ប្រព័ន្ធសុវត្ថិភាពបណ្តាញកុំព្យូទ័រ

១. សេចក្តីផ្តើម

នៅទូទាំងពិភពលោក មនុស្សបានប្រើប្រាស់ប្រព័ន្ធបណ្តាញកុំព្យូទ័រដើម្បីផ្លាស់ប្តូរព័ត៌មានគ្នាទៅវិញទៅមក។ ពួកគេទិញផលិតផល និង ចាយលុយដែលទុកក្នុងធនាគារតាមរយៈអិនធិណេត។ យើងបានទុកចិត្ត លើប្រព័ន្ធបណ្តាញកុំព្យូទ័រដែលធានា និងការពារទ្រព្យសម្បត្តិ ព្រមទាំងព័ត៌មានរបស់បុគ្គល។

ប្រព័ន្ធបណ្តាញសុវត្ថិភាពកុំព្យូទ័រ គឺជាការរួមចំណែករបស់មនុស្សម្នាក់ៗ ដែលត្រូវបានយល់ព្រមក្នុងការភ្ជាប់ទៅបណ្តាញ។

២. ការលួចចូលទៅក្នុងប្រព័ន្ធបណ្តាញសុវត្ថិភាពកុំព្យូទ័រ

២.ក. ហានិយភ័យនៃការលុកលុយចូលប្រព័ន្ធ

មិនថាតាមរយៈការប្រើខ្សែ ឬមិនប្រើខ្សែ ប្រព័ន្ធបណ្តាញកុំព្យូទ័រមានការរីកចំរើនយ៉ាងរហ័សក្នុងសកម្មភាពរៀងរាល់ថ្ងៃ។ ចំពោះបុគ្គល និងស្ថាប័ននានាគឺពឹងផ្អែកទៅលើប្រព័ន្ធបណ្តាញកុំព្យូទ័ររបស់ពួកគេសំរាប់ការងារជាច្រើនដូចជា: សារអេឡិចត្រូនិក ផ្ទែកគណនី រចនាសម្ព័នស្ថាប័ន និងការគ្រប់គ្រងទិន្នន័យផ្សេងៗ។ ការលុកចូលពីពួកខូច អាចធ្វើអោយបាត់បង់នូវប្រាក់ និង ខាតបង់ពេលវេលាការងារ តាមរយៈការលួច កែប្រែ ឬបំផ្លាញទិន្នន័យសំខាន់ៗ។

អ្នកឈ្លានពានអាចចូលទៅកាន់ប្រព័ន្ធបានតាមរយៈកម្មវិធីកុំព្យូទ័រ ឧបករណ៍វាយលុក ឬតាមវិធីសើបសូ ដូចជា: ទាយឈ្មោះអ្នកប្រើ និង លេខកូដ។ ពួកលុកលុយទាំងនោះត្រូវបានគេហៅថាចោរកុំព្យូទ័រ។

គោលបំណងរបស់ចោរដែលព្យាយាមចូលក្នុងប្រព័ន្ធគឺ:

- លួចព័ត៌មាន និង ទិន្នន័យ

លុកលុយចូលកុំព្យូទ័រដើម្បីយកទិន្នន័យ ឬព័ត៌មានអាថិកំបាំង។ ទិន្នន័យទាំងនោះអាចត្រូវបានយកទៅលក់សំរាប់គោលបំណងផ្សេងៗ។ ឧទាហរណ៍: លួចទិន្នន័យកម្មសិទ្ធិរបស់ស្ថាប័ន ដូចជា: ទិន្នន័យស្រាវជ្រាវ និងព័ត៌មានអភិវឌ្ឍន៍។

- លួចទ្រព្យសម្បត្តិ

ជាការលួចព័ត៌មានបុគ្គលក្នុងគោលបំណងលួចលួចទ្រព្យសម្បត្តិរបស់នរណាម្នាក់។ ចោរប្រើព័ត៌មានទាំងនេះដើម្បីទទួលបានឯកសារស្របច្បាប់ក្នុងការលួចលុយជាក្រឌីត និង ទិញផលិតផលតាមលំហ។ ចោរប្រភេទនេះកំពុងបង្កើនអោយមានបញ្ហាក្នុងសង្គម ដែលបាត់បង់ប្រាក់អស់រាប់លានកោតដុល្លា។

- កែប្រែ ឬ បំផ្លាញទិន្នន័យ

ជាការលុកលុយចូលប្រព័ន្ធដើម្បីបំផ្លាញ ឬកែប្រែ។ ឧទាហរណ៍នៃការបំផ្លាញទិន្នន័យ: ការបញ្ចូលមេរោគដែលរបំផ្លាញទិន្នន័យក្នុងឯកសារ។ ឧទាហរណ៍នៃការកែប្រែ: លុកលុយចូលកែព័ត៌មានដូចជាតម្លៃផលិតផល។

- ឆាវៅទៅលើសេវាកម្មផ្សេងៗ

ជាការចូលកែប្រែ ឬធ្វើអោយរញ្ជួយញ្ជែប្រព័ន្ធដំណើរការ និងសេវាកម្មផ្សេងៗ។

២.ខ. ប្រភពនៃការលុកលុយចូលប្រព័ន្ធ

ការវាយប្រហារប្រពន័ន្ធសុវត្ថិភាពមានប្រភពមកពីអ្នកនៅខាងក្នុង និងពីអ្នកនៅខាងក្រៅ:

ពីអ្នកនៅខាងក្រៅ:

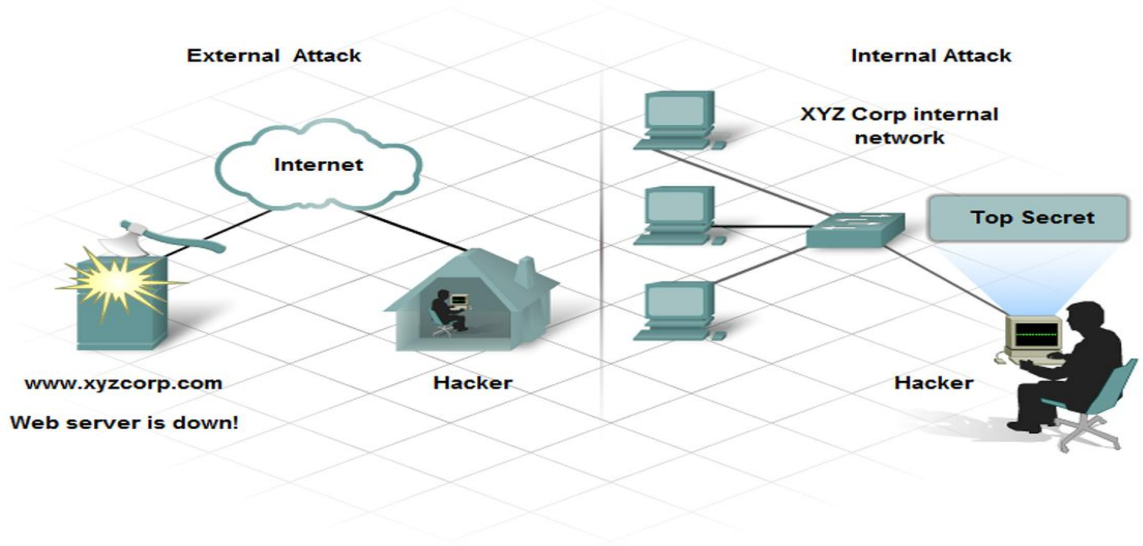
ការវាយលុកពីខាងក្រៅគឺចេញពីអ្នកធ្វើការផ្ទាល់ខ្លួន ដែលមិនមែននៅស្ថាប័នស្របច្បាប់ណាមួយ។

ពួកគេមិនមានសិទ្ធិក្នុងការចូលទៅកាន់ប្រព័ន្ធបណ្តាញកុំព្យូទ័រនោះទេ។ ពួកលុកលុយទាំងនោះធ្វើការតាមមធ្យោបាយរបស់ពួកគេដើម្បីចូលក្នុងប្រព័ន្ធតាមរយ:អិនធិណេត ប្រព័ន្ធភ្ជាប់បណ្តាញគ្មានខ្សែ ឬប្រព័ន្ធទូរស័ព្ទ។

ពីអ្នកនៅខាងក្នុង

ការលុកលុយពីខាងក្នុងកើតឡើងនៅពេលនរណាម្នាក់មានសិទ្ធិក្នុងការចូលទៅកាន់ប្រព័ន្ធតាមរយ: គណនីប្រើប្រាស់ ឬឧបករណ៍ផ្សេងៗដែលអាចចូលប្រព័ន្ធកុំព្យូទ័របាន។ អ្នកនៅខាងក្នុងបានដឹងអំពីរចនាសម្ព័ន និង មនុស្សនៅទីនោះ។ ជាធម្មតាពួកគេដឹងពីព័ត៌មានមានតម្លៃ និងរបៀបនៃការទាញយក។

ទោះបីជាយ៉ាងណា ការលុយទាំងនោះមិនសុទ្ធតែអ្នកនៅខាងក្នុងនោះទេ។ ករណីខ្លះ ការលុកចូលនេះអាចមកពីបុគ្គលិកស្មោះត្រង់ ដែលបានយកមេរោគ ឬកម្មវិធីហែកចូលប្រព័ន្ធសុវត្ថិភាពកំឡុងពេលដែលខាងក្រៅ និងមនុស្សមិនស្គាល់មុខនាំយកវាចូលទៅកាន់ប្រព័ន្ធកុំព្យូទ័រខាងក្នុង។ ក្រុមហ៊ុនភគច្រើនបានចំណាយនូវធនធានជាច្រើនដើម្បីការពារប្រឆាំងនឹងពួកវាយលុកពីខាងក្រៅ ប៉ុន្តែភាគច្រើននៃពួកលុកលុយគឺមានប្រភពមកពីខាងក្នុង។ តាមរយ:ការអោយព័ត៌មានពីក្រុមFBI បានអោយដឹងថា ៧០ភាគរយនៃការលុកលុយគឺនៅខាងក្នុង។



២.៤ Social Engineering and Phishing

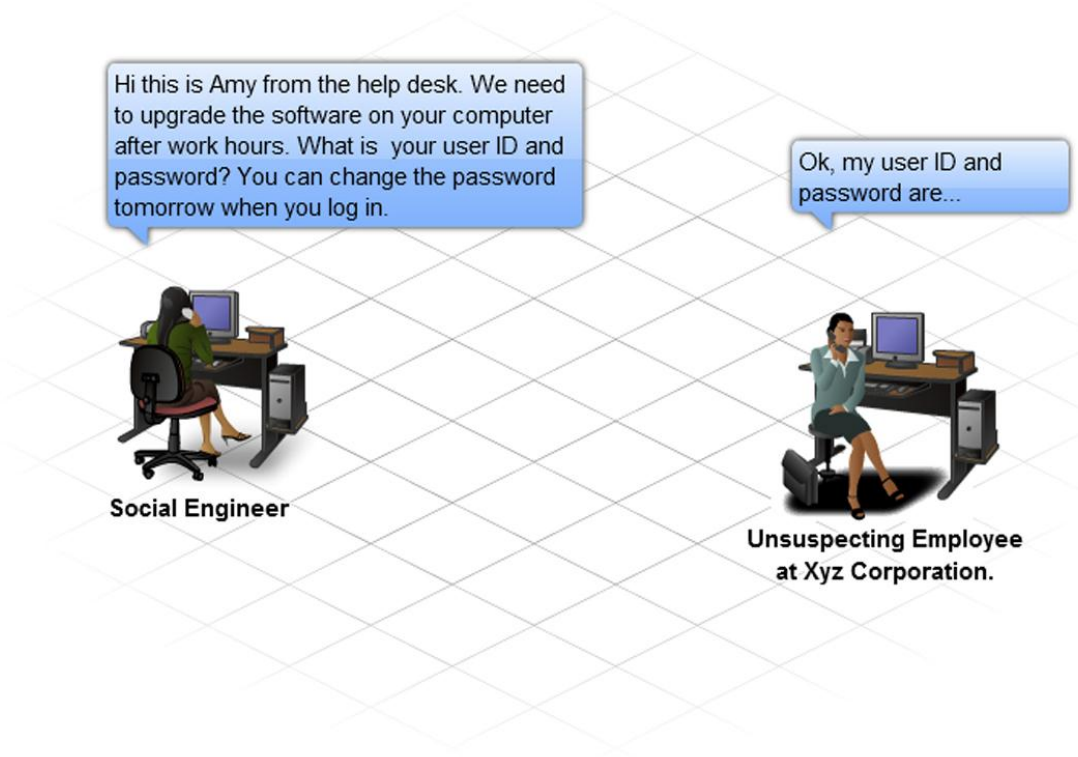
មធ្យោបាយម្យ៉ាងដែលងាយស្រួលសំរាប់ពួកហេក័រដើម្បីចូលក្នុងប្រព័ន្ធគឺការសើបសួរ។ នេះជាវិធីសាស្ត្រនៃការយកព័ត៌មានពីមនុស្សទន់ខ្សោយ ត្រូវបានគេហៅថា Social Engineering ។

Social Engineering

Social Engineering គឺជាសមត្ថភាពរបស់អ្វីមួយ ឬនរណាម្នាក់ក្នុងការទាក់ទាញចិត្តនៃក្រុមមនុស្ស ដើម្បីបំពេញគោលបំណងអ្វីមួយ។ ក្នុងបរិបទនៃកុំព្យូទ័រ និងបណ្តាញសុវត្ថិភាព Social Engineering គឺសំដៅលើបញ្ហកទេសនៃការប្រមូលព័ត៌មានដោយបោកបញ្ឆោតបុគ្គលិកនៅខាងក្នុងអោយអនុវត្តសកម្មភាពអ្វីមួយ ឬបង្ហាញព័ត៌មានសម្ងាត់។

ជាមួយនឹងបញ្ហកទេសទាំងនេះ ពួកហេក័របានទទួលផលប្រយោជន៍ និងសិទ្ធិស្របច្បាប់ដើម្បីចូលទៅកាន់ប្រភពខាងក្នុង និងព័ត៌មានឯកជន ដូចជា លេខគណនី និង លេខកូដ។

Social Engineering អាចជាអ្នកនៅខាងក្នុង ឬអ្នកនៅខាងក្រៅស្ថាប័ន ប៉ុន្តែភាគច្រើនពួកគេមិនបានអោយគេឃើញមុខនោះទេ។



Pretexting

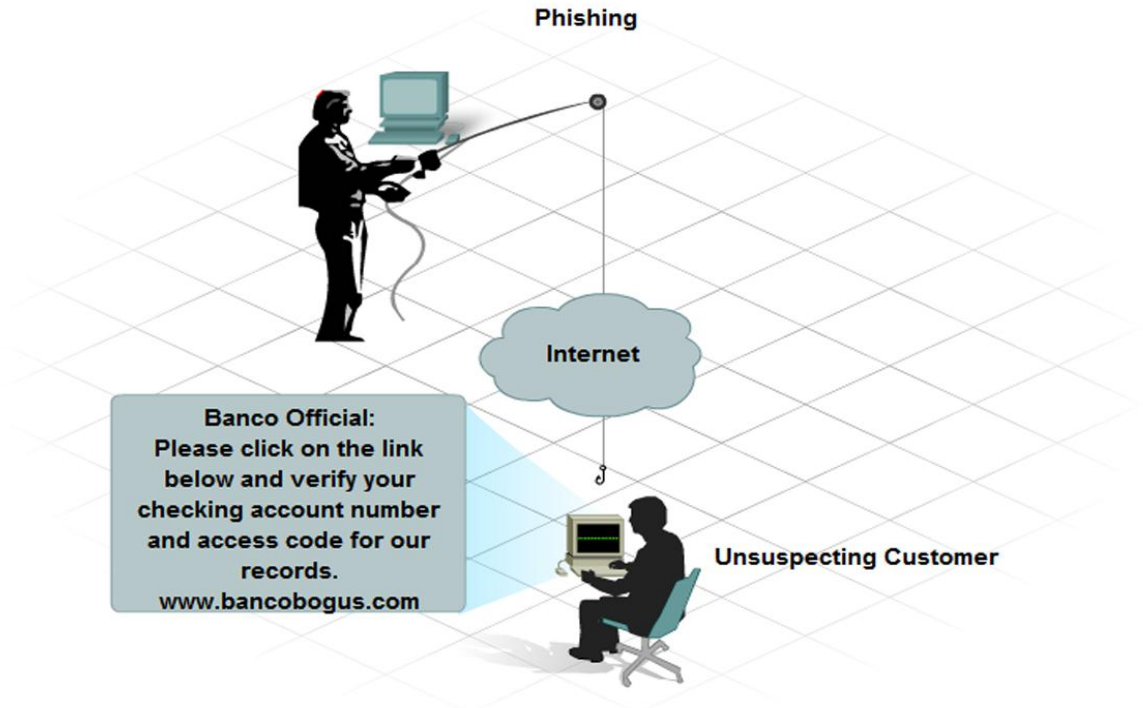
Pretexting គឺជាទំរង់មួយនៃSocial Engineering ហេាក័រប្រើដើម្បីទទួលព័ត៌មាន ឬអោយជនរងគ្រោះធ្វើសកម្មភាពអ្វីមួយអោយខ្លួន។ ជាធម្មតាហេាក័រភ្ជាប់ទំនាក់ទំនងតាមប្រព័ន្ធទូរស័ព្ទ។ ដើម្បីទទួលបានលទ្ធផល ហេាក័រត្រូវតែមានសមត្ថភាពក្នុងការបង្កើតសិទ្ធិស្របច្បាប់ជាមួយនឹងការតាំងចិត្តសំដៅទៅរកគោលដៅ។ ជាធម្មតាទាមទាអោយមានសមត្ថភាពខ្ពស់ និងស្រាវជ្រាវអោយបានច្រើនទៅលើអ្នកវាយលុកលុយ។ ឧទាហរណ៍ ប្រសិនបើហេាក័រលេខកូដ ពួកគេអាចប្រើព័ត៌មានទាំងនោះក្នុងការចូលទៅប្រព័ន្ធសុវត្ថិភាព។

Phishing

Phishing គឺជាទំរង់មួយនៃ Social Engineering ដែល Phisher បានក្លែងបន្លំជាអ្នកតំណាងអោយស្ថាប័នជាប់ពាក់ព័ន្ធណាមួយ។ ហេាក័រភ្ជាប់ទំនាកទំនងទៅកាន់គោលដៅដោយផ្ទាល់តាមរយៈសារអេឡិចត្រូនិច។ Phisher អានស្នើរសុំព័ត៌មានដើម្បីបញ្ជាក់អ្វីមួយ ដូចជាលេខកូដ ឬឈ្មោះអ្នកប្រើប្រាស់ ដើម្បីជាសវាងការកើតឡើងនូវបញ្ហាអ្វីមួយ។

Vishing / Phone Phishing

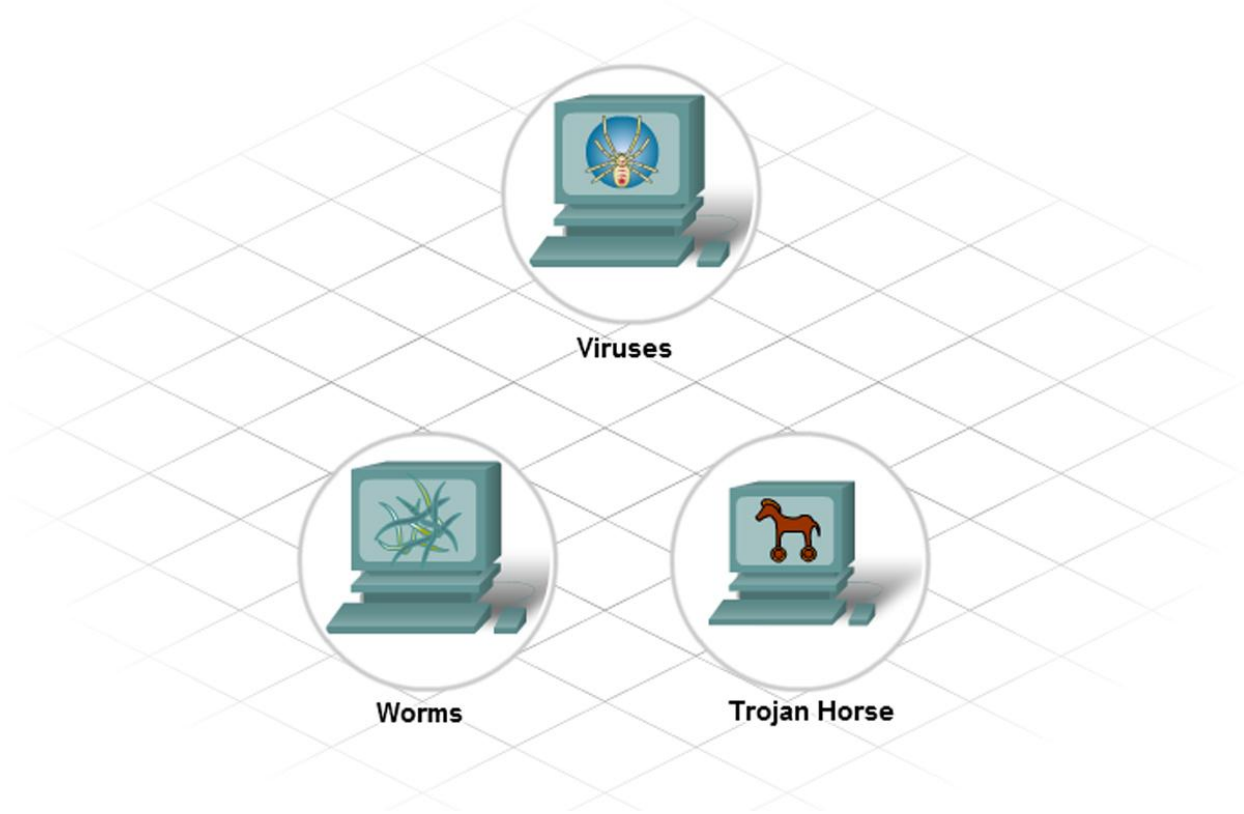
ទំរង់ថ្មីមួយនៃ Social Engineering ដែលប្រើសំលេងតាមរយៈ IP(VoIP) គឺត្រូវបានគេហៅថា Vishing។ ជាមួយនឹងVishing ជនរងគ្រោះត្រូវបានហេាក័រផ្ញើរសារជាសំលេងលក្ខណៈជាសេចក្តីណែនាំ ដើម្បីអោយហៅទៅលេខណាមួយ ដែលលេខលេចចេញឡើងមកនោះជាលេខសេវាកម្មរបស់ធនាគារណាមួយ។ បន្ទាប់មកការហៅទូរស័ព្ទនោះត្រូវបានស្តាត់ចាប់ដោយហេាក័រ។ លេខគណនីធនាគារ ឬលេខកូដដែលបានបញ្ចូនតាមរយៈទូរស័ព្ទសំរាប់បញ្ជាក់នោះ ត្រូវបានលួចដោយហេាក័រ។



៣. វិធីសាស្ត្រក្នុងការវាយប្រហារ

៣.ក ពពួកមេរោគ Worms និង Trojan Horses

ការគ្រប់គ្រងមិនច្បាស់លាស់នៅក្នុងសង្គមមួយ ធម្មតាជាការគំរាមកំហែងសន្តិសុខចំពោះមនុស្សទន់ខ្សោយ ដើម្បីបំពេញបំណងប្រាថ្នារបស់អ្នកប្រព្រឹត្ត ។ បន្ថែមលើការគ្រប់គ្រងមិនច្បាស់លាស់នេះ មានប្រភេទមួយចំនួននៃការវាយប្រហារដែលស្រូបយកផលចំណេញនៅក្នុង Computer Software ផងដែរ ។ ឧទាហរណ៍ នៃការវាយប្រហារបែបនេះរួមមាន: ពពួកមេរោគ Worms និង Trojan horses ។ រាល់ប្រភេទនៃ Software ដែលផ្តល់ទុក្ខទោសទាំងនេះត្រូវបានបង្កើតនៅលើ Computer ។ ពួកវាអាចធ្វើអោយខូច ប្រព័ន្ធ Computer, បំផ្លាញទិន្នន័យ, ក៏ដូចជាធ្វើអោយមិនអាចទំនាក់ទំនងទៅកាន់ប្រព័ន្ធ Network បាន, ប្រព័ន្ធផ្សេងៗ ឬ សេវាកម្មផ្សេងៗជាច្រើនទៀតផងដែរ ។ ពួកវាក៏អាចបញ្ជូនទិន្នន័យ និងពត៌មានលំអិតផ្ទាល់ខ្លួនពីអ្នកប្រើប្រាស់ត្រឹមត្រូវ ទៅអោយឧក្រិដ្ឋជនផងដែរ ។ មានករណីជាច្រើន ពួកវាអាចចំលងខ្លួនវា ហើយរាលដាលទៅកាន់ Computer ផ្សេងៗទៀតដែលបានភ្ជាប់ទៅកាន់ប្រព័ន្ធ Network ។ ពេលខ្លះបច្ចេកទេសទាំងនេះត្រូវបានប្រើប្រាស់រួមផ្សំជាមួយនឹងការគ្រប់គ្រងមិនបានត្រឹមត្រូវនៅក្នុងសង្គម ដើម្បីយកមកបោកប្រើអ្នកប្រើប្រាស់ដែលត្រឹមត្រូវអោយក្លាយទៅជាអ្នកវាយប្រហារ ។



ពពួកមេរោគ

មេរោគមួយ គឺកម្មវិធីមួយដែល ដំណើរការ និងរាលដាល ដោយធ្វើការកែប្រែកម្មវិធី ឬក៏ File ផ្សេងៗ ។ មេរោគមួយមិនអាចដំណើរការដោយខ្លួនវាផ្ទាល់បានទេ វាត្រូវការគេធ្វើសកម្មភាពលើវា ។ ការធ្វើសកម្មភាពលើវាម្តង មេរោគមួយវាមិនធ្វើអ្វីក្រៅពី ចំលងខ្លួនវា និងរាលដាលនោះទេ ។ ប្រភេទមេរោគទាំងនេះវាមានគ្រោះថ្នាក់ដូចជាវាអាចប្រើប្រាស់រាល់ Memory ដែលនៅទំនេរបានយ៉ាងលឿន និងនាំទៅរកនូវការបង្ហាក់ប្រព័ន្ធមួយ ។ មេរោគដែលកាន់តែធ្ងន់ធ្ងជាងនេះទៅទៀត វាអាចនឹងរៀបចំកម្មវិធីដើម្បីលុប ឬក៏ ធ្វើអោយខូច File ជាក់លាក់ណាមួយមុននឹងរាលដាលទៅកន្លែងផ្សេងៗទៀត ។

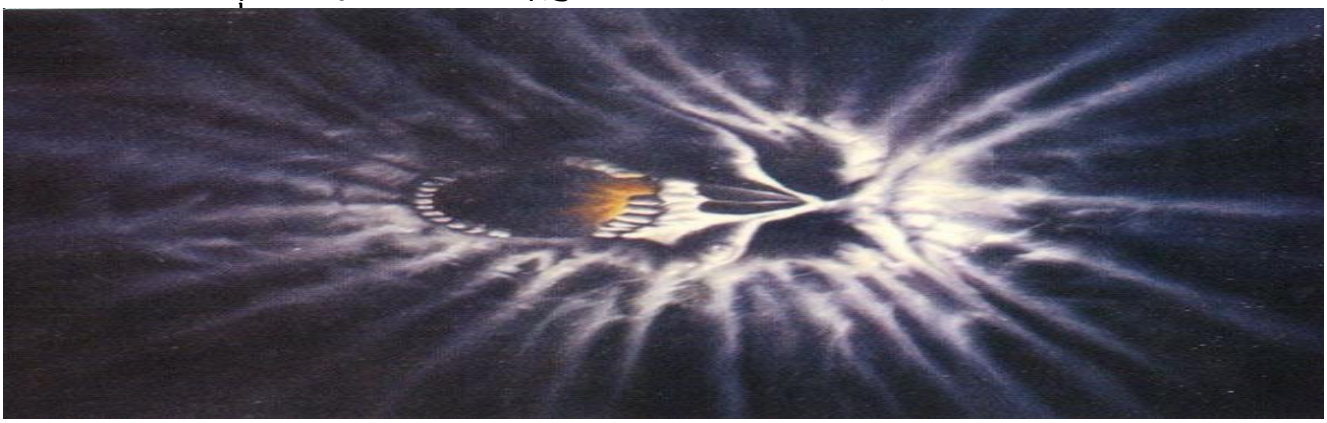
មេរោគជាច្រើនអាចត្រូវបានបញ្ជូនតាមរយៈ email attachments, downloaded files, instant messages ឬ តាមរយៈ diskette, CD ឬ តាមរយៈ ឧបករណ៍ USB ។

មេរោគ Worms

Worm គឺវាស្រដៀងទៅនឹងមេរោគមួយដែរ ប៉ុន្តែមិនដូចជាមេរោគទេ វាមិនត្រូវការភ្ជាប់ខ្លួនវាទៅនឹងកម្មវិធីមួយឡើយ ។ Worm វាប្រើប្រាស់ប្រព័ន្ធ Network ដើម្បីផ្ញើរខ្លួនវាដែលបានចំលងរួចទៅ Computer ដែលបានភ្ជាប់ប្រព័ន្ធ Network ។ Worm អាចដំណើរការដោយឯករាជ្យ និង រាលដាលខ្លួនវាយ៉ាងលឿន ។ ពួកវាមិនត្រូវការជាចាំបាច់ពីការធ្វើសកម្មលើវានោះទេ ឬ ការធ្វើអន្តរាគមន៍ពីមនុស្សឡើយ ។ ការរាលដាលយ៉ាងច្រើនដោយខ្លួនឯងនៅលើប្រព័ន្ធ Network worm អាចមានផលប៉ះពាល់ខ្លាំងជាងមេរោគតែវាមួយ ហើយវាឆ្លងពាសពេញ Internet បានយ៉ាងលឿន ។

មេរោគ Trojan Horses

Trojan horses គឺជាកម្មវិធីដែលមិនចំលងដោយខ្លួនឯង ដែលត្រូបានសរសេរដើម្បីអោយលេចឡើងដូចកម្មវិធីមួយត្រឹមត្រូវច្បាស់លាស់ដែរ តាមការពិតវាជាឧបករណ៍សំរាប់វាយប្រហារមួយសោះ ។ Trojan horse អាស្រ័យលើរូបរាងត្រឹមត្រូវរបស់វាដើម្បីបោកបញ្ឆោតជនរងគ្រោះយល់ថាវាជាកម្មវិធីថ្មីមួយ ។ វាអាចបណ្តាលអោយមានផលប៉ះពាល់តិចតួច ឬក៏ វាអាចផ្ទុកនូវ code ដែលអាចធ្វើអោយខូចនូវផ្នែនៃ hard drive របស់ Computer ។ Trojan អាចនឹងបង្កើតទ្វារក្រោយ (back door) នៅក្នុងប្រព័ន្ធមួយដែលអនុញ្ញាតអោយ hacker អាចចូលបាន ។



៣.ខ ការបិទសេវាកម្ម និងកំលាំងវាយប្រហាររបស់ជនកំណាច

ពេលខ្លះគោលបំណងរបស់អ្នកវាយប្រហារ គឺដើម្បីបិទការដំណើរការធម្មតារបស់ប្រព័ន្ធ Network ។ ប្រភេទវាយប្រហារនេះ ជាធម្មតាមានគោលបំណងក្នុងការបង្អាក់តួនាទីនៅក្នុងអង្គការមួយតែប៉ុណ្ណោះ ។

ការបិទសេវាកម្ម(DoS)

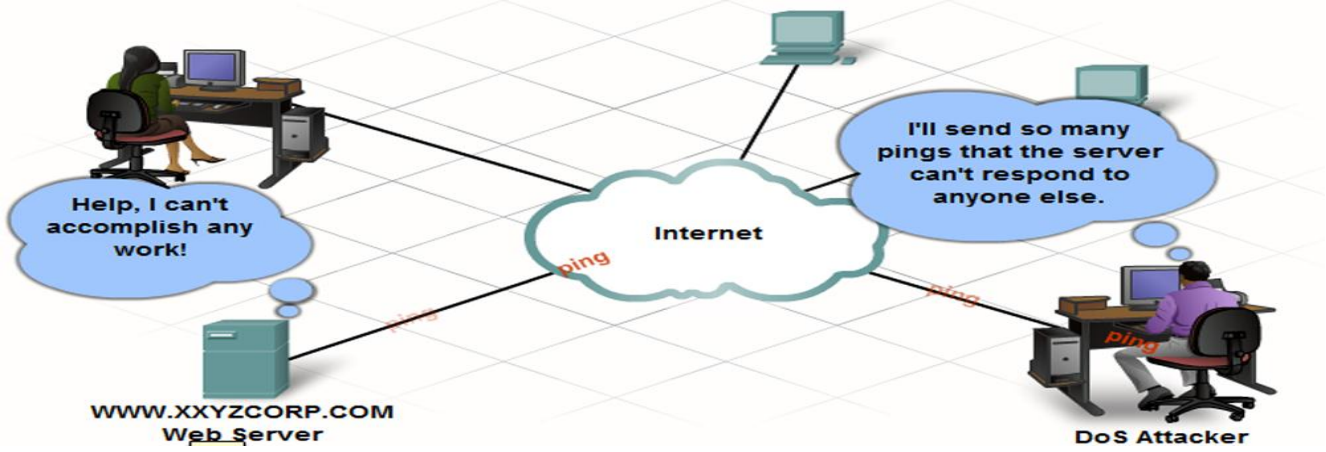
ការវាយប្រហារដោយបិទសេវាកម្ម(DoS) ជាការវាយប្រហារដោយឈ្លានពានទៅលើ Computer ផ្ទាល់ខ្លួនមួយ ឬក្រុមនៃComputer ជាមួយនឹងគោលបំណងចង់បិទសេវាកម្មរបស់អ្នកប្រើប្រាស់ ។ ការវាយប្រហារដោយបិទសេវាកម្ម អាចមានគោលបំណងចង់ បិទប្រព័ន្ធរបស់អ្នកប្រើប្រាស់, សេវាកម្ម, ឧបករណ៍ routers, និងទំនាក់ទំនងនៅក្នុងប្រព័ន្ធ Network ។
ជាទូទៅ ការវាយប្រហារដោយបិទសេវាកម្ម មានគោលបំណង៖

- ធ្វើអោយពោពេញទៅដោយការធ្វើចរាចរណ៍ នៅក្នុងប្រព័ន្ធ ឬប្រព័ន្ធ Network មួយ ដើម្បីការពារកុំអោយចរាចរណ៍នៅក្នុងប្រព័ន្ធNetworkត្រឹមត្រូវមួយមានលំហូរ
- ឆាឆៅការភ្ជាប់ទំនាក់ទំនងរវាង Client និង Server ក្នុងការប្រើប្រាស់សេវាកម្ម

ការវាយប្រហារដោយបិទសេវាកម្ម មានប្រភេទមួយចំនួន ។ សន្តិសុខ administrators ត្រូវដឹងពីប្រភេទ នៃការវាយប្រហារដោយបិទសេវាកម្ម ដែលអាចកើតឡើង និងធានាថាប្រព័ន្ធពួកគេត្រូវបានការពារ ។ មានពីរប្រភេទ នៃ ការវាយប្រហារដោយបិទសេវាកម្ម៖

❖ ការធ្វើអោយជន់ដំណាលគ្នា - ការជន់នៃ packets ដែលត្រូវបានផ្ញើទៅ Server មួយ នៃការស្នើសុំរបស់ Client មួយដែលបានភ្ជាប់ទៅ ។ Packets ទាំងនោះផ្តុំកន្លែងប្រភព IP Address មិនត្រឹមត្រូវ ។ Server នោះយកពេលវេលាព្យាយាមឆ្លើយតបទៅនឹង ការស្នើសុំក្លែងក្លាយទាំងនេះ ហើយដូច្នេះមិនអាចឆ្លើយតបមួយណាបានត្រឹមត្រូវឡើយ ។

❖ Ping of death: packet ដែលមានទំហំធំជាង ទំហំធំបំផុតដែលបានអនុញ្ញាត ដោយ IP (65,535 bytes) គឺត្រូវបានផ្ញើទៅអោយឧបករណ៍មួយ ។ នេះអាចបណ្តាលអោយទទួលបាននូវប្រព័ន្ធដែលខូច(crash) ។

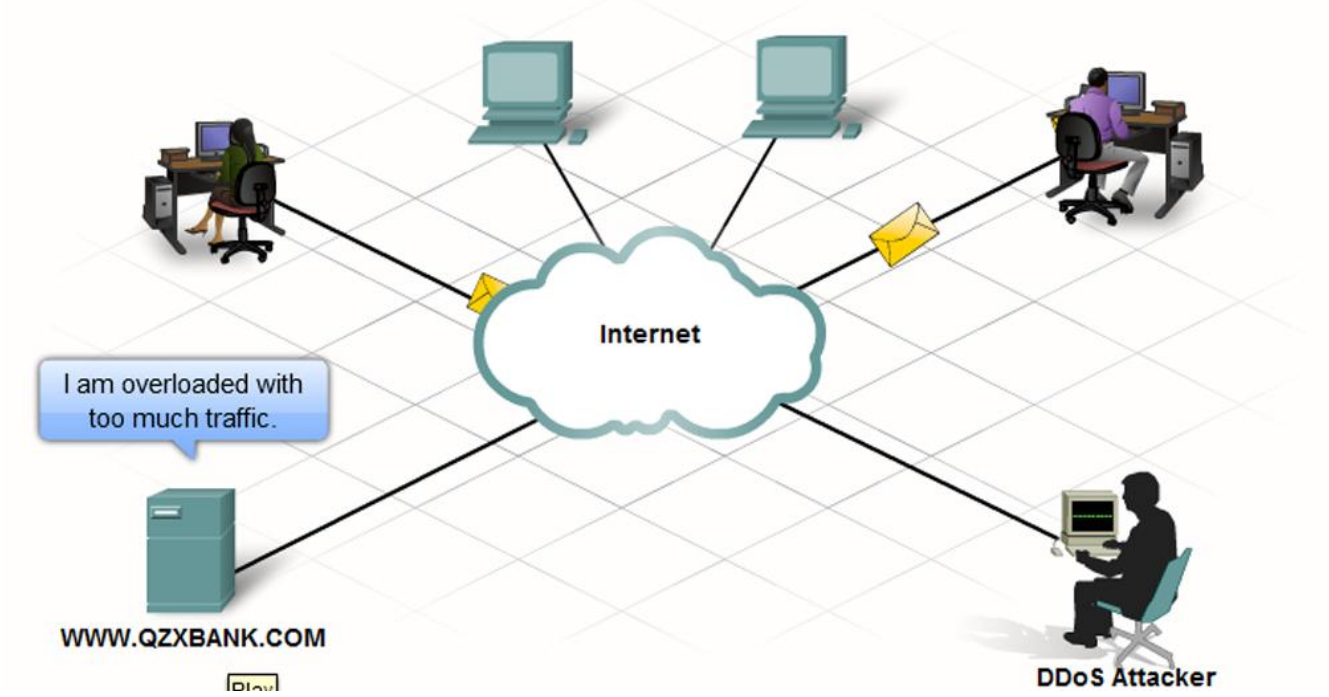


ការចែកចាយ ការវាយប្រហារដោយបិទសេវាកម្ម(DDoS)

DDos គឺជាទំរង់នៃការខូចខាតដ៏មានសក្តានុពល និងកាន់តែឆ្លាតវាងវៃ នៃ ការវាយប្រហារដោយបិទសេវាកម្ម ។ វាត្រូវបានបង្កើតឡើងដើម្បីធ្វើអោយជ្រួតជ្រាប និងគ្របសង្កត់លើទំនាក់ទំនងប្រព័ន្ធ Network ជាមួយនឹងទិន្នន័យគ្មានប្រយោជន៍ ។ DDoS ដំណើរការលើទំហំធំច្រើនជាង ការវាយប្រហារដោយ DoS ។ តួយ៉ាង មួយរយ ឬក៏មួយពាន់ នៃចំណុចដែលត្រូវវាយប្រហារ ដោយព្យាយាមសន្ធប់លើគោលដៅព្រមៗគ្នា ។ ចំណុចវាយប្រហារអាចជា Computer ត្រឹមត្រូវមួយដែលធ្លាប់បានធ្វើអោយខូចពីមុនមកដោយ DDoS code ។ ប្រព័ន្ធដែលរងគ្រោះជាមួយនឹង DDoS code ត្រូវបានវាយប្រហារនៅចំកន្លែងគោលដៅ នៅពេលដែលបានធ្វើការស្នើសុំ ។

Brute Force

មិនមែនរាល់តែការវាយប្រហារដែលបណ្តាលអោយសេវាកម្មប្រព័ន្ធ Network ត្រូវបានបិទ សុទ្ធតែមកពី ការវាយប្រហារដោយ DoS នោះទេ ។ ការវាយប្រហារដោយ Brute force ក៏ជាប្រភេទមួយផ្សេងទៀតនៃការវាយប្រហារមួយដែលអាចបណ្តាលអោយសេវាកម្មត្រូវបានបិទ ។
ជាមួយនឹង ការប្រហារដោយ Brute Force, Computer ដ៏លឿនមួយគ្រឿងត្រូវបានប្រើប្រាស់ដើម្បីទាយ លេខសំងាត់ ឬ ដើម្បីបកស្រាយ code សំងាត់(encryption) ។ អ្នកវាយប្រហារសាកល្បងនូវចំនួនលេខដ៏ច្រើនដែលអាចកើតមាននៅក្នុងភាពជោគជ័យដ៏រហ័ស ដើម្បីទទួលបានការចូល ឬក៏បំបែក code ។ ការវាយប្រហារដោយ Brute force អាចបណ្តាលអោយមានការបិទសេវាកម្ម ដោយយោងទៅលើការចរាចរណ៍ដ៏ច្រើនហួសហេតុទៅលើប្រភពជាក់លាក់មួយ ឬក៏ ដោយការបិទគណនីរបស់អ្នកប្រើប្រាស់ មិនអោយចូលបាន ។



៣.គ Spyware, Tracking Cookies, Adware និង Pop-Ups

មិនមែនរាល់ការវាយប្រហារសុទ្ធតែធ្វើអោយខូច ឬធ្វើអោយខូចភាពត្រឹមត្រូវរបស់អ្នកប្រើប្រាស់ ដោយការចូលទៅប្រើប្រាស់ប្រភពទិន្នន័យនោះទេ ។ ការគំរាមកំហែងជាច្រើនត្រូវបានបង្កើតឡើង ដើម្បីប្រមូលព័ត៌មានអំពីអ្នកប្រើប្រាស់ ដែលអាចប្រើប្រាស់ជាការផ្សព្វផ្សាយពាណិជ្ជកម្មមួយ, ការធ្វើទីផ្សារ និងគោលបំណងនៃការស្រាវជ្រាវ ។ ទាំងនេះរួមមាន Spyware, ការតាមដាន Cookies, Adware និងPop-up ។ នៅពេលដែលពួកវាអាចមិនធ្វើអោយខូច Computer ពួកវាលុកលុយលើភាពឯកជន និងអាចធ្វើអោយមានការរំខាន ។

Spyware

Spyware គឺជាកម្មវិធីមួយចំនួនដែលប្រមូលព័ត៌មានផ្ទាល់ខ្លួនពី Computer របស់លោកអ្នក ដោយគ្មានការអនុញ្ញាតពីលោកអ្នកជាមុន ។ ព័ត៌មាននេះត្រូវបានផ្ញើរទៅអ្នកផ្សព្វផ្សាយ ឬ មនុស្សជាច្រើនទៀតនៅលើ Internet ហើយអាចផ្ញើរទាំង លេខសំងាត់ និងលេខគណនីទៀតផង ។ Spyware ជាធម្មតាត្រូវបានដំឡើង ដោយមិនបានដឹងខ្លួននៅពេល មានការ download file, ការដំឡើងកម្មវិធីផ្សេងៗ ឬ ការ click popup ណាមួយ ។ វាអាចធ្វើអោយ Computer យឺតទៅៗ និងធ្វើការផ្លាស់ប្តូរការកំណត់ពីខាងក្នុង(internal setting) ហើយបង្កើតអោយមានផលប៉ះពាល់កាន់តែច្រើនឡើងសំរាប់ការគំរាមកំហែងផ្សេងទៀត ។ បន្ថែមពីលើនេះទៅទៀត Spyware អាចនឹងពិបាកខ្លាំងក្នុងការលុបវាចោលណាស់ ។

ការតាមដាន Cookies

Cookies ជាទំរង់នៃ Spyware មួយ ប៉ុន្តែវាមិនជាអាក្រក់គ្រប់ពេលនោះទេ ។ ពួកវាត្រូវបានប្រើសំរាប់ថតចំលងព័ត៌មានអំពីអ្នកប្រើប្រាស់ Internet នៅពេលដែលពួកគេចូលបើក website ផ្សេង ។ ។ Cookies អាចនឹងមានប្រយោជន៍ អាចទទួលយកបានដោយអាចយកមកធ្វើជារបស់ខ្លួន និងទុកប្រើប្រាស់ពេលក្រោយទៀតដោយការប្រើបច្ចេកទេសនៃការរក្សាទុក ។ មានគេហទំព័រជាច្រើនតម្រូវអោយ cookies អាចធ្វើការបាន(enable)ដើម្បីអនុញ្ញាតអោយអ្នកប្រើប្រាស់អាចភ្ជាប់ជាមួយបាន ។

Adware

Adware ជាទំរង់មួយនៃ Spyware ប្រើប្រាស់ដើម្បីប្រមូលព័ត៌មានអំពីអ្នកប្រើប្រាស់ដោយផ្អែកទៅលើគេហទំព័រដែលអ្នកប្រើប្រាស់បានចូល ។ បន្ទាប់មកព័ត៌មាននោះប្រើសំរាប់គោលបំណងនៃការផ្សព្វផ្សាយ ។ Adware ធម្មតាត្រូវបានដំឡើងដោយ អ្នកប្រើប្រាស់ដើម្បីជាថ្នូទទួលបានផលិតផលមិនគិតតំលៃ ។ នៅពេលអ្នកប្រើប្រាស់បើក window browser មួយ Adware អាចនឹងចាប់ផ្តើម browser ថ្មីមួយទៀតដែលព្យាយាមផ្សព្វផ្សាយពីផលិតផល ឬក៏ សេវាកម្មផ្សេងៗ ដោយវាអាស្រ័យលើការចូលមើលគេហទំព័រផ្សេងៗ របស់អ្នកប្រើប្រាស់នៅលើ Internet ។ Window browser ដែលយើងមិនចង់បានអាចនឹងបើកដដែលៗ ហើយអាចនឹងធ្វើអោយការចូលមើលគេហទំព័រផ្សេងៗនៅលើ Internet មានភាពលំបាកខ្លាំង ជាពិសេសធ្វើអោយមានភាពយឺតទៅៗ ក្នុងការភ្ជាប់ទៅកាន់ Internet ។ Adware អាចជាការលំបាកក្នុងការលុបវាចោលពីប្រព័ន្ធ ។

Pop-ups និង pop-unders

Pop-ups និង pop-unders ជាការបន្ថែមនៃការផ្សព្វផ្សាយនៅលើ Window ដែលបង្ហាញនៅពេលដែលកំពុងចូលមើលគេហទំព័រមួយ ។ មិនដូច Adware ទេ pop-ups និង pop-under មិនមានបំណងប្រមូលព័ត៌មានអំពីអ្នកប្រើប្រាស់ និង តួយ៉ាងវាចូលតែគេហទំព័រកំពុងបើកមើលនោះបណ្ណោះ ។

Pop-ups: បើកនៅពីលើ window browser ដែលកំពុងបើក ។

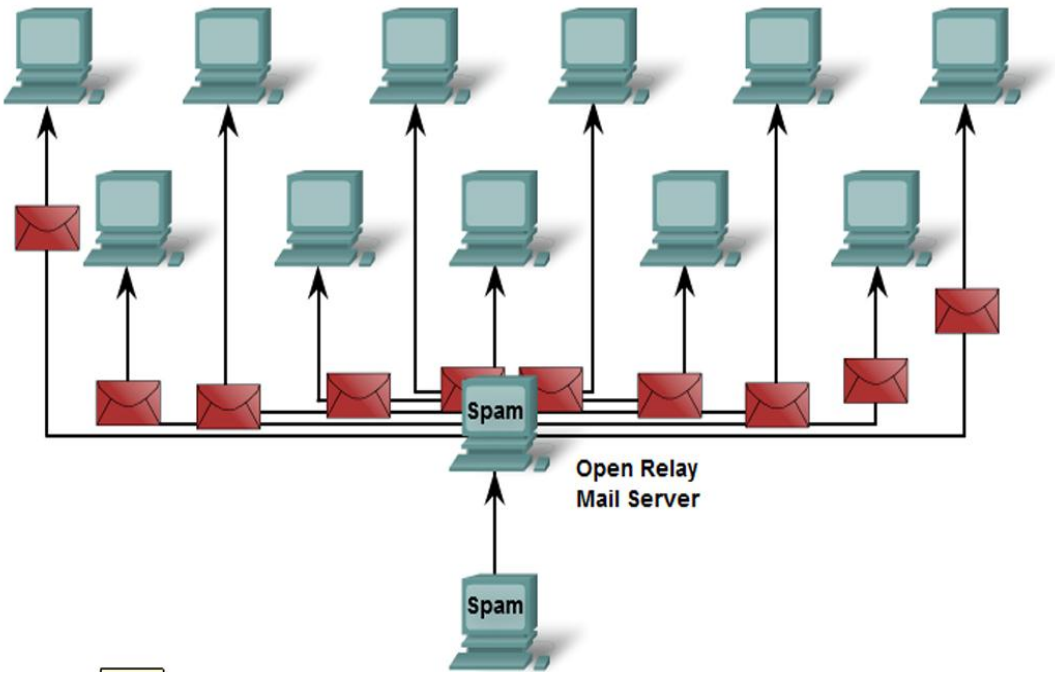
Pop-unders: បើកនៅពីខាងក្រោយ window browser ដែលកំពុងបើក ។

ពួកវាអាចនឹងធ្វើអោយរំខាន និង ជាធម្មតាផ្សព្វផ្សាយផលិតផល ឬក៏ សេវាកម្មណាដែលមិនគប្បីចង់បាន ។

៣.ឃ Spam

ការរំខានមួយផ្សេងទៀត គឺភាពច្រើនសំពីងសំពោងរបស់ email ដែលមិនចង់បាន ដែលបានកើនឡើងជាបន្តបន្ទាប់នៅលើបណ្តាញទំនាក់ទំនងអេឡិចត្រូនិច ។ ពេលខ្លះពាណិជ្ជករមិនចង់រំខានចំពោះគោលដៅទីផ្សាររបស់ខ្លួនទេ ។ ពួកគេចង់ផ្ញើរ email ផ្សាយពាណិជ្ជកម្មរបស់ខ្លួនទៅកាន់អ្នកប្រើប្រាស់អោយបានច្រើនតាមដែលអាចធ្វើទៅបាន ដោយសង្ឃឹមថាគ្រប់គ្នានឹងចាប់អារម្មណ៍ទៅលើផលិតផល និងសេវាកម្មរបស់ពួកគេ ។ វិធីសាស្ត្រនៃការចែកចាយដ៏ធំទូលាយដើម្បីរកទីផ្សារនៅលើ Internet នេះ គឺត្រូវបានហៅថា spam ។ Spam គឺជាការគំរាមកំហែងដ៏ធ្ងន់ធ្ងរនៅលើប្រព័ន្ធ Network ដែលអាចធ្វើអោយមានការផ្ទុកលើសចំណុះនៃ ISPs, email servers និងប្រព័ន្ធនៃអ្នកប្រើប្រាស់ផ្ទាល់ខ្លួន ។ មនុស្សម្នាក់ ឬ អង្គការមួយត្រូវមានទំនួលខុសត្រូវចំពោះការផ្ញើរ spam គឺហៅថា spammer ។ Spammer ជារឿយៗធ្វើការប្រើប្រាស់ email servers ដែលគ្មានសុវត្ថិភាពដើម្បីបញ្ជូន email ។ Spammer អាចនឹងប្រើប្រាស់បច្ចេកទេសក្នុងការ hack ដូចជាពពួកមេរោគ Worms និង Trojan horses ដើម្បីគ្រប់គ្រង Computer តាមផ្ទះ ។ Computer ទាំងនេះបន្ទាប់មកត្រូវបានប្រើប្រាស់ដើម្បីផ្ញើរ spam ដោយមិនចាំបាច់ធ្វើដោយ spammer ផ្ទាល់នោះទេ ។ Spam អាចនឹងត្រូវបានផ្ញើរតាមរយៈ email ឬក៏ ភ្លាមៗនេះអាចតាមរយៈ software ផ្ញើរសារផងដែរ ។

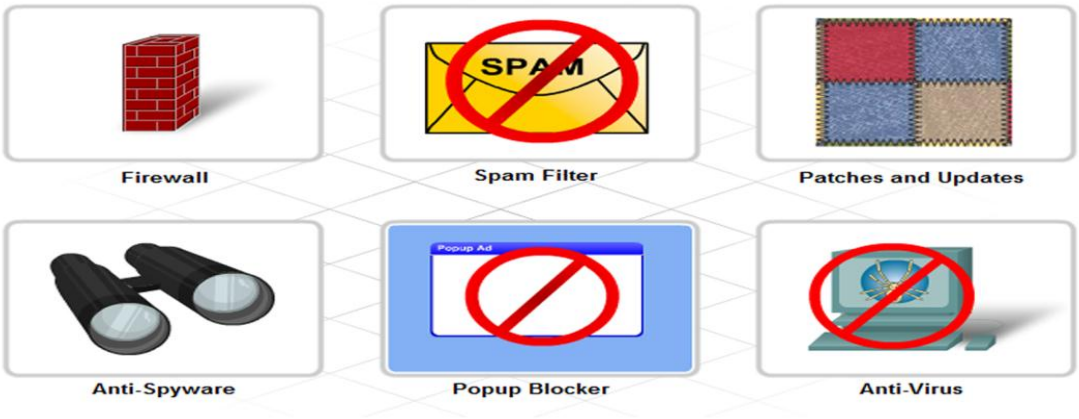
វាត្រូវបានវាយតំលៃថា រាល់អ្នកប្រើប្រាស់ទាំងអស់នៅលើ Internet ទទួលបាន ៣,000 email spam ក្នុងមួយឆ្នាំៗ ។ Spam ប្រើប្រាស់ទំហំច្រើនណាស់នៃ Internet bandwidth ហើយវាជាបញ្ហាធ្ងន់ធ្ងរគ្រប់គ្រាន់នឹងនាំអោយប្រទេសជាច្រើនឥឡូវមានច្បាប់មួយសំរាប់គ្រប់គ្រងទៅលើការប្រើប្រាស់ Spam ។



៤ Security Policy

៤.៥ Common Security Measures

Security risks មិនអាចកើតឡើងជោគជ័យនោះទេ ។ តែទោះជាយ៉ាងណាក៏ដោយ ការគ្រប់គ្រងទៅលើហានិភ័យអោយមានប្រសិទភាពហើយនិងការប៉ាន់ប្រមានអាចមានប្រយោជន៍យ៉ាងខ្លាំងក្នុងការកាត់បន្ថយការកើតឡើងនូវ Security risks ។ ដើម្បីកាត់បន្ថយចំនួននៃហានិភ័យ វាមានសារៈសំខាន់ដើម្បីយល់ថា មិនមានផលិតផលតែមួយអាចធ្វើអោយអង្គាមួយមាន Secure. បណ្តាញសុវិត្តិភាពដែលមានទំនុកចិត្តគឺវាបានមកពីការរួមបញ្ចូលនៃផលិតផលជាច្រើនហើយនិងសេវាកម្ម បានបញ្ចូលយ៉ាងម៉ត់ចត់ជាមួយ Security Policy ហើយនិងការតាំងចិត្តខ្ពស់ទៅលើ Policy ។ Security Policy មួយគឺជាលក្ខណធម្មតាមួយនៃច្បាប់ដែលអ្នកប្រើប្រាស់ត្រូវតែយកចិត្តទុក ដាក់ទៅលើវានៅពេលមានការចូលទៅប្រើប្រាស់បច្ចេកវិទ្យា ហើយនិងពត៌មានទ្រព្យសម្បត្តិ ។ វាអាចជារឿងសាមញ្ញ ដែលព្រមអោយប្រើ Policy រឺក៏អាចជាពីរបីរយទំព័រក្នុងព្រំកំនត់ ហើយនិងបកស្រាយគ្រប់ទិត្តភាពនៃការភ្ជាប់ទំនាក់ទំនងរបស់អ្នកប្រើប្រាស់ ហើយនិងការប្រើបណ្តាញតាមនីតិវិធី ។ Security Policy មួយគួតែមានចំនុចសំខាន់សំរាប់ប្រាប់ពីរបៀបនៃបណ្តាញមួយគឺមានសុវត្តិភាព ជាអ្នកគ្រប់គ្រង បានសាកល្បងរួច ហើយនិងមានការរីកចំរើន ។ គ្រប់ខណៈពេលដែលអ្នកប្រើប្រាស់នៅផ្ទះមិនមានការពារនូវ Security Policy ជាលក្ខណធម្មតាមួយ បណ្តាញមួយនិងមានសាយភាយនូវទំហំនិងដែនកំនត់ ផលប្រយោជន៍នៃការកំនត់ Security Policy សំរាប់អ្នកប្រើប្រាស់ ទាំងអស់មានការកើនឡើងយ៉ាងខ្លាំង ។ Security Policy ទាំងនោះរួមមាន ការកំនត់លក្ខណសំគាល់ និងបញ្ជាក់ការពិតនៃ Policies ប្រពន្ធលេខកូដ ការបញ្ជាអោយចូលទៅកាន់ Policies ហើយនិងការគ្រប់គ្រងឧប្បត្តិវហេតុបានត្រឹមត្រូវ ។



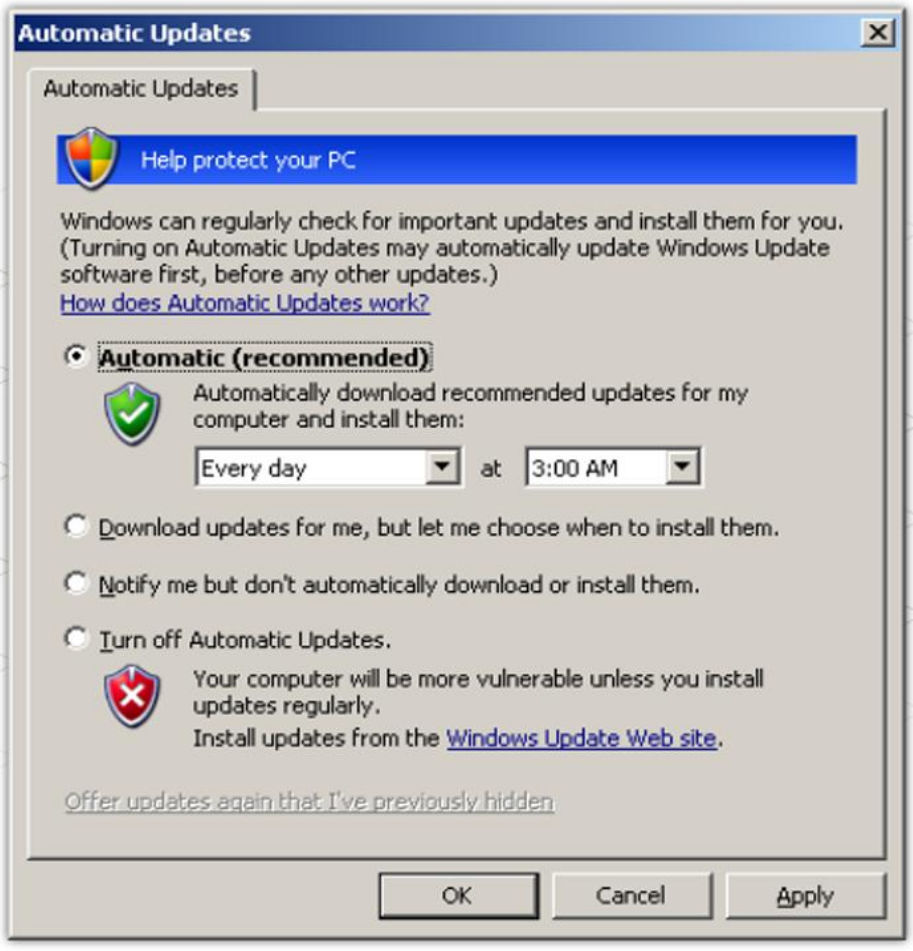
Security Policy រួមមាន

1. ការកំនត់លក្ខណសំគាល់ និង បញ្ជាក់ការពិតនៃ Policies។
   - ភាពជាក់លាក់នៃអំនាចរបស់មនុស្សដែលអាចចូលទៅកាន់ប្រភពរបស់បណ្តាញ ហើយនិង ការត្រួតពិនិត្យបានត្រឹមត្រូវ ។
   - វារួមមាន physical access ដើម្បីតភ្ជាប់ឧបករណ៍តូចៗ ហើយនិង critical ប្រភពបណ្តាញ មានដូចជា Servers, Switches, Routers, and Access points.
2. ប្រពន្ធលេខសំងាត់
   - ធ្វើអោយច្បាស់ថាលេខសំងាត់ត្រូវតែទាមទារអោយតិចសមរម្យហើយផ្លាស់ប្តូរជាទៀតទាត់ ។
3. ការបញ្ជាអោយចូលទៅកាន់ Policies
   - ការកំនត់ពីរបៀបនៃការបញ្ជារបស់អ្នកប្រើប្រាស់ដែលអាចចូលទៅកាន់បណ្តាញមួយ និង ចំងាយដែលបញ្ជាភ្ជាប់បាន ។
4. ការមើលថែរក្សាបណ្តាញអោយបានត្រឹមត្រូវ
   - ការមើលថែរក្សានូវភាពជាក់លាក់នៃប្រពន្ធប្រតិបត្តិការណ៍របស់ Device និងការ update end user application.
5. ការគ្រប់គ្រងឧប្បត្តិវហេតុបានត្រឹមត្រូវ
   - ពិពណ៌នាពីរបៀបនៃឧប្បត្តិវហេតុដែលនិងត្រូវបានប្រើ។
   - Procedures កំនត់នូវឯកសណ្ឋាន login, audit, ហើយនិង ដំនើរការណ៍នៃការថែរក្សាសំរាប់ hosts និង networks devices. រួមទាំងការប្រើនូវការវាយតំលៃសំរាប់បង្កាដើម្បីកាត់បន្ថយនូវហានីភ័យ ការវាយតំលៃនូវសកម្មភាពដ៏ល្អដើម្បីដឹងពីរបៀបនៃការវាយប្រហាទៅលើប្រពន្ធសុវិត្តិភាព ។ Security Procedures អាចរៀបចំពីលក្ខណធម្មតា មិនមានតំលៃថ្លៃ ដូចជា ការថែរក្សា up-to-date បោះពុម្ពពេញ Software ដើម្បីអនុវត្តទៅលើភាពស្មុកស្មាញនៃFirewall ហើយនិង ការរំលោភបំពាន ប្រពន្ធនៃការរកឃើញ ។
   - ឧបករណ៍សុវត្តិភាព និងApplication មួយចំនួនត្រូវបានប្រើប្រាស់ក្នុងសុវត្តិភាពបណ្តាញមាន
     - Software patches and updates
     - Virus protection
     - Spyware protection
     - Spam blockers
     - Pop-up blockers - Firewalls

៤.៥ Updates and Patches

មួយក្នុងចំនោមវិធីសាស្ត្រធម្មតាដែល hacker ប្រើដើម្បីចូលដល់ hosts or បណ្តាញគឺត្រូវឆ្លងកាត់Software vulnerabilities. វាមានសារៈសំខាន់ដើម្បីថែរក្សា software applications up-to-date ជាមួយប្រពន្ធសុវត្ថិភាពចុងក្រោយបង្អស់នៃ patches and updates ដើម្បីជួយរារាំងការវាយប្រហា។ patches គឺជាផ្នែកមួយតូចនៃកូដដែលផ្តោតយ៉ាងសំខាន់ទៅលើបញ្ហា ។ An update មានទាំងការបូកបញ្ចូលមុខងារទៅSoftware package ជាពិសេសការជុះជុលសំរាប់ភាពជាក់លាក់បំផុត ។

OS(ប្រពន្ធប្រតិបត្តិការណ៍ មានដូចជា Linux, Windows, etc.) and application vendors បន្តផ្តល់អោយកែតំរ៉ូវហើយនិងការជុះជុលសុវត្ថិភាពដែលអាចត្រឹមត្រូវ ស្គាល់ vulnerabilities ក្នុងSoftware. ក្នុងលក្ខខណ្ឌនេះ vendors ជាធម្មតាកាត់បន្ថយការប្រមូលនៃ ការជុះជុលនិងការកែតំរ៉ូវដែលហៅថា Service packs. ជាសំណាងល្អ មានប្រពន្ធប្រតិបត្តិការណ៍ជាច្រើនបានផ្តល់ការជុះជុលដោយស្វ័យប្រវត្តិ ដែលអនុវត្តតាម OS and កែតំរ៉ូវ application អោយក្លាយជាការ downloaded ស្វ័យប្រវត្តិ ហើយនិង Installed on a host.



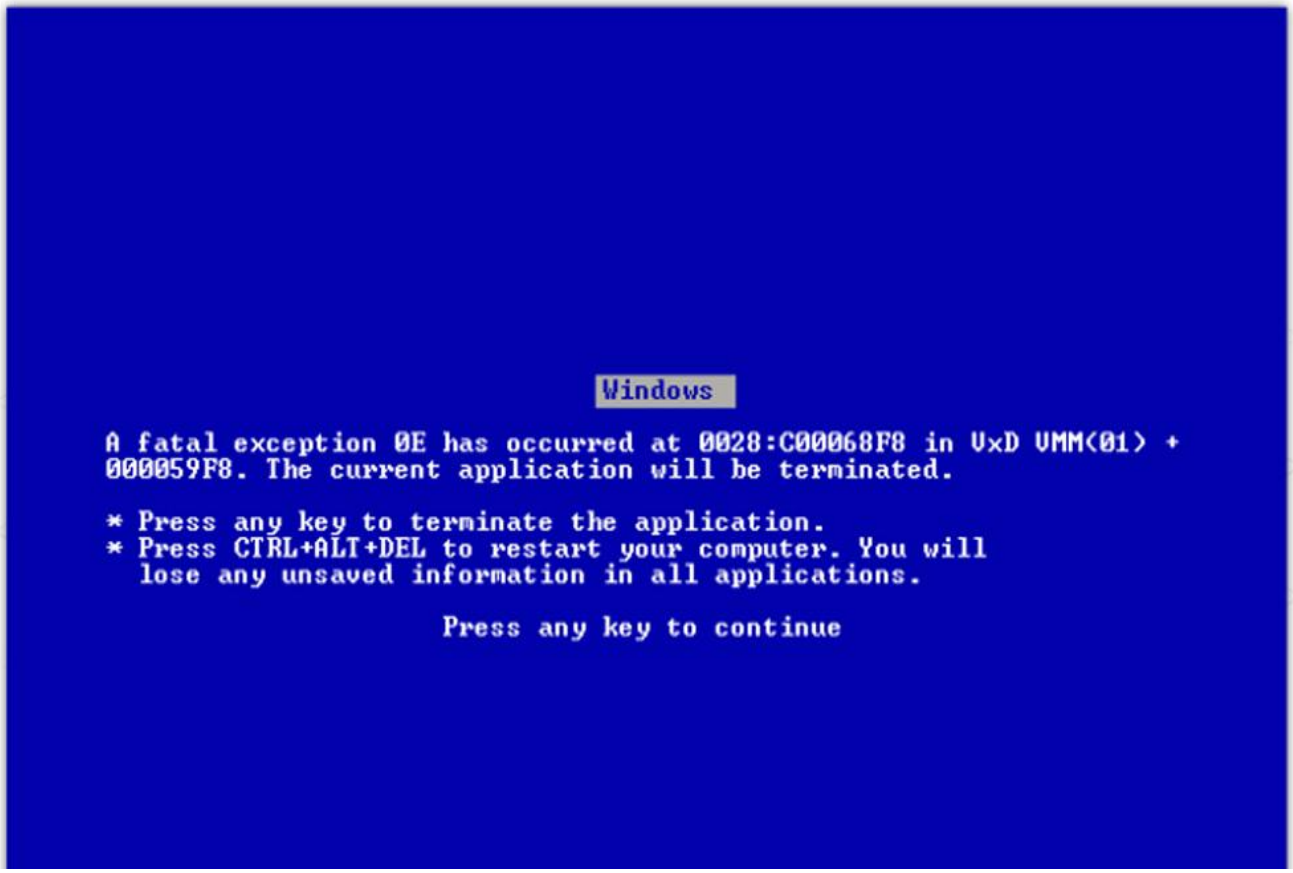
៤.គ Antivirus Software

Antivirus Software (Detecting a virus)

ថ្វីបើ OS ហើយនិង Application មានទាំងអស់ទាំងការជុះជុលនិងការកែតំរ៉ែក៏ដោយ ពួកវានៅតែទទួលបានការចូលលុកលុយដដែល ។ ឧបករណ៍មួយចំនួយដែលបានភ្ជាប់ទៅនិងបណ្តាញគឺទទួលរងអំពើពី Virus, Worms and Trojan horses. ទាំងអស់វាធ្វើអោយមានការរំខានដល់ OS code, ប៉ះពាល់ដល់ការអនុវត្តិកំព្យូទ័រ កែប្រែ Application និងបំផ្លាញទិន្នន័យ ។

រោគសញ្ញាមួយចំនួននៃ Virus, Worms, or Trojan horse ដូចជា

- កំព្យូទ័រដំនើការផ្លែកពីធម្មតា
- កម្មវិធីមិនឆ្លើយតបទៅនិង Mouse and keystrokes.
- កម្មវិធីដំនើរការ និងបិទដោយខ្លួនវា
- កម្មវិធីសាអេឡិចត្រូនិចចាប់ផ្តើមការបញ្ជូនចេញមានចំនួនធំ
- ប្រើ CPU កំរិតខ្ពស់
- មានការមិនបានកំនត់ រឺក៏ចំនួនលេខធំមួយ នៃ Processes running.
- កំព្យូទ័រយឺតនិងរអាក់រអួល



Anti-virus Software

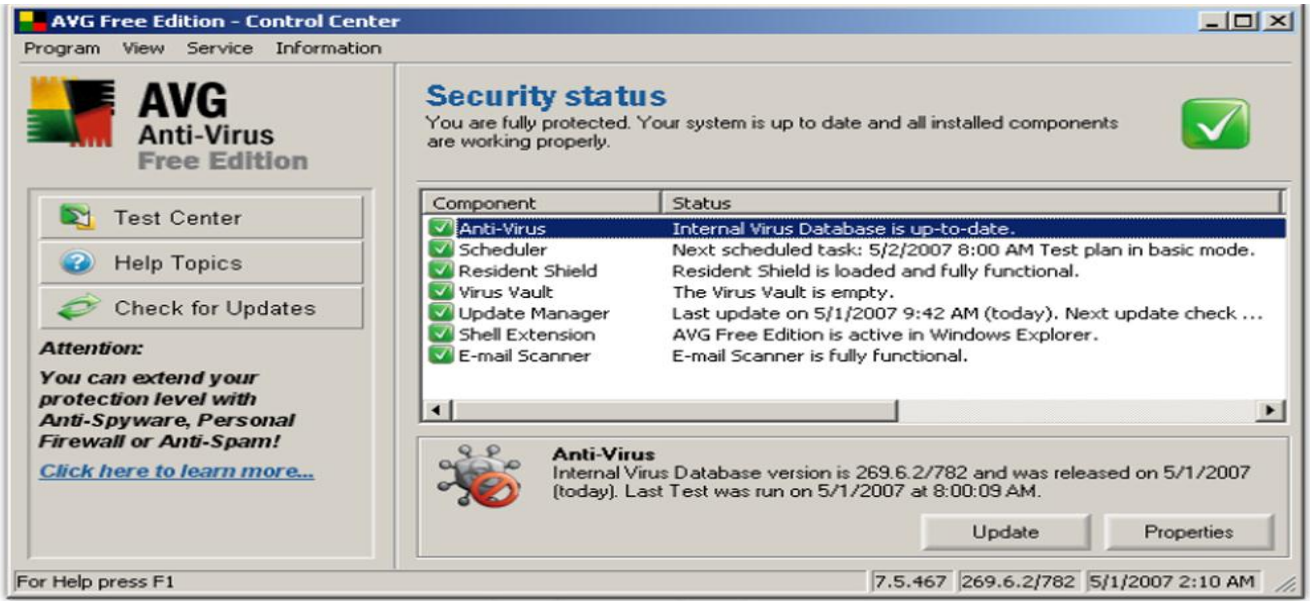
Anti-virus software អាចប្រើបានទាំងពីរ គឺ tool សំរាប់ការការពារ និងជាប្រតិករសំរាប់ការឆ្លើយតប ។ វាការពារការបង្ករោគ ការស៊ើបរក ការលុបចោល Viruses, worms, and Trojan horses. Anti-virus software គួតែតំលឡើងនៅគ្រប់កំព្យូទ័រដែលភ្ជាប់ទៅនិងបណ្តាញ ។

ចំនុចពិសេសមួយចំនួនដែលមាននៅក្នុង កម្មវិធី Anti-Virus

- **Email checking** =រកមើលការទទួលនិងការផ្ញើរចេញសារអេឡិចត្រូនិច ហើយនិងការកំនត់នូវមន្ទិលសង្ស័យនៃការទាញទិន្នន័យ ។
- **Resident dynamic scanning** =ត្រួតពិនិត្យការប្រតិបត្តិ Files និងdocuments នៅពេលដែលពួកវាត្រូវបានអនុវត្តិ ។
- **Scheduled scans**=រកមេរោគអាចជាពេលវេលាដែលត្រូវ run នៅចន្លោះពេលទៀងទាត់មួយ ហើយនិងត្រួតពិនិត្យ drives ជាក់លាក់ រឺក៏កំព្យូទ័រទាំងមូល ។
- **Automatic Updates** =ត្រួតពិនិត្យសំរាប់ការ download ស្គាល់ពីប្រភេទនៃមេរោគ និងលក្ខណសំគាល់ ។

Anti-virus software ជាសមត្ថភាពមួយទៅលើមេរោគក្នុងការសំលាប់វា ។ ម្យ៉ាងវិញទៀតនៅពេលដែលមេរោគគឺបានកំនត់អត្តសញ្ញាណច្បាស់លាស់ វាមានសារសំខាន់ដើម្បីធ្វើរបាយការណ៍វា រឺក៏លក្ខណមួយចំនួនរបស់មេរោគទៅលើបណ្តាញ Administrator ។ នេះគឺជាការសំរេចបានធម្មតាដោយការបញ្ជូនរបាយការណ៍ឧប្បត្តរហេតុសំអាងទៅលើប្រពន្ធបណ្តាញសុវត្តិភាពរបស់ក្រុមហ៊ុន។

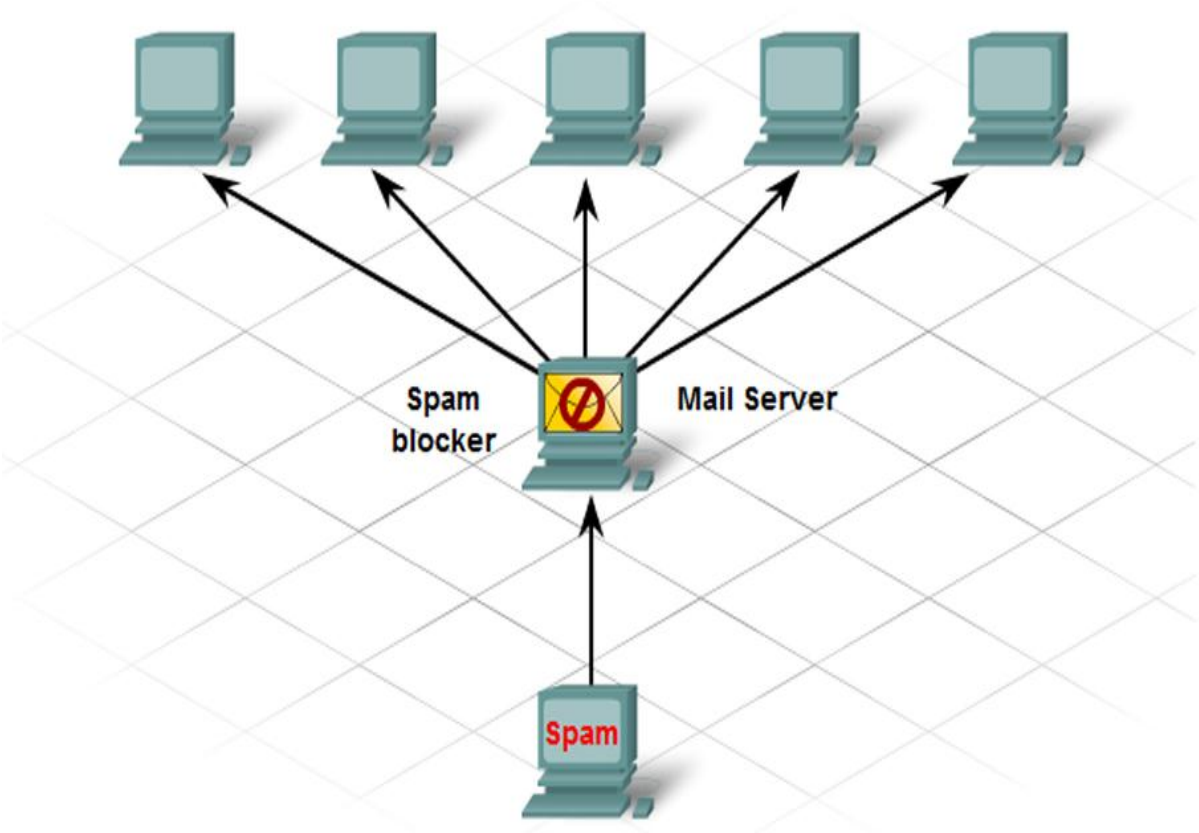
បណ្តាញអ្នកគ្រប់គ្រងផងដែរអាចមានរបាយការណ៍ថ្មីពីការវាយប្រហាទៅលើភ្នាក់ងារនៃតំបន់អ្នកគ្រប់គ្រងរដ្ឋដែលមានបញ្ហាសុវិត្តភាព ។



៤.៣ Anti-Spam

Spam មិនមែនគ្រាន់តែរំខានប៉ុននោះទេ វាអាច overload សាអេឡិចត្រូនិច servers ហើយ និងថាមពលនៃការចាប់យកមេរោគនិងការវាយប្រហាសុវិត្ថិភាពដទៃទៀត ។ បន្ថែមពីលើនេះទៀត Spammers បានយកការគ្រប់គ្រងទៅលើ hosts ដោយបង្កើតដាក់លើវាក្នុង form នៃ virus or a Trojan horse ។ hosts គឺអាចប្រើដើម្បីផ្ញើរសារដោយមិនចាំបាច់អ្នកប្រើប្រាស់មានចំនេះដឹង ។ កំព្យូទ័រមួយបានធ្វើមធ្យោបាយអោយស្គាល់ Spam mill

Anti-spam software ការពារhosts ដោយការកំនត់spam និងការអនុវត្តិទៅលើសកម្មភាព ដូចជាផ្លាស់ប្តូរទីតាំងវាចូលទៅក្នុងធុងសំរាម រឺលុបវាចោល ។ វាដំនើរការនៅលើម៉ាស៊ីន ប៉ុន្តែអាចដំនើរការនៅលើ សាអេគិចត្រូនិច Servers ផងដែរ ។ ក្នុងលក្ខខណ្ឌនេះមាន ISPs ជាច្រើននៅក្នុង Spam. Anti-spam software មិនបានរៀបទៅតាម Spam ទាំងអស់នោះទេ ដូចនេះហើយ វាមានសារសំខាន់ដើម្បីបើកសាអេឡិចត្រូនិចដោយប្រុងប្រយ័ត្ន ។ វាផងដែរបានកំនត់នូវអ្វីដែលបានកើតឡើងដោយមិនបានដឹងមុន ដែលចង់អោយសាអេឡិចត្រូនិចដូចជា Spam ។



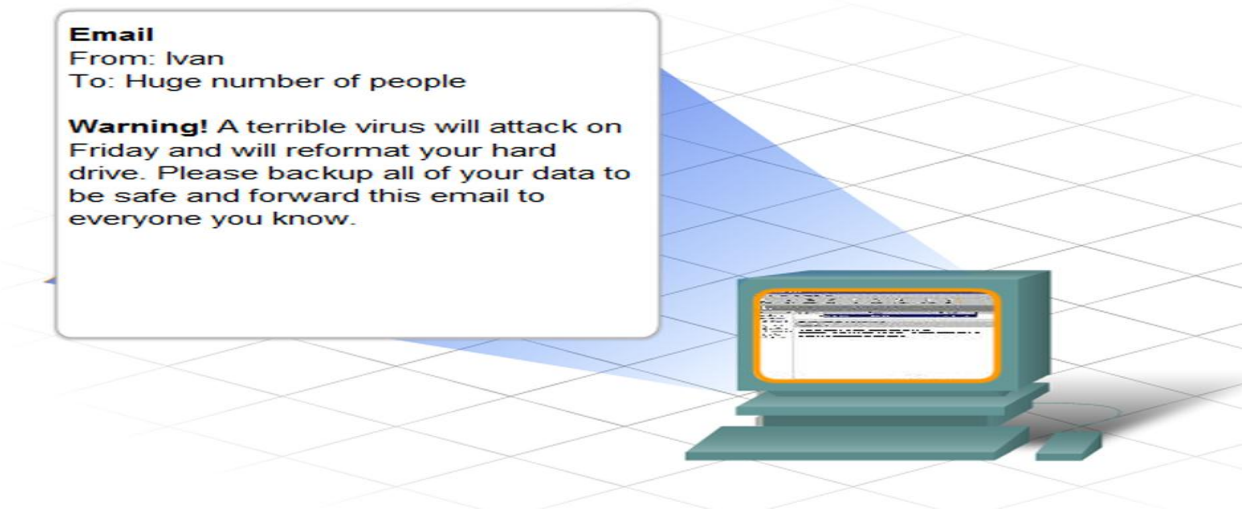
ក្នុងលក្ខខណ្ឌនេះក្នុងការប្រើSpam blockers, សកម្មភាពនៃការការពារដ៏ទៃទៀតដើម្បីការពារការរីករាលដាលនៃSpam មានដូចជា

- កែតំរ៉ែ OS and Application នៅពេលវាទំនេរ ។
- ដំនើរការកម្មវិធីកំចាត់មេរោគយ៉ាងទៀងទាត់ ហើយឧស្សាUpdate វា ។
- Don not forward suspect emails.
- កុំបើកភ្ជាប់សាអេឡិចត្រូនិច ជាពិសេសពីមនុស្សដែលយើងមិនស្គាល់ ។
- បង្កើតច្បាប់ក្នុងសាអេឡិចត្រូនិចដលម្បីលុប Spam ដែលបានបញ្ជូនដោយ anti-spam software។
- កំនត់ប្រភពនៃ Spam ហើយនិង របាយការណ៍របស់វាទៅលើអ្នកគ្រប់គ្រងបណ្តាញ ដូច្នេះវាអាច blocked បាន ។
- របាយការណ៍ឧប្បត្តិវហេតុទៅលើភ្នាក់ងារអ្នកគ្រប់គ្រងរដ្ឋ ដែលបានចែកជាមួយការរំលោភច្បាប់ដោយ Spam ។

មួយក្នុងចំនោមប្រភេទទាំងអស់នៃ Spam ដែលបានបញ្ជូនមកគឺជាការប្រកាសអាសន្នរបស់មេរោគ ។ នៅពេលដែលការប្រកាសអាសន្នរបស់មេរោគបានបញ្ជូនតាមសាអេឡិចត្រូនិចពិតប្រាកដមែន នោះចំនួនដ៏ធំនៃពួកវាគឺជាទំហំបញ្ឆោតហើយនិងមិនមែនជាការពិត ។ ប្រភេទនៃ spam នេះអាចបង្កើតជាបញ្ហាជាច្រើន ពីព្រោះមនុស្សត្រូវបានគំរាមដោយមហន្តរាយគួរអោយភ័យខ្លាច និងធ្វើអោយមាន email ច្រើនរាប់មិនអស់ ។ លើសពីនេះទៅទៀត administrator របស់ប្រព័ន្ធ Network

អាចធ្វើអោយហួសពេលក្នុងការឆ្លើយតប និងខាតពេលវេលាក្នុងការស៊ើបអង្កេតជាមួយនឹងបញ្ហាដែលមិនមាន ។ ចុងក្រោយ email ដ៏ច្រើននេះអាចជួយអោយមានការរាលដាលរបស់ពពួកមេរោគបាន ដូចជា ពពួក Worms និង Trojan horses ។ មុននឹងបញ្ជូន email ព្រមាន របស់មេរោគ យើងត្រូវពិនិត្យមើលថា វាបញ្ឆោត ឬអត់ដោយចូលទៅគេហទំព័រដូចជា:

http://vil.mcafee.com/hoax.asp or http://hoaxbusters.ciac.org/ ។



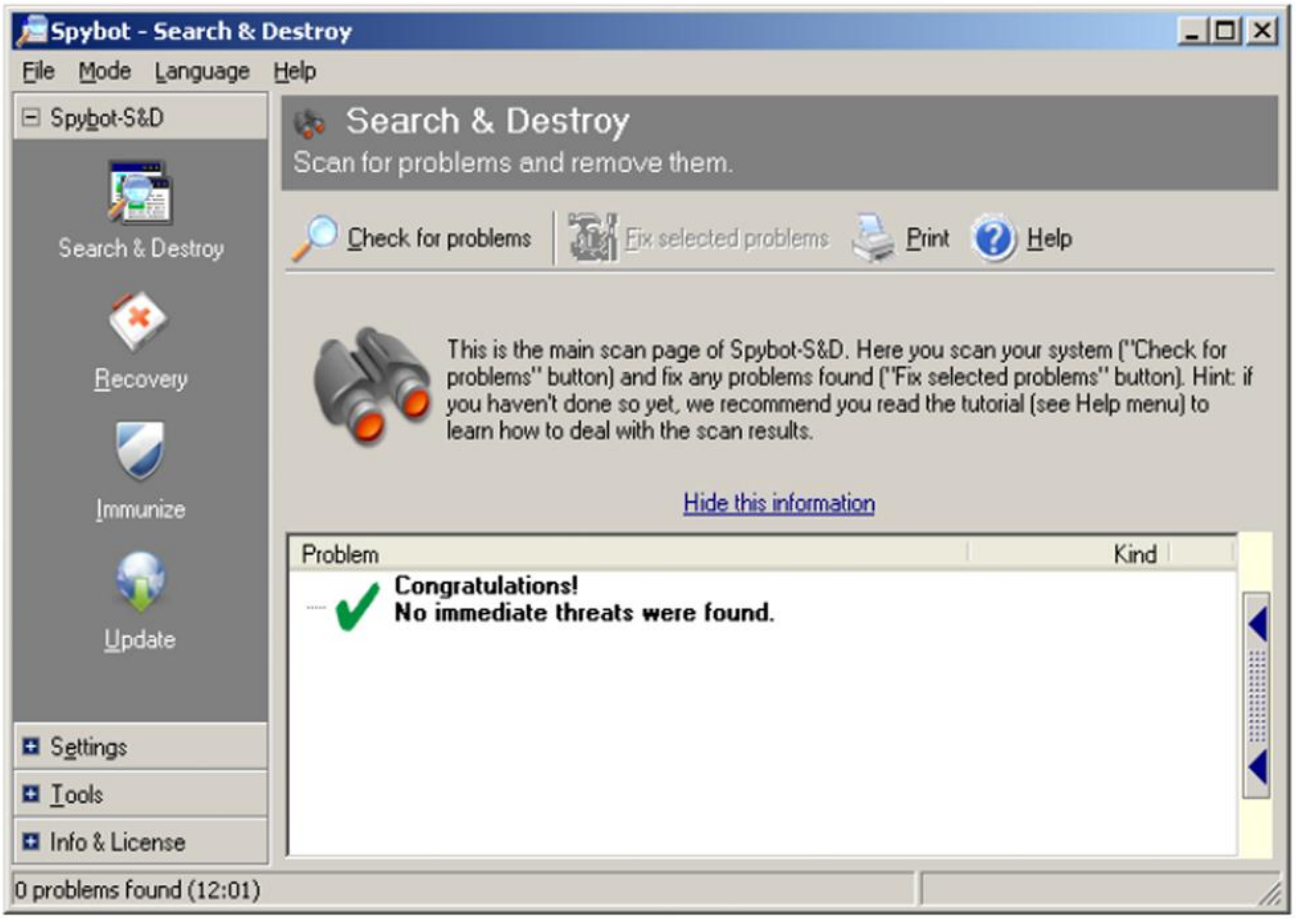
៤.៦ Anti-Spyware

Anti-Spyware and Adware

Spyware and adware អាចបណ្តាលជាជំងឺមួយដែរ ។ បន្ថែមទៅលើការ ប្រមូលព័ត៌មានដែលមិនបានអនុញ្ញាតអោយ ពួកគេអាចនឹងប្រើប្រាស់ប្រភពធនធាន computer ដែលមានសារៈសំខាន់ និងអាចធ្វើអោយប៉ះពាល់ដល់ដំណើរការ ។ Anti-spyware software វាធ្វើការកត់សំគាល់ និងលុបចោលនូវ spyware applications ក៏ដូចជាការ ការពារការដំឡើងនៅពេលក្រោយទៀត ។ Application spyware ជាច្រើនបានបញ្ចូលនូវការកំណត់ចំណាំ និងការលុបនៃ cookies និង adware ផងដែរ ។ Packages anti-virus មួយចំនួនរួមមាន តួនាទីរបស់ anti-spyware ។

Pop-up Blockers

Software pop-up stopper ត្រូវបានដំឡើងដើម្បីការពារ pop-ups និង pop-unders ។ មាន web browsers ជាច្រើនបានបញ្ចូល pop-up blocker feature ដាក់ជា default ។ ចំណាំថា កម្មវិធីមួយចំនួន និងគេហទំព័រមួយចំនួនបង្កើតមកមានសារៈសំខាន់ និងទាក់ទាញ pop-ups ។ Pop-up blockers ជាច្រើន ផ្តល់អោយមានការ override feature សំរាប់គោលបំណងនេះ ។



៥. Firewalls

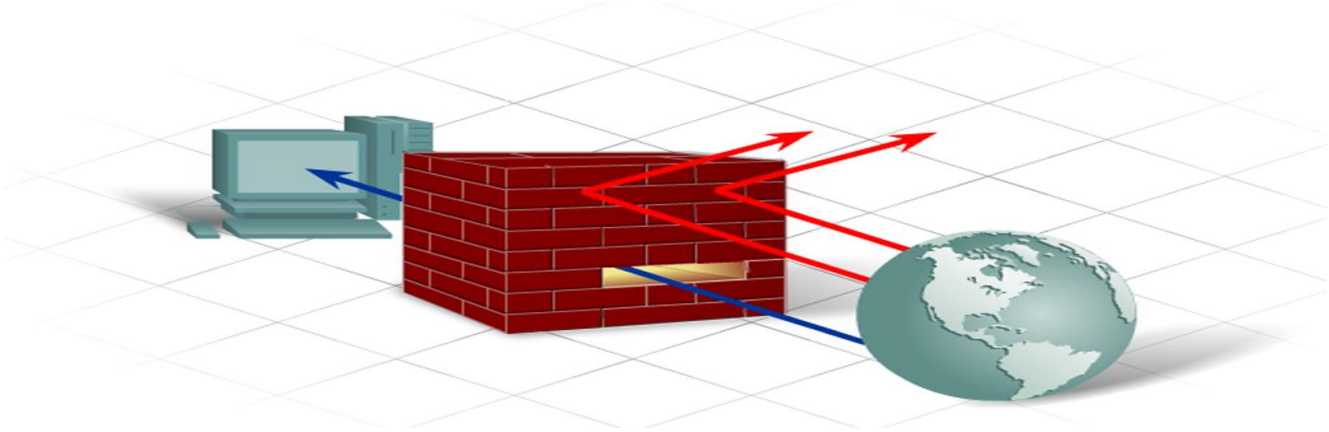
៥.១. តើអ្វីទៅជា Firewall?

វាពិតជាមានសារៈសំខាន់ណាស់ក្នុងការគ្រប់គ្រងអោយបានជាប់លាប់ល្អទៅលើការបញ្ជូន កម្មវិធី រឺឯកសារនានាតាមរយៈ Network ដើម្បីបន្ថែមទៅលើការការពារ client កុំព្យូទ័រ ពីការទទួលទិន្នន័យនានាពី server នោះ អ្នកគួរតែយកចិត្តទុកដាក់ទៅលើ Firewall របស់កុំព្យូទ័រ ។តើ Firewall ជាអ្វីទៅ? ហើយវាពិតជាអាចការពារនូវការជ្រៀតចូលនូវ Virus, Warm និង Spyware មែនរឺ ?

Firewall គឺជា Tool មួយក្នុងចំណោម Security Tool ទាំងឡាយ ដែលមានតួនាទីការពារកុំព្យូទ័ររបស់យើងដូចជា anti-virus, anti-spyware ផ្សេងៗទៀតដែរ ប៉ុន្តែវាធ្វើការការពារ internal network របស់យើងទៅនឹងការឆ្លងនានាដែលយើងមើលមិនឃើញ ។បន្ថែមលើនេះ Firewall វាមាននាទីស្ថិតនៅចន្លោះកណ្តាលនៃ network ពីរ រឺច្រើនសម្រាប់គ្រប់គ្រងទៅលើការបញ្ជូនទិន្នន័យ រឺទទួលទិន្នន័យ ក្នុងគោលបំណងជួយការពារនូវការ access ណាមួយមិនច្បាស់លាស់មកកាន់កុំព្យូទ័ររបស់យើង ។ ផលិតផល រឺ កម្មវិធីដែលមានប្រភេទជា Security Firewall នេះបាន ប្រើនូវ Technique យ៉ាងច្រើន សម្រាប់កំណត់ថាតើ network មួយ គួររឺពុំគួរអនុញ្ញាតអោយ access ។

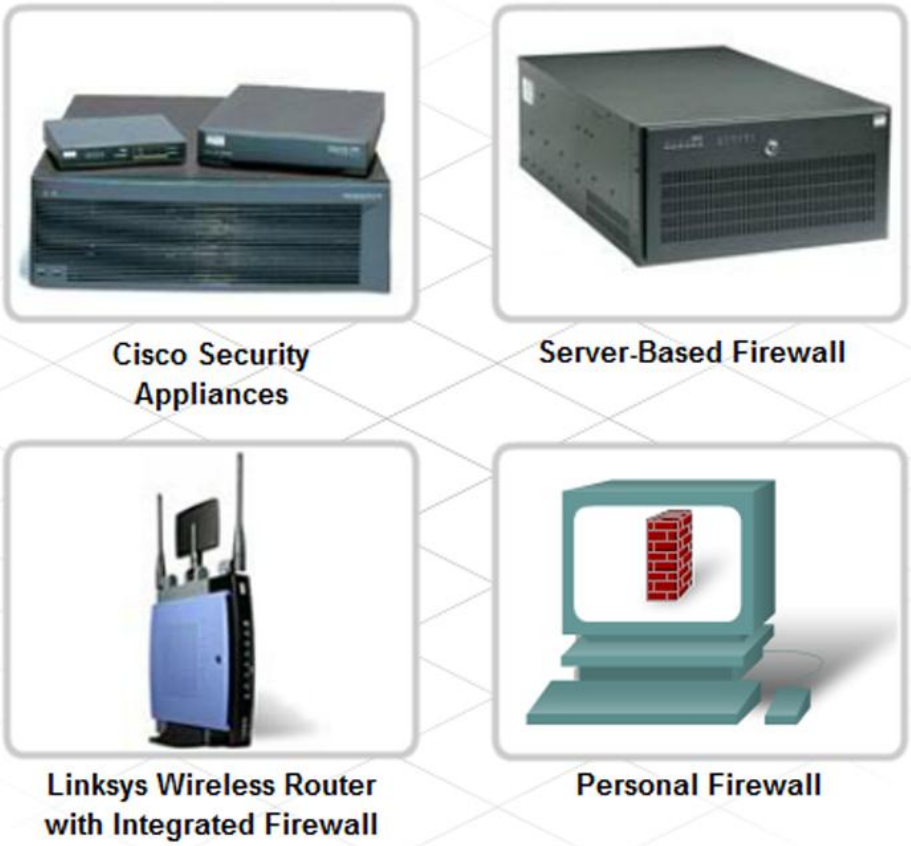
Packet Filtering: ការពារ រឺអនុញ្ញាតនូវការ access ដោយផ្អែកទៅលើ IP រឺ MAC address ដែលវា ធ្វើការនៅក្នុង network level នៃស្រទាប់ OSI ។បន្ថែមលើនេះ វាមានការជះឥទ្ធិពលតិចតួចបំផុតទៅ លើដំណើរការ network ។

Application /Web Site Filtering: ការពារ រឺអនុញ្ញាតនូវការ access ដោយផ្អែកទៅលើកម្មវិធីដែលវា ធ្វើការនៅ application level នៃស្រទាប់ OSI ។ការបិទនូវរាល់ website អាចត្រូវបានកំណត់តាមរយៈ URL Address របស់ website រឺក៏ Keyword ។លើសពីនេះវាមានប្រសិទ្ធភាពខ្ពស់ក្នុងការការពារ computer របស់អ្នក ។



Stateful Packet Inspection (SPI): Firewall ដែលរុករកពត៌មាន គុណភាព និង សន្និដ្ឋានដោយប្រុងប្រយ័ត្ននូវរាល់ការជ្រៀតចូលផ្សេងៗ រឺការ request internal host ដែលធ្វើការនៅ Multilayer ដូចជា application layer, session layer និង network layer ។វាមានប្រសិទ្ធខ្ពស់ក្នុងការការពារដំណើរការយ៉ាងល្អ និងផ្តល់ភាពងាយស្រួលដល់អ្នកប្រើប្រាស់ ។

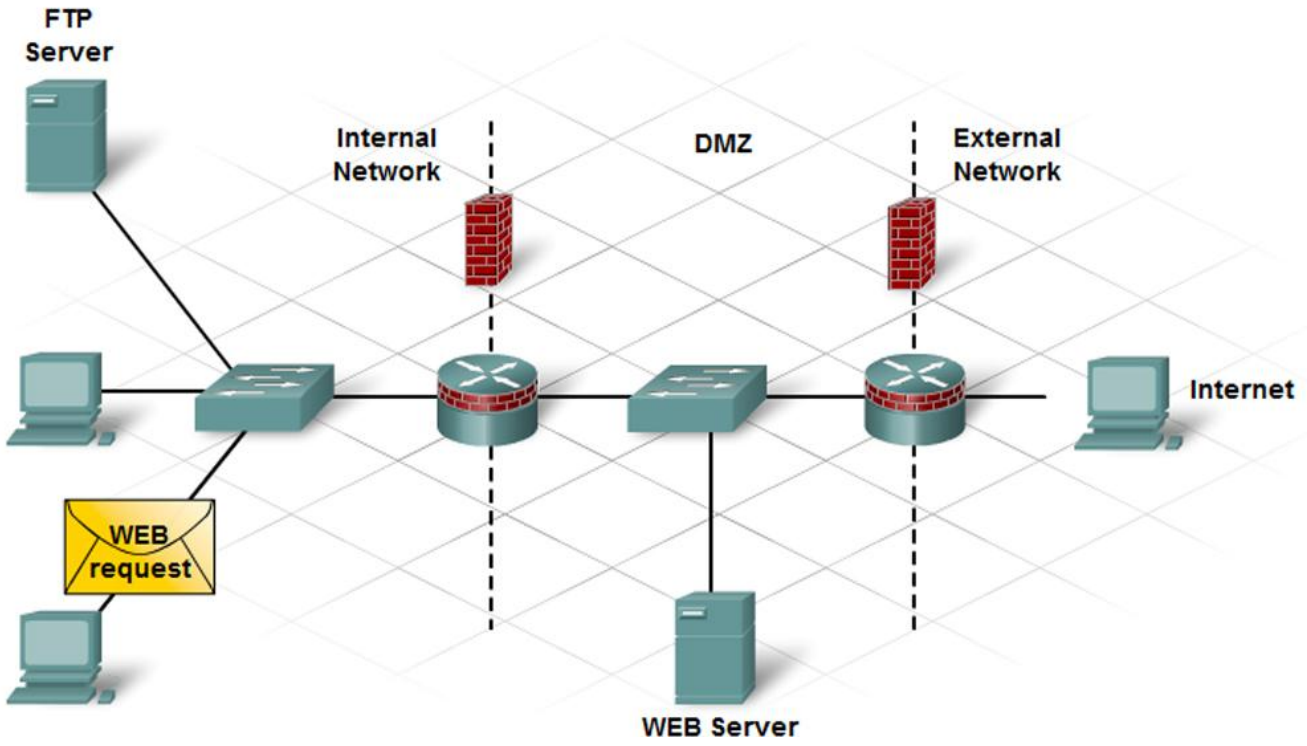
យើងក៏អាចសំគាល់ផងដែលថា រាល់ Firewall Product អាច support នូវសមត្ថភាពច្រោះពត៌មាន មួយ រឺច្រើនដែលបានបង្ហាញខាងលើនេះ ។លើសពីនេះ Firewall តែងតែដំណើរការនូវ Network Address Translation (NAT) ។

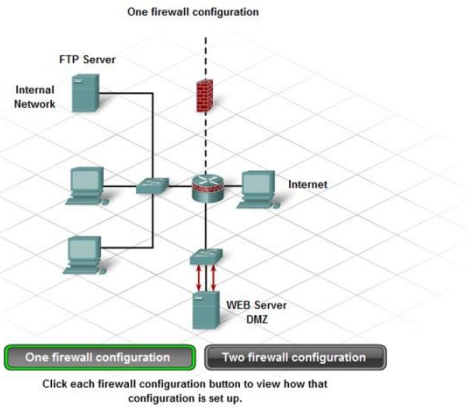


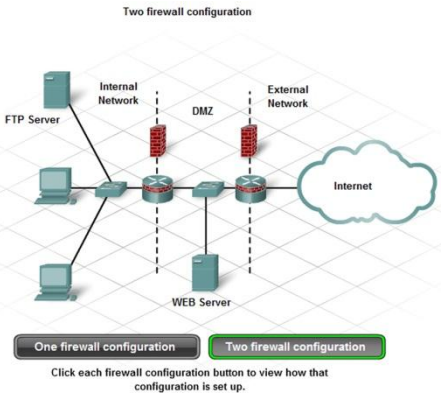
៥.២ ការប្រើប្រាស់ Firewall

Single firewall configuration

Single firewall ត្រូវបានចែកចេញពី ៣ប្រភេទ គឺ external network, internal network និង Demilitarized zone (DMZ) ។រាល់ការបញ្ជូនទិន្នន័យត្រូវបានបញ្ជូនទៅអោយ Firewall ពី external network ។បន្ទាប់មក Firewall បានតម្រូវអោយមានការអង្កេតទៅលើការបញ្ជូន និងកំណត់ថាតើ DMZ គួរតែត្រូវបានអោយឆ្លងកាត់ដែរឬទេ ថាតើវាត្រូវឆ្លងកាត់ដែលមានលក្ខណៈ internal ដែរឬទេ និង ថាតើ DMZ នោះគួរតែត្រូវបានច្រានចោលដែរឬទេ ។







Two firewall configuration

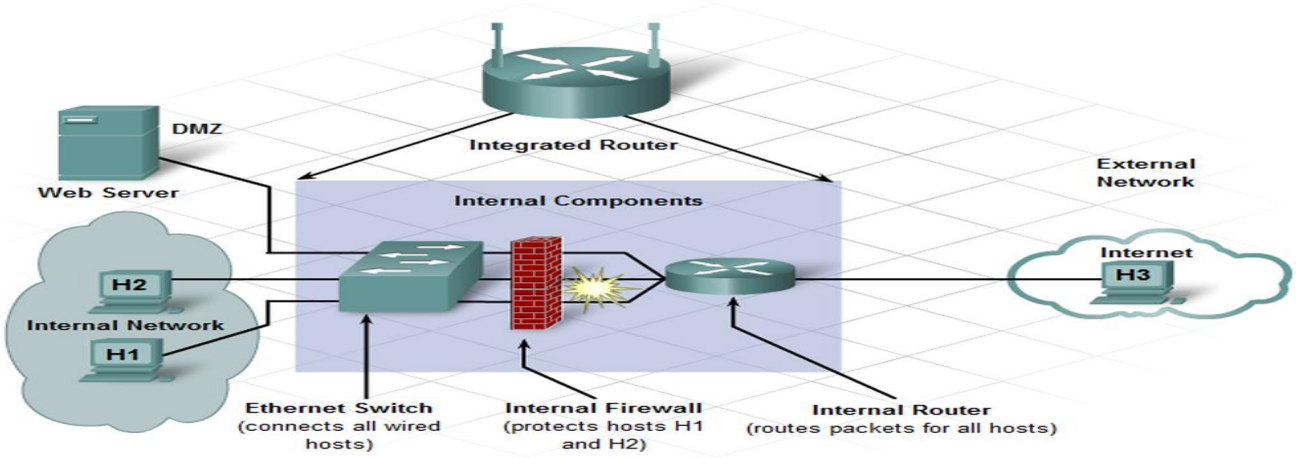
នៅក្នុង two firewall configuation មានទាំង internal និង external firewall ជាមួយនិង DMZ ដែលស្ថិតនៅចន្លោះរវាង internal និង external នេះ ។ External firewall មានភាពមិនតឹងតែង និង ការ អនុញ្ញាតអោយអ្នកប្រើប្រាស់ internet access ទៅកាន់សេរវ៉ាកម្មផ្សេងទៀតក្នុង DMZ ក៏ដូចជា ការ អនុញ្ញាតអោយបញ្ជូនទិន្នន័យដែលអ្នកប្រើប្រាស់ request អោយឆ្លងកាត់ ។ internal firewall មាន លក្ខណៈតឹងតែង និងការការពារប្រសើរជាង internal network ពីអ្នកប្រើប្រាស់ដែលយើងមិន ស្គាល់ រឺ ដឹង ។

Single firewall configuration មានភាពល្អប្រសើរសម្រាប់ជំនួញធុនតូច ។យ៉ាងណាមិញ two firewall configuration មានភាពល្អប្រសើរសម្រាប់អនុវត្តទៅលើជំនួញធុនធំ ដែលមានការបញ្ជូន ទិន្នន័យ និង network ដែលស្មាគស្មាញ ។

សំភារៈ network ជាច្រើននៅតាមផ្ទះ ដូចជា integrated routers ជាទូទៅរួមបញ្ចូលនៅកម្មវិធី Multi function firewall ។Firewall ប្រភេទនេះ ផ្តល់អោយនូវ Network Address Translation (NAT), Stateful Packet Inspection (SPI), IP, DMZ Application និង web site filtering ។

ពេលដែល DMZ ត្រូវបានបើក ក្នុងទម្រង់ធម្មតា នៅផ្នែកខាងក្រៅ Host អាច access ទៅគ្រប់ port នៅលើ Server ដូចជា 80 (HTTP), 21 (FTP), និង 110 (Email POP3) ។

Wireless access point ក្នុង integrated router ត្រូវបានចាត់ទុកថាជា internal network ។វាពិតជា មាន សារៈសំខាន់ណាស់ក្នុងការយល់ដឹងថា wireless access point មិនមានសុវត្ថិភាពនោះឡើយ អ្នក ដែលភ្ជាប់ទៅ wireless ដែលមានតែការការពារផ្នែក internal network និងនៅក្រៅ firewall ។ Hacker ទាំងឡាយអាច access ទៅ internal network និងឆ្លងកាត់នូវ Security ទាំងអស់ដោយ ងាយស្រួល ។



៥.៣ Vulnerability Analysis

ស្របជាមួយការប្រើប្រាស់នៅ Firewall គេក៏ឃើញមានកម្មវិធី រឺ Tool សម្រាប់តេស្ត host និង network security ដែលគេស្គាល់ថាជា network scanner ហើយជួយបង្ហាញនូវតំបន់ណាដែលអាចវាយប្រហារសុវត្ថិភាព និងផ្តល់នូវជំនួយជាជំហានៗក្នុងការទទួលនូវរាល់ពត៌មានដែលប៉ះពាល់ កុំព្យូទ័រ ។បើទោះជាសមត្ថភាពរបស់ Vulnerability Tool មានសភាពខុសៗគ្នា តាមការបង្កើតរៀងៗខ្លួនរបស់ក្រុមហ៊ុន តែពួកវាក៏មានលក្ខណៈរួមជាច្រើនដូចខាងក្រោម ៖

- ចំនួន host ដែលអាចកំណត់នៅក្នុង network
- ផ្តល់នូវ service host ជាច្រើន
- ភាពត្រូវគ្នា របស់ OS និង Version និងលើ host
- ប្រើប្រាស់នូវ Packet filter and firewall