორთულია, ვირუსი არ მოქმედებს.

გ) ეძახით ვირუსების მოშორების სპეციალისტს და ფულს იხდით.

დ) თავად აშორებთ ვირუსს საკუთარი ცოდნით. ამ შემთხვევაშიც მოგიწევთ სხვადასხვა ანტივირუსული უტილიტების გამოყენება და პარტიშენების ანალიზი, მაგრამ ფულის დახარჯვას გადარჩებით.

8. კონკრეტულად რისი გაკეთება შეუძლია ვირუსს და რა სარგებელი აქვთ ვირუსების ავტორებს?

პასუხი: არსებობს ვირუსების მრავალი ტიპი, განსხვავებული როგორც აგებულებით, ისე ქცევით. ვირუსს შეუძლია

ა) მოიპაროს თქვენი კონფიდენციალური მონაცემები, ელფოსტის, ვებსაიტების და მესენჯერების პაროლები. საკრედიტო ბართების კოდები და ბანკის ანგარიშები, პროგრამების ლიცენზიის კოდები.

ბ) დაშიფროს ინფორმაციის შემცველი მოწყობილობები AES-256 და უფრო მაღალი ალგორითმით, რის შედეგადაც თქვენს მონაცემებს სამუდამოდ უნდა გამოემშვიდობოთ, თუ რა თქმა უნდა ვირუსის ავტორს გარკვეული თანხა არ გადაურიცხეთ.

გ) წაშალოს თქვენს კომპიუტერში არსებული ყველა ფაილი, ისე რომ მათი აღდგენა ძალიან გაგიჭირდება.

დ) დაავირუსოს პროგრამული ფაილები თავისი მავნე კოდის ინექციით. ამ დროს ერთადერთი გამოსავალი არსებობს: რაც არ უნდა ძვირფასი პროგრამები გქონდეთ, ყველა მათგანი უნდა წაიშალოს.

ე) გამოიყენოს თქვენი კომპიუტერი როგორც ბოტი, სამთავრობო და სხვა ორგანიზაციების სერვერებზე შეტევის მოსაწყობად, ამ დროს ფიქსირდება შემტევის (ანუ თქვენი) IP მისამართი. ზემოთაღნიშნული ქმედება კი საქართველოს სისხლის სამართლის საპროცესო კოდექსით აკრძალულია, შესაბამისად გვარიანი თანხა გექნებათ გადასახდელი.

ვ) გამოიყენოს თქვენი კომპიუტერი მასობრივი კომპიუტერული გზავნილების (სპამი) დასაგზავნად, რაც ასევე არალეგალურია და საერთაშორისო კანონებით დასჯადია.

ზ) დააზიანოს კომპიუტერის პროგრამული უზრუნველყოფა, კერძოდ ოპერაციული სისტემა. ზოგჯერ ხდება ისეც რომ, ოპერაციულ სისტემის ზედმეტი დატვირთვის და არასწორი ბრძანებების გამო იტვირთება პროცესორი და სხვა ნაწილებიც, რის გამოც აპარატურა მწყობრიდან გამოდის.

თ) გამოიყენოს თქვენი კომპიუტერი საკუთარი თავის გასამრავლებლად. აქვე შევეხოთ სარგებელს. ვირუსების ავტორების მთავარი მიზანია კომერციული მოგება ვირუსების წერით ანუ იშოვონ რაც შეიძლება მეტი ფული. თუმცა ეს არა ერთადერთი მიზეზი. შეიძლება ავტორი ამას გაბოროტების გამო აკეთებს, ან უბრალოდ ცნობისმოყვარეობა აწუხებს.

10. რას მირჩევდით ვირუსებისგან დასაცავად?

პასუხი:

ა) შეიძინეთ ლიცენზირებული პროგრამული უზრუნველყოფა.

ბ) ნუ დასვამთ უცხო ხალხს საკუთარ კომპიუტერზე.

გ) ნუ გახსნით საეჭვო წერილებს, რომლებიც თქვენს ელფოსტაზე მოდის.

დ) ნუ შეხვალთ საეჭვო რეპუტაციის საიტებზე.

ე) ყველა ფაილი რასაც გადმოიწერთ, ანტივირუსით დაასკანერეთ(თუ გაქვთ რა თქმა უნდა).

ვ) ნუ დაგეზარებათ ვინდოუსის გადაყენება.

ზ) თუ თქვენი თავის იმედი არ გაქვთ მიმართეთ კომპეტენტურ პირს და ნუ დაგენანებათ ფული ამ მომსახურებაში, თუ ის კეთილსინდისერად სრულდება.

თ) ნუ ენდობით ინტერნეტში ამა თუ იმ ახალი პროგრამული პროდუქტის რეკლამას. ნუ გადმოწერთ ნურაფერს სანამ არ დაეკითხებით ვინმე კომპეტენტურს ან არ დაასკანერებთ ანტივირუსით.

ი) გაანახლეთ ოპერაციული სისტემა და პროგრამული უზრუნველყოფა და ა.შ.

11. როგორ დავადგინოთ პიროვნების კომპეტენტურობა და როგორ დავეხმაროთ მას ?

პასუხი: გამოძახებისას მოუყევით არსებული სიტუაციის შესახებ, თქვენი ეჭვები და ვარაუდები, რათა აღმოჩენილი იქნას ვირუსის გავრცელების წყარო. რაც შეეხება კომპეტენტურობას, აუცილებლად დაუსვით კითხვები ვირუსების, მათი გავრცელების და მოშორების გზების შესახებ. ჰკითხეთ როგორ დაიცვათ თქვენი კომპიუტერი მათგან და ა.შ.

აუცილებლად დააკვირდით მის მოქმედებებს და გადაამოწმეთ პასუხი ინტერნეტში მისი წასვლის შემდეგ.

თუ მან კითხვებზე ან არ გიპასუხათ ან არასწორად გიპასუხათ, შემდეგში ნუღარ მიმართავთ და ნუ გადაყრით თანხას ტყუილად.

12. გამიგია რომ ვინდოუსის გადაყენების მერე ვირუსები ქრება, მართალია ეს თუ ტყუილი?

პასუხი: ტყუილია, რადგან არსებობს ვირუსები, რომლებიც იყენებენ დამატებით პარტიშენებს, რომლებიც გადაყენების შემდეგადაც დავირუსებული რჩება.

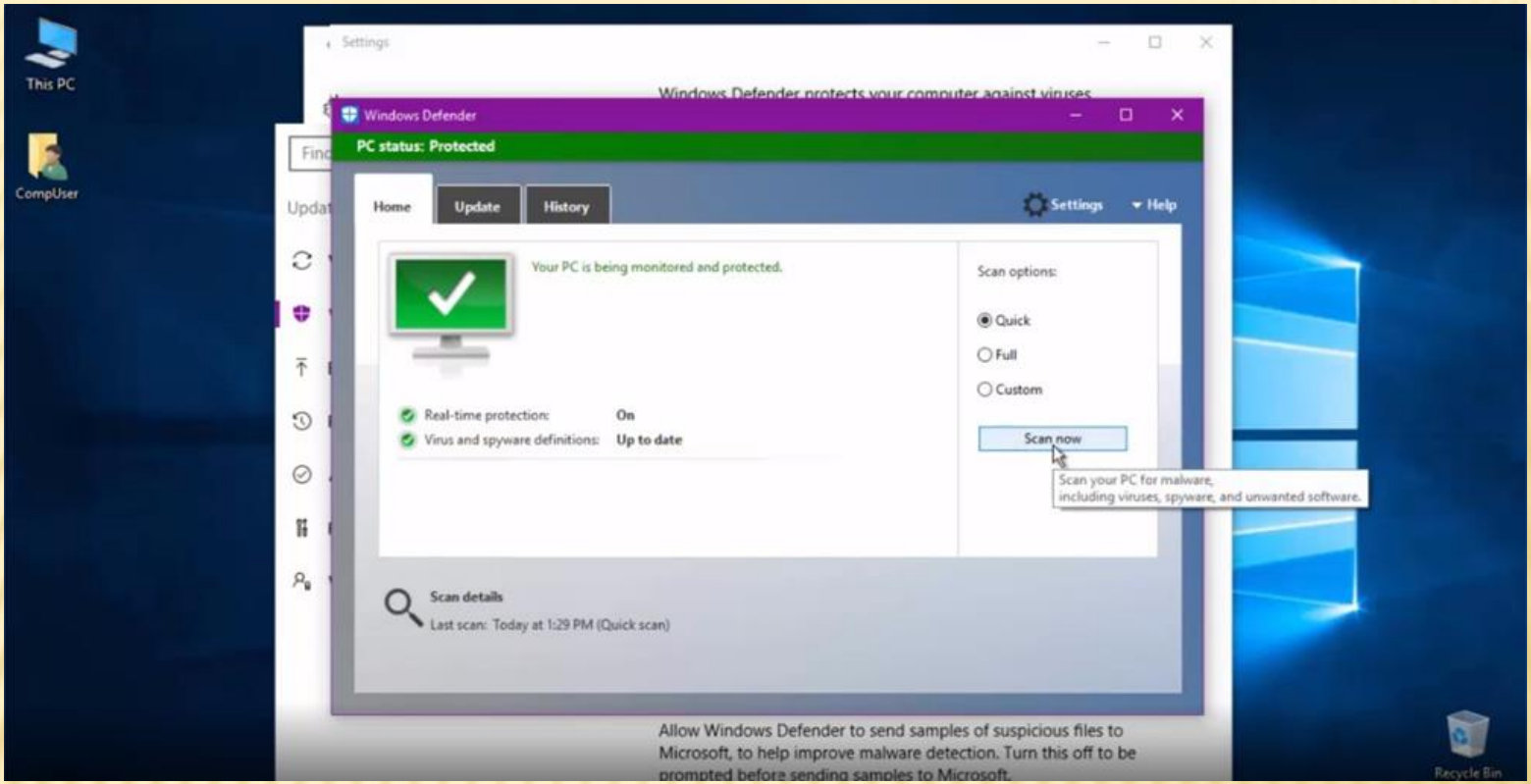
თუ თქვენ ამ პარტიშენებზე შეხვალთ, ისევ დავირუსდებით, ამიტომაც სანამ ვინდოუსს გადააყენებინებთ, ჯერ ყველა პარტიშენი გაწმინდეთ.

რაც შეეხება ვინდოუსის გადაყენებას ვირუსებისგან გაწმენდის შემდეგ, ეს აუცილებელია. ეს ტყუილი კი ზარმაცი ინსტალატორების მოგონილია, რომლებთაც ეზარებათ ვირუსების მოძებნა და მხოლოდ გადაყენებით კმაყოფილდებიან.

13. კომპიუტერი არ ჭედავს, ყველაფერი ნორმალურად მუშაობს, გამოდის ვირუსი არ მყავს?

პასუხი: რათქმაუნდა ეს კარგია, მაგრამ სულაც არ ნიშნავს იმას, რომ ვირუსი არ გყავთ.

სავარუდოდ თქვენ გყავთ ტროიანული ტიპის ვირუსი, რომელიც მხოლოდ მონაცემების ჩაწერა/გაგზავნით შემოიფარგლება და კომპიუტერს ძირითად შემთხვევებში არ აზიანებს. თუმცა შესაძლებელია ვირუსი არ გყავდეთ.



Windows 10-ის ოპერაციულ სისტემაში ვირუსებისაგან დასაცავად არსებობს ჩაშენებული ანტივირუსი სახელით Windows Defender, რომლის მოძებნაც შესაძლებელია პარამეტრებში (Settings) და მერე „განახლებებში და უსაფრთხოებაში“ (Update & Sequrity). ანტივირუსის ჩართვა, გამორთვა ხდება On/Off გადამრთველით სექციიდან Real-time protection. ანტივირუსის ფანჯრის გახსნა ხდება ღილაკით Open Windows Defender.

კომპიუტერის სრული დასკანირებისათვის უნდა მოვნიშნოთ ოპცია Full და ასევე დავაჭიროთ ღილაკს Scan now. შემოწმებამ შეიძლება წაიღოს დიდი დრო და საბოლოოდ იქნება გამოტანილი შეტყობინება მოხდა თუ არა ვირუსის აღმოჩენა და მისი ავტომატურად წაშლა.

იმ შემთხვევაში თუ კომპიუტერის გასუფთავება ვირუსებისაგან ვერ ხერხდება სპეციფიკური მიზეზების გამო, უნდა გამოვიყენოთ ფუნქცია Scan Offline - მოხდება კომპიუტერის გადატვირთვა და კომპიუტერის შემოწმება ოპერაციული სისტემის გაშვებამდე. ამ შემთხვევაში იზრდება ვირუსის აღმოჩენის ალბათობა.

უნდა გავითვალისწინოთ, რომ Windows Defender ავტომატურად წყვეტს მუშაობას, თუ კომპიუტერში გაშვებულია სხვა ანტივირუსული პროგრამა.