Part 1

Pananda ng mga hakbang laban sa ilegal na access

Maayos ba ang inyong personal computer?
(Para sa mga gumagamit ng personal computer)

Hindi awtorisadong pag-access

Ang ilegal na access ay nangangahulugan ng hindi awtorisadong pag-access sa isang network na ipinatupad noong ika-13 ng Pebrero, 2000 sa ilalim ng Act on the Prohibition of Unauthorized Computer Access (Unauthorized Computer Access Law) (*1). Ito ay isang gawain o akto na tulad ng mga nababanggit sa ibaba.

- Akto o gawain na nag-aaccess sa kontrol (*3) ng isang computer at sumasalakay dito sa pamamagitan ng kahinaan (security hole) (*2) ng OS, application, o hardware ng computer (akto ng pagsalakay).
- Paggamit ng user ID o password ng isang tao (*4) nang walang sapat na pahintulot mula sa may-ari nito upang gumamit ng serbisyo na nakalaan para sa may-ari ng account ("Spoofing Act").
- Pagbibigay ng user ID at password ng isang tao sa ikatlong partido nang walang pahintulot mula sa may-ari nito.

Ang bookmark na ito ay para sa mga gumagamit ng personal computer. Tandaan na ito ay hindi sapat upang maiwasan ang ilegal na access sa network ng kumpanya (organisasyon), kaya't kinakailangan ang ibayong pag-iingat.

Halimbawa, ganitong istorya

・Patibong ng password

Si Ginoong A ay madalas na lumalahok sa mga Internet auction at siya ay madalas na bumibili at nagbebenta ng mga baseball cards. Ginamit ni Ginoong A ang kanyang pangalan bilang password upang hindi niya malimutan ang kanyang user ID at password sa tuwing maglolog in siya sa isang auction.

Isang araw, nang sinubukan niyang mag-log in sa isang auction, lumabas ang mensahe na "Password is different" (na nangangahulugan na iba ang password para sa account) at kahit ilang beses pa niya itong sinubukan, hindi talaga siya makapag-log in. At dahil sa wala naman siyang naaalala na nagpalit siya ng password, nakipag-ugnayan siya sa kumpanyang nangangasiwa sa auction, at mula sa kanila, napag-alaman niya na napalitan nga ang kaniyang password.

Ito ay resulta ng paggamit ng madaling password. Ang password na ginamit niya sa auction ay madaling hulaan kaya't ito ay madaling nanakaw.

・Patibong ng palaging bukas na koneksyon

Si Ginoong B ay gumagamit ng Internet para sa kaniyang CATV (cable TV). Dahil sa wala naman dagdag na bayad para sa koneksyon ng Internet, hindi siya nag-aalala sa panahon na siya ay nakakonekta dito, kaya't ito ay hinahayaan lamang niya na bukas.

Hindi mahalaga para kay Ginoong B ang seguridad at hindi siya nagsasagawa ng mga update (Microsoft Update at iba pa) na nagtatama sa mga security hole (kahinaan).

Hanggang sa isang araw, nang gagamitin na ni Ginoong B ang kanyang koneksyon, nakatanggap siya ng mensahe na "suspending access immediately and carrying out required management, since a certain government organization is attacked from Mr. B's personal computer" (nangangahulugan na ang access sa internet ay sinuspinde at nagsasagawa ng kinakailangang imbestigasyon dahil sa mayroong isang organisasyon ng pamahalaan na inatake gamit ang personal computer ni Ginoong B), mula sa isang organisasyon ng seguridad ng impormasyon at koneksyon. Dali-daling pinutol ni Ginoong B ang kanyang koneksyon sa Internet.

Dahil sa palaging konektado sa internet ang personal computer ni Ginoong B, ito ay nasa isang walang kalabang-labang estado, lingid sa kaalaman ni Ginoong B, at dahil sa estadong nagamit ng kawatan ang nasabing personal computer sa pag-atake sa iba.

・Patibong ng wireless LAN

Ang pamilya ni Ginoong C ay gumagamit ng dalawa o higit pang personal computers. Dahil sa nais gamitin nang bawat miyembro ang kanilang sariling personal computer sa kanilang sariling silid, napagdesisyunan nila na gumamit na lamang ng wireless LAN, na magbibigay sa bawat computer ng kakayanan na kumonekta sa Internet nang hindi gumagamit ng LAN cable. Nang magkaroon sila ng kagamitan para sa wireless LAN, hindi nila binasa ang mga direksyon sa paggamit nito, basta na nila ginamit ang nasabing kagamitan nang walang binabago sa mga settings nito.

Matapos ang ilang linggo ng paglalaro ng mga online games, napansin nila na naging mabagal ang kanilang personal computer, at bagamat hindi ginagamit ang personal computer, patuloy pa rin na nagbi-blink ang access lamp ng hard disk nito.

Isang araw, may dumating na bill mula sa kumpanya ng credit card. Nang suriin ang nasabing bill, nakasaad rito na ang kanilang credit card ay ginamit para sa online shopping, ngunit ni isa sa kanilang pamilya ay walang naaalala na ginamit ito.

Ang numero at impormasyon ng credit card ni Ginoong C ay naka-save sa kanilang mga personal computer upang magamit ito sa online shopping nang sinumang miyembro ng kanyang pamilya, ngunit dahil sa hindi maayos ang seguridad ng kanilang kagamitan para sa wireless LAN, ang nasabing file ay na-access ng ibang tao at ginamit para sa online shopping.

Sa kasong ito, ang naging sanhi ng ilegal na access sa kanilang computer ay ang "madaling password at setup", "hindi pagkakaayos sa security hole o kahinaan ng seguridad", at "madaling kontrol sa access". Ang halimbawang ito ay maaring mangyari sa sinumang gumagamit ng Internet. Kaya't simula ngayon, gamitin ang mga hakbang laban sa seguridad upang maayos at matiwasay na magamit ang koneksyon sa Internet.

1. Gamitin ang Update program (patch) (mga hakbang laban sa pagsalakay)

Ang mga depekto (kahinaan) sa seguridad ng mga OS, tulad ng Windows, Macintosh, Linux, at mga Internet browser tulad ng Internet Explorer, Firefox at iba pa ay maaring maging sanhi ng mga problema sa seguridad.

Ang depekto sa seguridad ay tinatawag na security hole (kahinaan). Kung ang ginagamit na OS at application ay mayroong security hole, ito ay mas madaling pasukin ng virus at mas madaling ilegal na ma-access, dahil dito, mas malaki rin ang panganib na manakaw o mabura ang mga personal na data at impormasyon ng may-ari.

Upang maiwasan ang ganitong uri ng panganib, mahalaga ang paggamit ng update program (patch) na siyang mag-aayos sa anumang security hole ng OS o application. Ang update program ay isang uri ng program na ginawa ng mga lumikha ng software na naglalayon na magawa o maisaayos ang mga security hole.

Para sa mga gumagamit ng Windows, i-set ang automatic update na makikita sa Microsoft Update. Ang patch na ipinamamahagi ng Microsoft Corp. ay para sa OS, Internet Explorer, mga programa ng Microsoft Office, at iba pa.

- **Microsoft Update**
  http://www.update.microsoft.com/microsoftupdate/v6/

Mababasa mula sa Website na makikita sa ibaba ang mga direksyon kung paano ito gamitin.

- **Paano ang gamitin ng Microsoft Update**
  http://www.microsoft.com/japan/protect/computer/updates/mu.mspx

.

2. Ingatan ito bagamat ito ay isang password lamang (hakbang laban sa spoofing).

Ang mga information system (serbisyo) ay humihingi mula sa bawat indibidawal (ikaw) na gumagamit nito ng kombinasyon ng user ID at password. Bagamat mayroon ilang information system na nagtatalaga ng kakaibang user ID para sa bawat indibidwal, ang bawat indibidwal na ito naman ang siyang lilikha ng sarili nilang password (magpapalit). Kapag ang user ID at password ay ibinigay ninyo sa iba o nanakaw mula sa inyo, maari itong gamitin ng ibang tao sa pagpapanggap bilang kayo upang magkaroon ng access sa pinangangalagaan ninyong information system.

Sa pamamagitan nito, maaring ma-access ang inyong online bank, kung saan maari silang makapag-withdraw o di kaya naman ay magamit ang inyong account sa pagsali sa mga online auction, kung saan kayo ang magbabayad para sa mga mamahaling bagay o kagamitan na kanilang bibilhin.

Ang kombinasyon ng inyong User ID at password ang tanging paraan ng isang information system upang kayo ay makilala kaya't siguruhin na hindi ito madaling hulaan, huwag na huwag rin itong ipapaalam sa iba, at regular na palitan ang inyong password.

Halimbawa ng paggawa ng password:

(1) Pagsamahin ang malalaki at maliliit na letra, numero, at pananda. Pagsama-samahin ang mga pananda (!, #, at iba pa), numero, at mga character ng alpabeto sa pamamaraan na tumutugma sa pamantayan ng inyong sistema.

(2) Mahabang password
Mahigit sa walong letra

(3) Gumamit ng password na hindi ninyo malilimutan at mahirap hulaan. Mas makababuti kung ang pagkakaayos ng mga character ay walang layunin at walang kahulugan.

Mga hakbang laban sa pagnanakaw ng password:

(1) Regular na palitan ang password.
(2) Huwag itong isulat sa isang papel.
(3) Huwag i-save sa personal computer.
(4) Huwag itong ipaalam sa ibang tao.

3. Mga pag–iingat sa oras ng koneksyon sa Internet (mga hakbang laban sa pagsalakay)

Kapag ang personal computer ay nakakonekta sa Internet sa bahay o ibang lugar, ito ay maaring nasa estado na madaling ilegal na ma–access (akto ng pagsalakay), batay sa pamamaraan ng koneksyon.

Sa mga koneksyon na gumagamit ng pampublikong linya (linya ng telepono na naglalaman rin ng koneksyon para sa mobile phone) at modem, tumataas ang posibilidad na ilegal na ma–access ang inyong personal computer kapag kayo ay konektado sa Internet. Sa mga ganitong pagkakataon, pinapayuhan namin kayo na gumamit ng security software para sa seguridad ng inyong personal computer.

Sa mga koneksyon na gumagamit ng ADSL line at modem, ang mga makabagong ADSL modem ay kadalasan mayroon na rin router function. sa pamamagitan ng router function na ito, bumababa ang panganib na ilegal na ma–access ang inyong mga personal computers kapag konektado na sa Internet, ngunit kapag ang setup ng nasabing router function ay mali, tumataas naman ang posibilidad na ilegal na ma–access ang inyong personal computer. Kung iseset ninyo ang router function sa ganitong pamamaraan, gumamit ng software para sa seguridad magbibigay ng proteksyon sa inyong personal computer mula sa ilegal na pag–access na ipapaliwanag sa mga susunod pang bahagi.

Kapag ang personal computer ay direktang nakakonekta sa Internet, at walang ibang dinadaan na kagamitan na tulad halimbawa ng isang CATV circuit o cable modem, o koneksyon na gumagamit ng fiber optics circuit at VDSL modem, mas mataas ang posibilidad na ilegal itong ma–access mula sa panig ng Internet.

Kapag ang personal computer ay direktang nakakonekta sa Internet, mataas ang posibilidad na ilegal itong ma–access mula sa panig ng Internet.

Sa ganitong pagkakataon, inirerekomenda namin ang paggamit ng router o firewall apparatus. Gayunpaman, ang mga ganitong uri ng kagamitan ay makakatulong lamang kung ito ay naaangkop sa inyong koneksyon at maayos ang setup. Kung mali ang setup ng router o firewall apparatus, tumataas ang posibilidad ng ilegal na ma–access ang inyong personal computer. Sa pagse–setup, gumamit ng software para sa seguridad na magbibigay ng proteksyon sa inyong personal computer mula sa ilegal na pag–access na ipapaliwanag sa mga susunod pang bahagi.

Sa mga lugar kung saan maraming iba't–ibang tao ang gumagamit ng iisang LAN, tulad halimbawa ng mga pampublikong wireless LAN hot spot, LAN–access sa mga hotel, at iba pa, maari kayong salakayin ng ibang gumagamit ng parehong LAN habang gumagamit kayo ng Internet. Sa mga ganitong pagkakataon, gumamit ng software para sa seguridad na magbibigay ng proteksyon sa inyong personal computer mula sa ilegal na pag–access na ipapaliwanag sa mga susunod pang bahagi.

4. Setup para sa pag–iwas sa ilegal na access

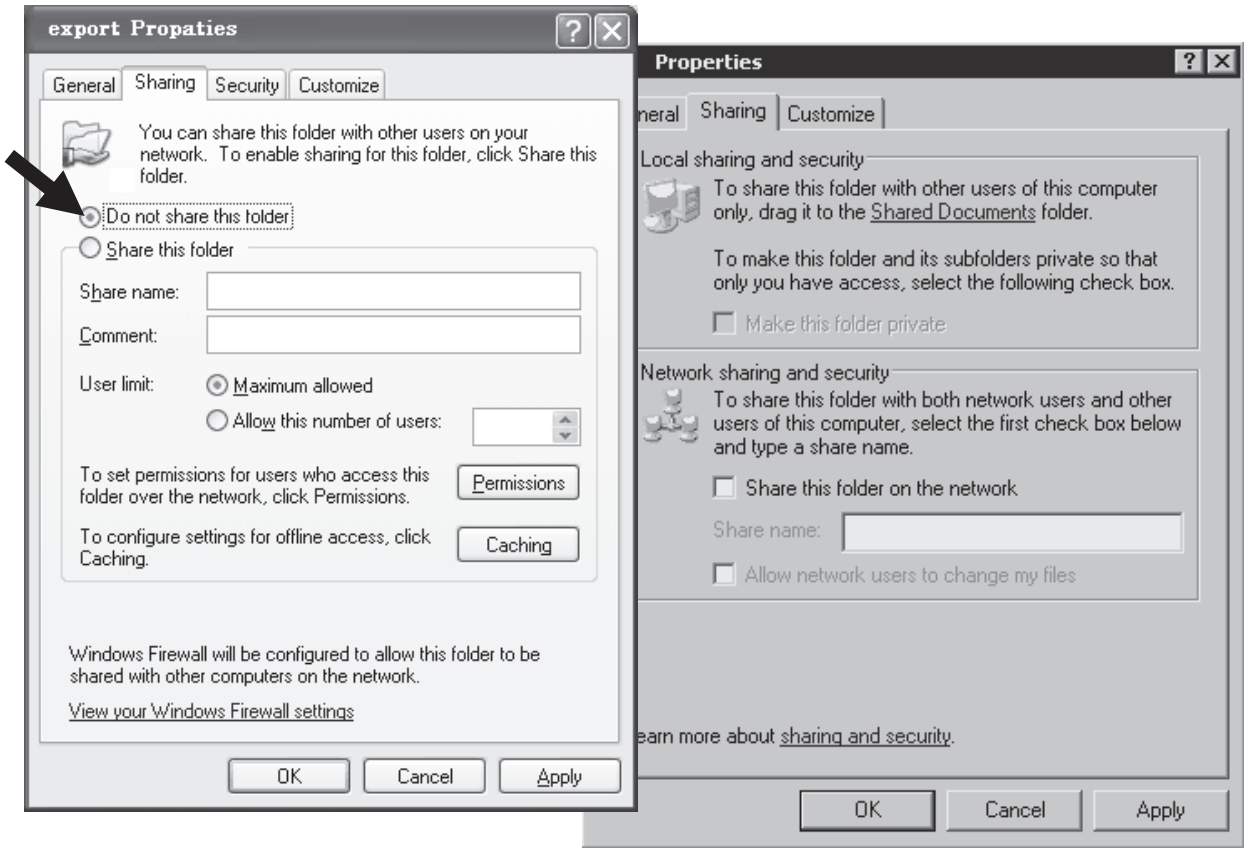
① Kanselahin ang file sharing setup.

Kung ang isang personal computer ay nakakonekta sa isang LAN sa isang hotel, ang buong network ay makikita sa My Network, at lahat ng mga folders sa ibang personal computer na nakakonekta sa parehong LAN ay maaring makita. Ito ay dahil sa ang kanilang file sharing setup ay naka–set sa ganitong paraan. Sa ganitong setup, para mo na ring sinasabi na “Tingnan ninyo ang mga laman ng aking personal computer”. Kapag konektado kayo sa isang LAN na mayroong iba’t–ibang gumagamit, pansamantalagang kanselahin ang inyong file sharing.

Kapag ang sharing setup ng isang computer ay gumagana, ang icon ng nasabing folder ay magiging katulad ng hitsura ng icon na makikita sa kaliwa.

Upang makita ang setting para sa sharing ng isang folder, itapat ang inyong mouse pointer sa folder, “right click” →″Properties″ → ″Sharing″.

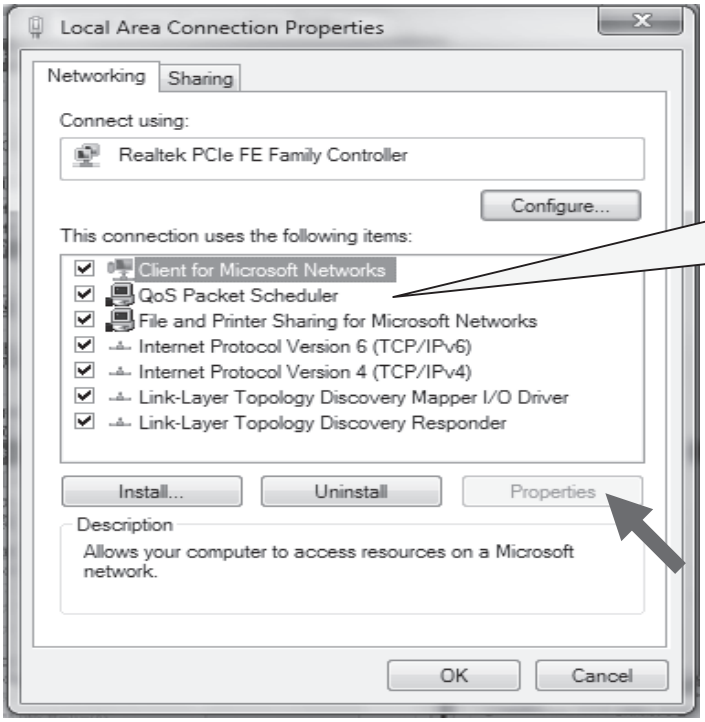
Kapag ang gamit na OS ay Windows XP Professional Edition, makikita ninyo ang screen na tulad ng nasa kaliwa [Tandaan na kung Windows XP Home Edition ang ginagamit, iba ang inyong makikita (screen sa kanan)].



② Pagpapalit ng settings ng Local Area Connection.

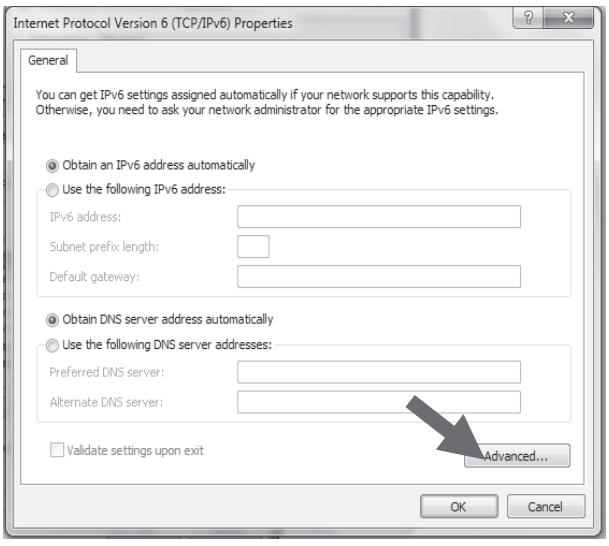
Higit sa rito, inirerekomenda namin na palitan ang setting ng inyong Local Area Connection, at huwag palabasin ang inyong personal computer sa Microsoft Windows Network.

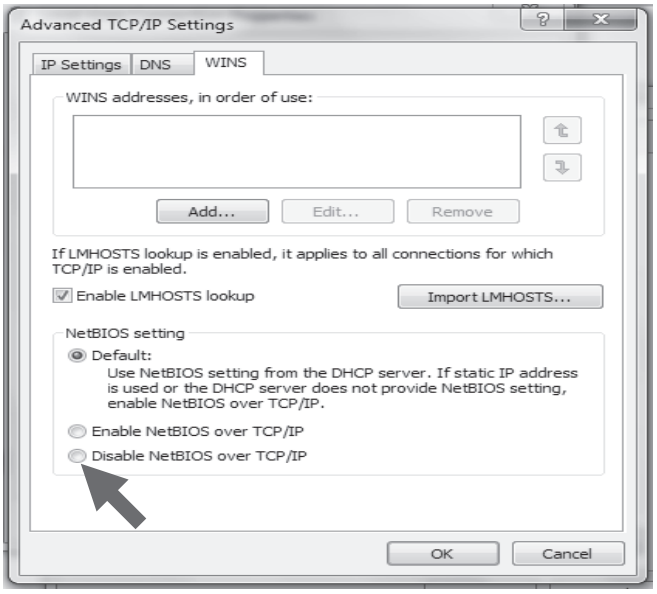
Pamamaraan ng paggawa:
"Start" → → "Control Panel" → "Network and Internet Connections" → itapat ang mouse pointer sa "Local area connection" at pindutin ang right-click → "Properties" → "Local Area Connection Properties"



Tanggalin ang mga tsek sa mga checkbox maliban sa checkbox ng "Internet Protocol (TCP/IP)".

Matapos piliin ang "Local Area Connection Properties" → Piliin ang "Internet Protocol (TCP/IP)" → i-click ang "Advanced" → i-click ang "WINS" → piliin ang "Disable NetBios over TCP/IP"





(Mga Tala)

Huwag kalilimutang ibalik sa orihinal ang mga settings kapag gamit na ninyo ang network na madalas o sadya na ninyong ginagamit.

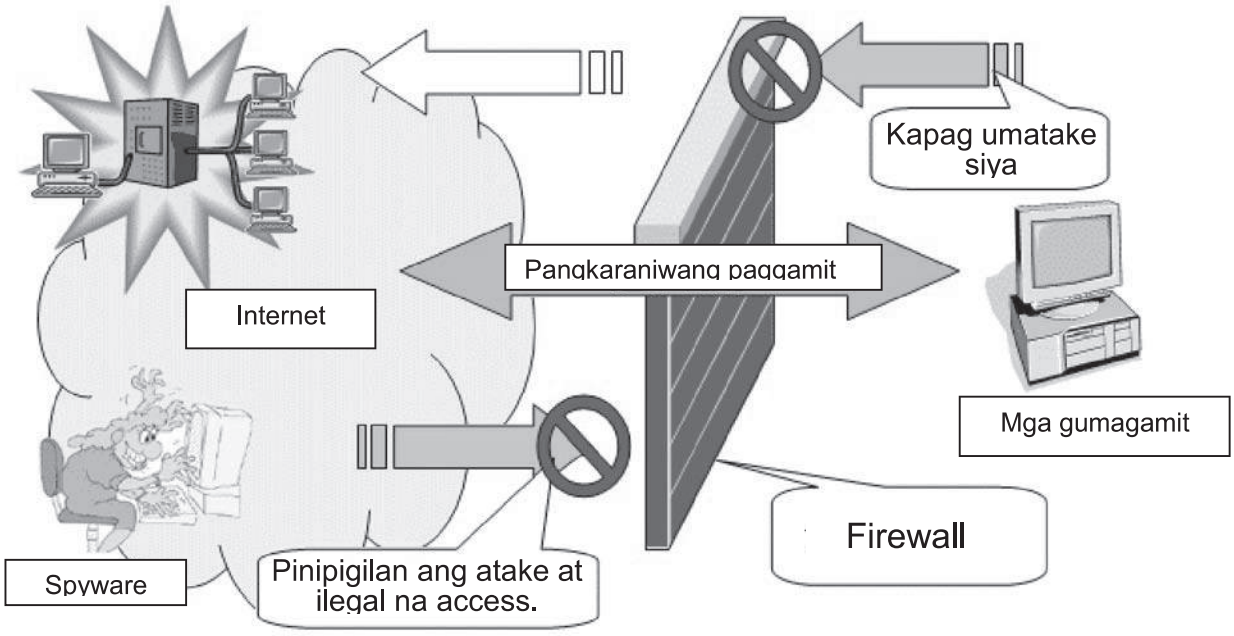
Kapag isinagawa ninyo ang setup na nauna nang ipinakita, hindi ninyo magagamit ang file sharing sa isang network printer o isang network.

Kung hindi kayo gumagamit ng network printer o file sharing, walang magiging problema sa paggamit ng setup na ito.

5. Rekomendasyon ng paggamit ng firewall software (integrated security software)

Ang firewall ay isang mahalagang kagamitan laban sa ilegal na access. Maliban sa paggamit ng mga anti-virus at anti-spyware software, inirerekomenda namin ang paggamit ng integrated security software ng isang OS o firewall o isang personal na firewall software. Binabantayan ng firewall ang pagpapalitan ng mga data na namamagitan sa isang personal computer at Internet. Kapag may napansin itong data o file na maaring makasama sa personal comouter, poprotektahan nito sng personal computer sa pamamagitan ng paghadlang o pag-block sa nasabing file o data.

Higit sa rito, kung halimbawang gumamit kayo ng isang personal computer na mayroong spyware, at sinubukan ng spyware na ito na magpadala ng inyong personal na impormasyon sa ibang personal computer, magpapakita ng babala ang firewall, sa pamamagitan nito, maiiwasan ang higit pang pinsala.

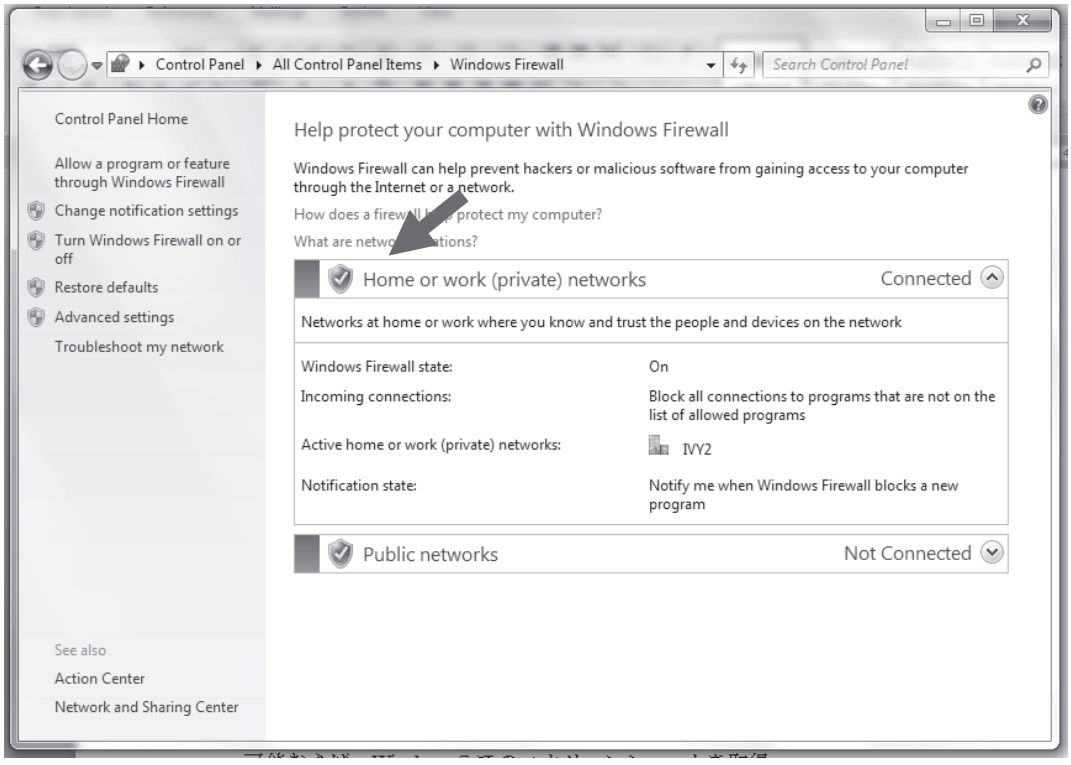


Sa mobile environment, hindi gumagamit ng router o firewall, dahil dito, pinapayuhan namin kayo na gamitin ang firewall function ng inyong personal computer o mag-install kayo ng isang integrated security software na mayroong sariling firewall.

Kung Windows XP ang ginagamit ninyo, inirerekomenda namin na gamitin ninyo ang Windows firewall na kasama ng OS.

Bagamat may kakayahan ang Windows firewall na i-block o hadlangan ang masasamang program mula sa Internet, hindi naman nito kaya na i-block o hadlangan ang anumang masamang program na nasa loob na mismo ng inyong personal computer (sa Windows Vista, sunod na OS sa Windows XP, ang pag-block o paghadlang sa mga atake mula sa magkabilang panig ay posible na). Gayunpaman, epektibo pa rin ang pag-atake sa mga kahinaan ng OS at mga applications na ginagawa ng mga masasamang-loob. Kaya kung hindi ninyo ginagamit ang integrated security software o firewall na may kakayahan na gumamit ng personal na firewall software, inirerekomenda namin na gamitin na ninyo ang feature na ito.

Pamamaraan ng Paggawa:
"Start" → "Control Panel" → "Windows Security Center" → "Windows firewall"



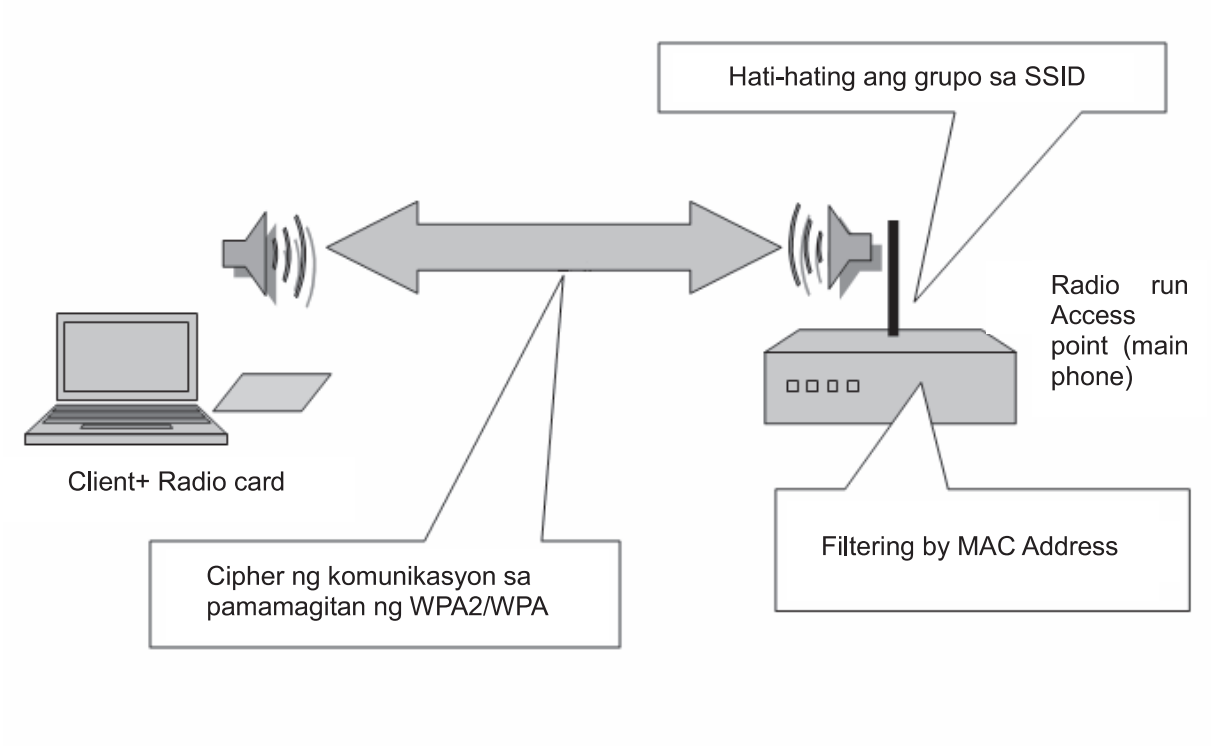
6. Pundasyon ng Wireless LAN

Ang wireless LAN ay isang maginhawang kaayusan ng network na maaring gamitin sa bahay man o opisina.

Ang kagamitan para sa wireless LAN ay naglalabas ng mga electric waves, na siyang magsisilbing signal para sa mga personal computers upang makakonekta ang mga ito sa Internet. Sa ganitong kaayusan, hindi na kinakailangan pang gumamit ng mga network cable. Gayunpaman, kapag hindi isinaayos ang security setup ng ganitong kaayusan, mayroong panganib na manakaw ang impormasyon na nilalaman ng mga personal computers nang hindi napapansin ng nagmamay–ari ng mga ito.

Ang mga makabagong kagamitan para sa wireless LAN ay mayroong security setup na kailangang ayusin.

Sa pamamagitan ng mga paalalang nakalista sa ibaba, makasisiguro kayo na magagawa ninyo ang mga kinakailangang hakbang (para sa mga detalye, basahin ang mga manwal ng instruksyon na kasama ng inyong kagamitan para sa wireless LAN).



■ **Wireless LAN access point (pangunahing telepono)**

☐ I-set ang WPA2/WPA (*5).

* Dahil sa mga kahinaan na natuklasan sa WEP (*6), huwag na itong gamitin.

☐ I-set ang SSID (*7)

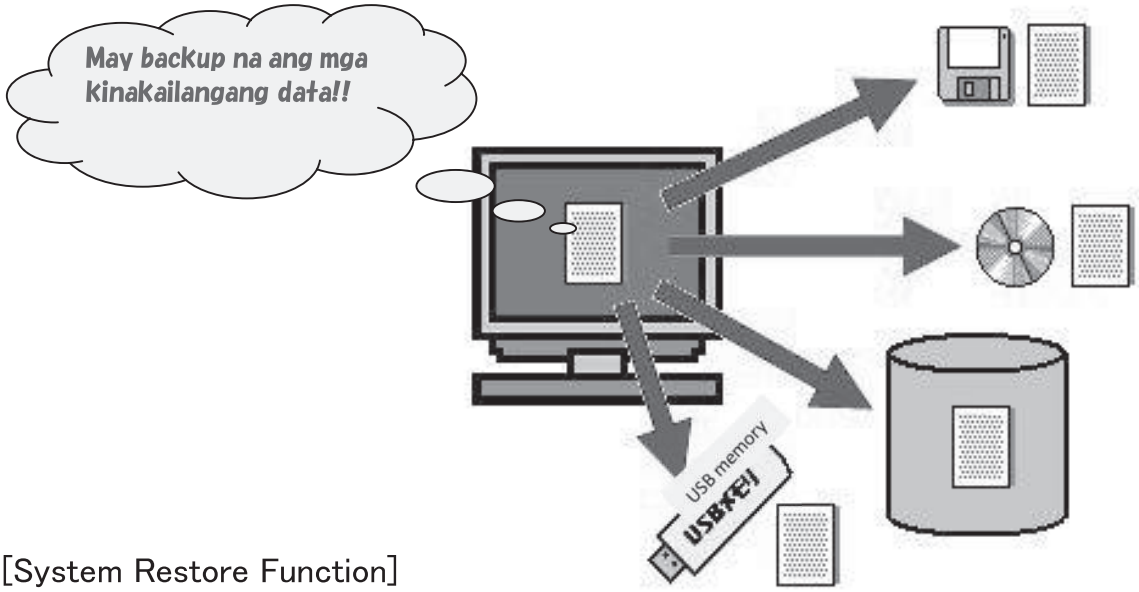
☐ I-set ang Filtering by MAC Address (*8).

☐ Tanggihan ang anumang koneksyon tangka ng koneksyon mula sa mga hindi kilalang terminal.

■ I-set ang personal computer sa paraan na tutugma sa settings ng access point.

7. Siguruhin na mayroon kayong back up ng mga data para sa panahon ng emerhensiya

Kapag ang isang personal computer ay nagkaroon ng malicious program o ang system ay nabago, o kung ito ay ilegal na ma-access ng iba (nasalakay), may mga pagkakataon na kinakailangan itong ibalik sa dati o i-restore. Ugaliin ang pagba-back up ng inyong mga data araw-araw. Higit sa rito, itabi ang orihinal na CD-ROM na naglalaman ng mga orihinal na application. Kapag ang mga nilalaman ng hard disk ay nasira mula sa ilegal na access, dapat itong ibalik sa dati o i-restore sa pamamagitan ng pagre-reinstall mula sa orihinal na CD-ROM, at iba pa.



[System Restore Function]

Ang Windows XP ay may kakayahan na ibalik sa dati o i-restore ang system. Kapag ang function na ito ay ginamit, maaring ibalik ang system sa dati nitong estado.

Halimbawa, kapag ang system ay nabago sa pamamagitan ng ilegal na access (nasalakay), maari itong ibalik sa dating estado bago ito binago sa pamamagitan ng

System Restore. Kapag mayroon kayong file o program na ginamit at sa palagay ninyo ay mayroong kakaiba sa operasyon nito, inirerekomenda namin na gamitin na ninyo ang System Restore. Tingnan ang mga sumusunod na sites para sa detalyadong hakbang.


Paraan (Microsoft Corp.) ng pagbabalik sa dati o pagre-restore ng Windows XP gamit ang System Restore function.

http://support.microsoft.com/default.aspx?scid=kb;ja;306084

8. Kung magkaroon ng sira o pinsala…

Kung sa inyong palagay ay nagkaroon ng mga malicious program sa inyong personal computer mula sa ilegal na pag-access dito, isailalim muna ang nasabing personal computer sa inspeksyon sa pamamagitan ng isang updated na security software (anti-virus o anti-spyware software). Kapag hindi ninyo matanggal o maalis ang malicious program, maghanap ng impormasyon tungkol sa nasabing program mula sa website ng security software, at gawin ang mga hakbang (ng pagtatanggal) na makikita sa website.

Para sa mga walang security software, kung mayroong koneksyon sa Internet, maaring malaman ang pangalan ng malicious program sa pamamagitan ng paggamit ng libreng online scans (online check para sa malicious programs) na ibinibigay ng mga kumpanyang gumagawa ng security softwares. Kapag alam na ang pangalan ng malicious program, maghanap ng impormasyon tungkol dito mula sa parehong website na nagsagawa ng scan, at alamin ang mga hakbang na maaring gawin upang matanggal ang nasabing program.

9.Sanggunihing impormasyon

Sumangguni sa mga sumusunod na mga artikulo at hakbang.

- **Hakbang laban sa ilegal na access**
  http://www.ipa.go.jp/security/fusei/ciadr.html
- **FAQ o madalas na katanungan ukol sa ilegal na access ng computer**
  http://www.ipa.go.jp/security/ciadr/faq01.html
- **security at home : Ang computer ay protektado (Microsoft Corp.)**
  http://www.microsoft.com/japan/protect/

10. Pagpaliwanag ng mga salita

(*2) Kahinaan

Sa larangan ng information security, ang kahinaan ay tumutukoy sa mga pagkakamali o mahinang bahagi sa disenyo ng isang system, network, application, o protokol ng pagpagsasagawa na maaring maging sanhi ng hindi inaasahang pangyayari. Ito ay maaring kahinaan ng operating system o kahinaan ng isang application. Higit sa kahinaan ng applications, ang kakulangan ng security setup ay maari rin maging sanhi ng kahinaan ng buong system. Ito ay kilala rin sa tawag na security hole.

(*3) Access control (access control)

Sa computer security, ang may–ari o Administrator ang may kontrol kung sino ang bibigyan ng awtorisasyon o pahintulot na ma–access ang mga resources ng isang computer system.

(*4) User ID at password

Batay sa Act on the Prohibition of Unauthorized Computer Access, ito ay tumutukoy sa pagkakakilanlan ng isang gumagamit ng system. Bagamat maari rin gumamit ng marka, tatak ng daliri o fingerprint, lagda, tunog, anino, at iba pa, bilang pagkakakilanlan ng isang gumagamit, tanging user ID at password lamang ang ginagamit sa tekstong ito.

(*5) WPA2/WPA (Wi–Fi Protected Access)

Ito ay isang pamantayan ng seguridad para sa computer networks na nilikha ng Wi–Fi Alliance bilang kapalit ng WEP. Nilikha ito upang tugunan ang kahinaan ng WEP at mas palakasin ang seguridad.

Ang WPA2 ay mas bagong bersyon ng WPA na gumagamit ng AES (Advanced Encryption Standard), ito ay isang mas makapangyarihang algorithm.

(*6) WEP (Wired Equivalent Privacy)

Ito ay isang security algorithm na nilikha para sa IEEE na gumagamit ng RC4 algorithm bilang batayan.

Gayunpaman, maraming kahinaan ang natuklasan at naiulat tungkol sa WEP.

(*7) SSID (Service Set IDentifier)

Ito ay isang ID o pagkakakilanlan ng isang access point (AP).

Ito ay kilala rin sa tawag na ESSID.

(*8) MAC Address (Media Access Control Address)

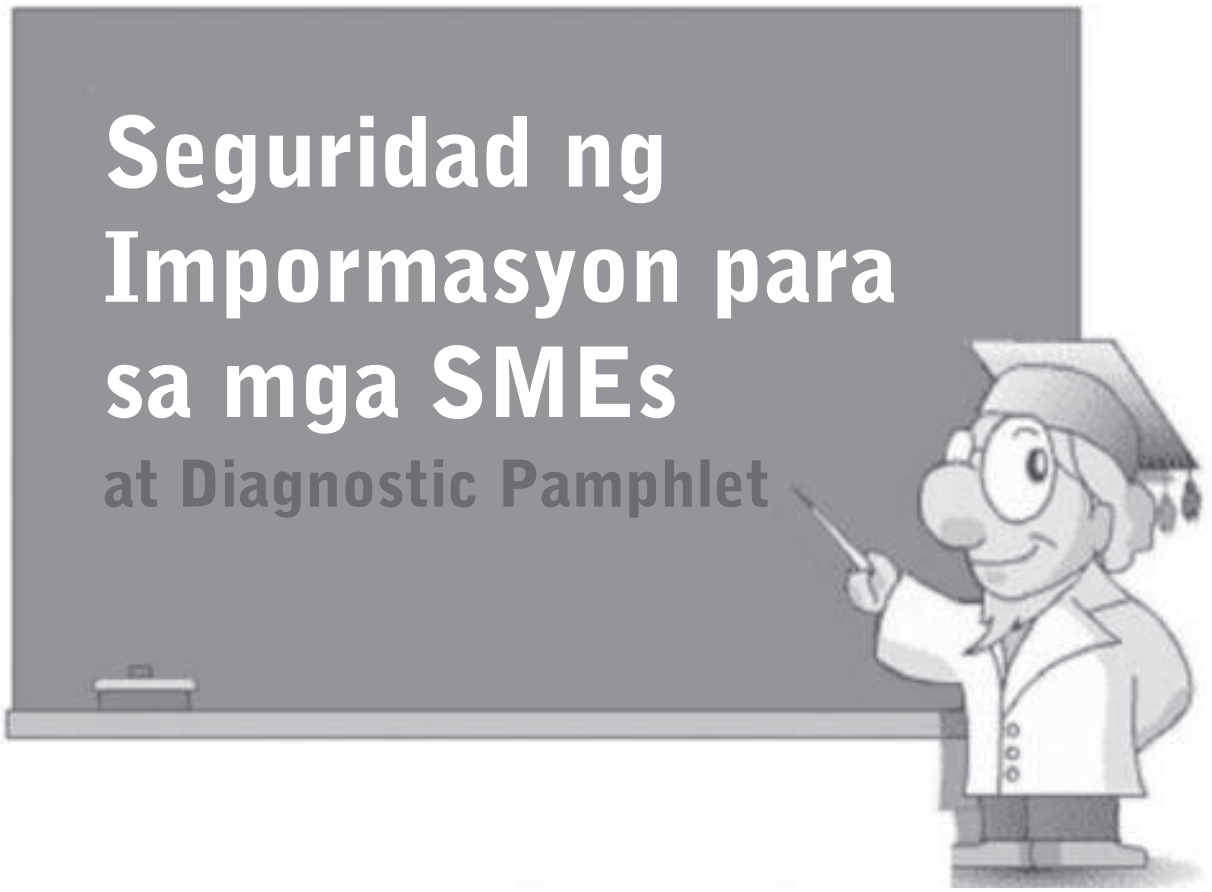
Isang walang katulad na ID o pagkakakilanlan na nakatalaga sa isang wireless LAN adapter (wireless headset).

* Ang mga datos na ito ay independyenteng administratibong ahensya. Ang mga datos na ito ay mula sa Information Technology Promotion Agency security center, na matapos isalin ng pamahalaang ng Japan, ay ipapamahagi sa bawat bansa na kabilang sa ASEAN.
Higit sa rito, ang paggamit, pagbabago, pagkopya, pagpapadala, at pagsasahimpapawid ng mga datos upang pagkakitaan na walang sapat na pahintulot mula sa pamahalaan ng Japan ay mahigpit na ipinagbabawal.
(Para sa mga katanungan: Information Security Center, Kalihiman ng Gabinete) （NISC）〒100-0014　2-4-12　Nagata-cho　poc@nisc.go.jp）

ASEAN・JAPAN
Information Security Awareness

Notes:

Part 2


Seguridad ng
Impormasyon para
sa mga SMEs
at Diagnostic Pamphlet

Bagong Edisyon

Para sa inyo, mga tagapangasiwa ng maliliit-at-katamtamang laki na negosyo

Limang minuto lang!

Para sa inyo, mga tagapangasiwa ng maliliit-at-katamtamang laki na negosyo

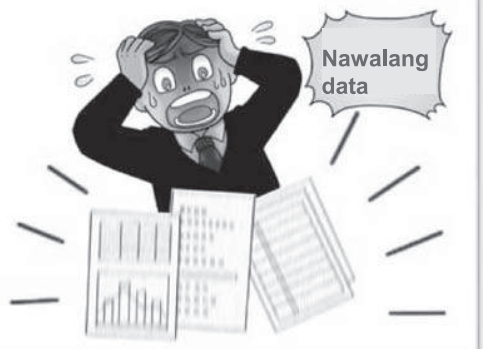
Ang maliit na pagkakamali ay maaring magdulot ng malaking problema!

Bukod sa abalang idudulot nito sa kustomer, dahilan rin ito upang mabawasan ang kanilang tiwala sa inyong kumpanya.

Dahil sa nalantad ang personal na impormasyon ng mga kustomer, mawawalan sila ng tiwala sa inyong kumpanya.

Ang kustomer ay mapapadalhan ng email na naglalaman ng virus na maaring maging sanhi ng suspensyon ng inyong negosyo!

Ang mga data tungkol sa bagong produkto ay nawala at mahuhuli ang pagbebenta nito!



Bago ang lahat, i-tsek ang sitwasyon ng seguridad ng inyong kumpanya sa loob lamang ng limang minuto gamit ang "Diagnostic Sheet ng Kumpanya!" !

Kaya itong gawin sa loob ng 5 minuto

Diagnostic sheet ng kumpanya

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo

Tungkol sa pamamahala ng impormasyon

Ano ang resulta ng ginawa ninyong tsek gamit ang diagnostic sheet para sa kumpanya? Ang mga aytem na pinili maliban sa “paglalabas” ay kinakailangang gawin batay sa mga hakbang na nakalarawan sa ibaba.

Bilang **1** sa diagnostic sheet ng kumpanya — Tungkol sa pag-iimbak

Ang mga kritikal na impormasyon na iniiwan lamang na nakakalat sa isang mesa ay nanganganib na manakaw ng iba. Kinakailangang itago at pangalagaan ang mga kritikal na impormasyon upang masiguro na walang ibang makakakita o makakakuha nito maliban sa mga taong dapat mangasiwa nito.

Halimbawa ng isang hakbang

Panatilihing malinis at maayos ang mesa. Gumamit ng isang aklatan o lalagyan na mayroong kandado.

Bilang **2** sa diagnostic sheet ng kumpanya — Tungkol sa paglalabas

Sa tuwing dadalhin ang mga kritikal na impormasyon papalabas ng opisina, mayroong panganib na ito ay manakaw o maiwala nang dahil sa kapabayaan.
Kung sa simula pa lamang ay lalagyan na ng password ang mobile phone at personal computer o ang data file at iba pa, maiiwasan na makita ng iba ang impormasyon sakaling manakaw o mawala mga ito.

Halimbawa ng isang hakbang

Kung dadalhin sa labas ang mga kritikal na impormasyon, gumamit ng security system, lagyan ng password ang notebook PC, USB memory, mobile phone, at personal digital assistant at mahigpit na pag-ingatan ang mga ito.

Bilang **3** sa diagnostic sheet ng kumpanya — Tungkol sa pagtatapon

Kung ang mga dokumentong naglalaman ng mga kritikal na impormasyon ay basta na lamang itatapon sa basurahan, ito ay maaring mapasakamay ng ibang tao na maaring maging sanhi ng aksidenteng paglabas ng impormasyon. Ang paggupit o paggamit ng shredder upang sirain ang mga dokumentong naglalaman ng kritikal na impomasyon ay isang hakbang upang maiwasan ang paglabas ng impormasyon at iba pa.

Halimbawa ng isang hakbang

Ang mga importanteng dokumento, CD, at iba pa ay hindi dapat basta itapon sa basurahan. Sirain muna ang mga ito gamit ang shredder at iba pa.

Bilang **4** sa diagnostic sheet ng kumpanya — Tungkol sa pagtatapon

Bagamat ang mga impormasyon na naka-save sa storage media na tulad ng personal computer at CD/USB memory ay nabura na gamit ang “delete function” at iba pa, maari pa rin muling maibalik ang mga ito gamit ang “restoration tool” at iba pa. Upang masiguro na nabura na o wala na ang mga nasabing impormasyon mula sa personal computer o storage medium, kinakailangang gumamit ng software na para sa pagbubura ng mga impormasyon.

Halimbawa ng isang hakbang

Itapon ang mga ito matapos na gamitin ang software o matapos itong ipasira sa isang espesyal na kontratista at iba pa.

Ayon sa inyo, “Walang “kritikal na impormasyon” ang aming kumpanya.” Ngunit wala bang data ang inyong kumpanya?

- Paraan ng pakikipag-ugnayan sa bisita o kustomer
- Adres at impormasyon tungkol sa suweldo ng mga empleyado
- Impormasyon tungkol sa accounting ng kumpanya
- Rekord ng mga transaksyon at halaga ng mga ito ng bawat kustomer
- Impormasyon tungkol sa mga bagong produkto na maaring malagay sa alanganin kapag napasakamay ng kalaban sa negosyo.
- Information which dealt with it from the customer and was called cautions

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo

Tungkol sa opisina

Bagamat mas kombenyente ang paggamit ng maliliit na personal computer, smart phone, at personal digital assistant, mas madali naman na manakaw ang mga ito. Ang mga kontrol sa kaligtasan ng isang opisina ang pangunahing pundasyon ng seguridad.

Bilang **5** sa diagnostic sheet ng kumpanya — **Tungkol sa opisina**

Ang impormasyon ay maaring manakaw kung hindi lilimitahan ang pagpasok ng ibang tao maliban sa mga taong may kaugnayan sa kumpanya. Kung mayroong hindi awtorisadong tao na kinakailangan lumapit sa server, silid-aklatan, o kaha-de-yero, pigilan sila mula sa paghawak ng kahit na ano.

Halimbawa ng isang hakbang

Kung mayroong hindi kilalang tao sa inyong opisina, kausapin ang mga ito at alamin kung ano ang kailangan, o kaya naman ay magtalaga ng isang resepsyonista.

Bilang **6** sa diagnostic sheet ng kumpanya — **Tungkol sa opisina**

Kombenyente ang pagdadala ng notebook PC, personal digital assistant, at USB memory, ngunit kaakibat ng kaginhawaang ito ang higit na panganib na manakaw ang mga ito. Itago ang mga ito sa inyong kahon kung kayo ay aalis.

Halimbawa ng isang hakbang

Ilagay ang notebook PC, personal digital assistant, at iba pang kagamitan (CD, USB memory, external hard disk, at iba pa) sa isang kahon kung kayo ay aalis.

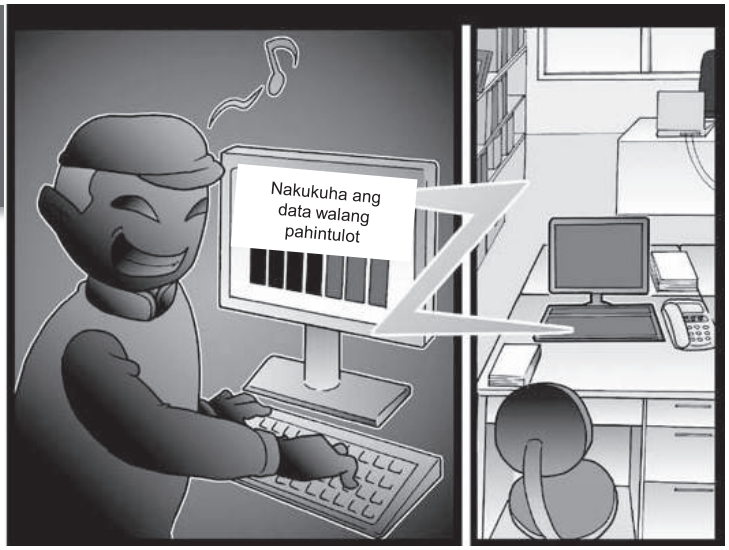
Bilang **7** sa diagnostic sheet ng kumpanya — **Tungkol sa opisina**

Makakatulong ang pagbibigay ng responsibilidad ng pagkakandado at pag-iiwan ng rekord ng oras ng pag-uwi sa pinakahuling tao na umaalis ng opisina. Maayos na pamahalaan ang pagkakandado at pag-rerekord.

Halimbawa ng isang hakbang

Ibigay ang responsibilidad ng pangangalaga ng susi, pagkakandado ng opisina, at pagre-rekord ng (oras, taong umalis) pag-alis at iba pa.

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo



Tungkol sa personal computer

Upang maprotektahan ang personal computer mula sa virus o ilegal na access, palawakin ang kaalaman ukol sa seguridad at regular na gawin ang mga hakbang laban dito.

Bilang **8** sa diagnostic sheet ng kumpanya — Tungkol sa personal computer

Kapag pinabayaan ang kakulangan o kahinaan sa seguridad (tinatawag na security hole), nagkakaroon ng panganib na magkaroon ng virus na magsasamantala sa kakulangan o kahinaang ito.

[Sanggunian]
Tungkol sa Windows Update, bumisita sa website ng Microsoft Corp.,
http//www.microsoft.com/security/.
Tingnan ang page ng Safety & Security Center.

Halimbawa ng isang hakbang

Siguruhing bago ang bersyon ng inyong software sa pamamagitan ng paggamit ng Windows Update at iba pang update program.

Bilang **9** sa diagnostic sheet ng kumpanya — Tungkol sa personal computer

Maraming impormasyon ang maaring aksidenteng mailabas sa pamamagitan ng mga file-trading software. Ang Winny, Share, at iba pa ay mga halimbawa ng ganitong uri ng software.

Halimbawa ng isang hakbang

Huwag gumamit ng file-trading software, tulad ng Winny at Share, kung kailangang gumamit nito, ituro ang tama at responsableng paggamit nito.

Bilang **10** sa diagnostic sheet ng kumpanya — Tungkol sa personal computer

Kapag hindi malinaw ang patakaran ng pangasiwaan ukol sa paggamit ng indibidwal na personal computer at personal computer ng kumpanya, magiging mahirap ang pagsisiguro ng seguridad. Sa simula pa lamang, magbigay ng malinaw na patakaran ukol sa paggamit ng indibidwal na personal computer at personal computer ng kumpanya, at huwag silang hayaan na gamitin ang personal computer ng kumpanya para sa ibang gawain maliban sa sadyang gamit ng mga ito.

Halimbawa ng isang hakbang

Kung hindi ipinagbabawal ang paggamit ng indibidwal na personal computer, gumamit ng license system, at iba pa.

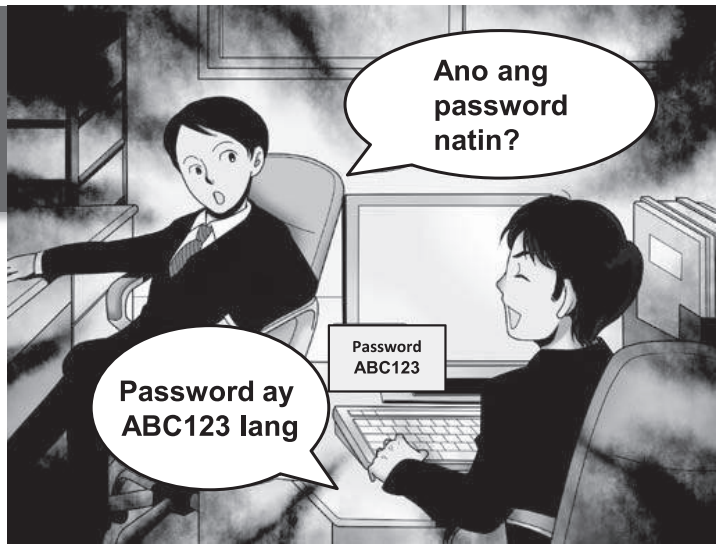
Bilang **11** sa diagnostic sheet ng kumpanya — Tungkol sa personal computer

Ang mga personal computer na maaring gamitin ng sinuman ay maaring maabuso. Magsagawa ng mga hakbang upang maprotektahan ang mga personal computer mula sa hindi awtorisadong paggamit.

Halimbawa ng isang hakbang

Huwag hayaang gamitin ng iba ang personal computer. Patayin ito o lagyan ng login password upang hindi magamit ng iba sa tuwing aalis kayo sa inyong upuan.

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo



Tungkol sa password at virus

Password ay ABC123 lang

Ang pagpapabaya sa password ay maaring maging sanhi ng aksidenteng paglabas ng impormasyon. Kaya't ingatan ito.

Bilang **12**,**13**,**14** sa diagnostic sheet ng kumpanya

Tungkol sa password

Siyasatin kung ang inyong password para sa paggamit ng mga serbisyo sa Internet ay madaling hulaan at maabuso. Isa sa mga sanhi ng nito ay ang paggamit ng madadaling hulaan na password tulad ng pangalan o kaarawan. Kapag nahulaan ng iba ang password, ang inyong account ay magagamit nila sa ilegal na paraan. Sa pamamagitan ng paggamit ng komplikadong password na binubuo ng pinaghalu-halong maliliit at malalaking letra, numero, at iba pang signs, at regular na pagpapalit ng password, maiiwasan ang kapinsalaang tulad nito.

Halimbawa ng isang hakbang

Kaagad na i-reset ang password na ginamit ng empleyado na nagbitiw na o regular na palitan ang password ng mga rehistradong empleyado, at iba pa.

Bilang **15** sa diagnostic sheet ng kumpanya

Tungkol sa virus

Dumadami ang mga virus na nagnanakaw ng ID, password, at numero ng credit card. Gumamit ng anti-virus software at mag-ingat sa pagpasok sa mga kahina-hinalang sites, o pagbubukas ng mga natatanggap na e-mail.

Halimbawa ng isang hakbang

Lagyan ng anti-virus software ang mga personal computer. Huwag magbukas o pumunta sa mga website na walang kaugnayan sa negosyo. Turuan sila na huwag magbubukas ng kahina-hinalang e-mail.

Its company diagnostic sheet No.**16**

Tungkol sa mga hakbang laban sa virus.

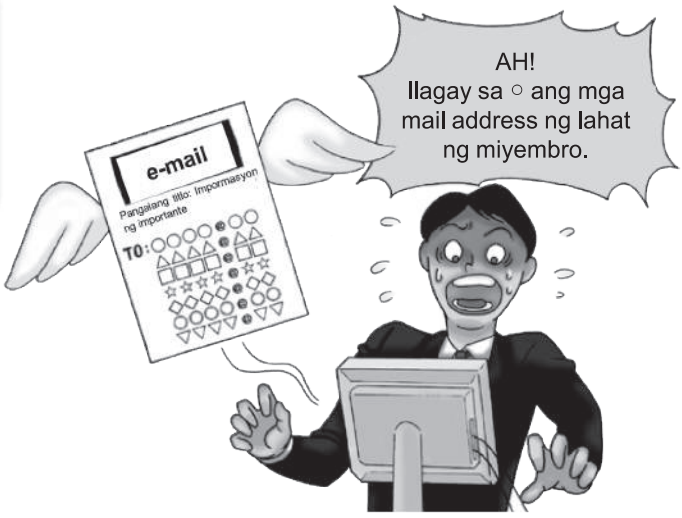
Dahil sa mayroong bagong computer virus na natutuklasan araw-araw, kapag hindi updated ang anti-virus software, mayroong panganib na magkaroon ng virus ang inyong personal computer. Siguruhin na palaging updated ang inyong anti-virus software.

Halimbawa ng isang hakbang

Ayusin ang setup ng inyong anti-virus software sa paraan na awtomatikong mag-aupdate ang virus definition file.

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo

Tungkol sa e-mail at backup



Ang pagpapadala ng maling e-mail ay maaring magdulot ng pinsala hindi lamang sa inyong sarili kundi pati na rin sa mga taong nakapaligid sa inyo.

Its company diagnostic sheet No.**17**

Tungkol sa e-mail

Maraming pangyayari kung saan ang mga mahahalagang impormasyon ay nalantad sa mga taong hindi naman dapat makaalam nito nang dahil sa maling E-mail address o numero ng FAX na napadalhan ng impormasyon. Siguruhin na tama ang E-mail address o numero ng FAX na papadalhan bago ipadala ang impormasyon.

Halimbawa ng isang hakbang

Bago ipadala o i-send ang E-mail o FAX, muling i-tsek ang address o numerong papadalhan.

Its company diagnostic sheet No.**18**

Tungkol sa e-mail

Ang aksidenteng pagbibigay sa ibang tao ng E-mail address ng iba ay isang uri ng aksidenteng paglalabas ng impormasyon. Kapag magpapadala ng E-mail sa dalawa o higit pang katao, ugaliing i-tsek ang mga E-mail address na papadalhan.

Halimbawa ng isang hakbang

Gamitin nang tama ang To, CC, at BCC.

Bilang **19** sa diagnostic sheet ng kumpanya

Tungkol sa e-mail

Kapag magpapadala ng kritikal na impormasyon sa pamamagitan ng e-mail, o magsusulat ng kritikal na impormasyon sa isang document file, at iba pa, protektahan ito gamit ang password, bago ito i-attach sa e-mail.

Halimbawa ng isang hakbang

Kapag magpapadala ng e-mail na naglalaman ng kritikal na impormasyon na nakapaloob sa isang file na protektado ng password, ipaalam ang password sa mismong tao na gagamit ng file sa pamamagitan ng pagtawag sa kanila sa telepono, at iba pa.

Bilang **20** sa diagnostic sheet ng kumpanya

Tungkol sa buckup

Ang mga data na naka-save sa personal computer ay maaring mawala nang dahil sa pagkasira nito, maling operasyon, at iba pa. Kung regular na gumagawa ng backup, maihahanda ninyo ang inyong mga sarili para sa mga hindi inaasahang sitwasyon na tulad nito.

Halimbawa ng isang hakbang

Regular na gumawa ng backup para sa mga files na naglalaman ng kritikal na impormasyon o itago ang backup sa ibang lugar maliban sa orihinal na lugar at iba pa.

Ang diagnostic pamphlet na ito ay para sa information security ng maliliit-at-katamtamang laki na negosyo

Tungkol sa mangagawa at kostmer

Napakahalaga na malaman at maunawaan ng isang empleyado ang kahalagahan ng information security, at pilitin na mapangalagaan ito sa araw-araw.

Bilang **21** sa diagnostic sheet ng kumpanya — Tungkol sa mangagawa

Bagamat ang pangangalaga at pananatiling lihim sa mga kritikal na impormasyon ng kumpanya ay sadyang kasama na sa mga patakaran sa trabaho at iba pa, kailangan pa rin na ipaunawa ito nang mabuti sa mga empleyado.

Halimbawa ng isang hakbang

Sa kaso ng pag-aampon, kailangang panatilihing lihim ang lahat ng impormasyon.

Bilang **22** sa diagnostic sheet ng kumpanya — Tungkol sa mangagawa

Ang impormasyon ay araw-araw na ginagamit at nakakasalamuha sa trabaho, dahil dito, madalas na napapabayaan ito ng pangasiwaan. Makabubuti na paulit-ulit na ipaalala sa mga empleyado ang kahalagahan ng pangangalaga sa mga ito.

Halimbawa ng isang hakbang

Mayroong mga pagpupulong na regular na isinasagawa upang ipaliwanag ang kahagalagan ng pag-kontrol sa mga impormasyon.

Bilang **23** sa diagnostic sheet ng kumpanya — Tungkol sa kostmer

Bago magbigay ng kompidensyal na impormasyon sa isang kustomer, kinakailangang siguruhin ang katauhan ng kustomer na pagbibigyan ng impormasyon. Ipinagbabawal ang pagbibigay ng mga sikreto o pribadong impormasyon sa ibang kasosyo.

Halimbawa ng isang hakbang

Mayroong gagawing kontrata kung saan nililiwanag ang mga pagiging sikreto ng mga nilalaman ng dokumento.

Bilang **24** sa diagnostic sheet ng kumpanya — Tungkol sa aksidenteng pagsusulatan

Bago magbigay ng kompidensyal na impormasyon sa isang kustomer, kinakailangang siguruhin ang katauhan ng kustomer na pagbibigyan ng impormasyon. Sa maikling pananalita, makakabuti na malaman ninyo ang inyong gagawin at kung kailan ito dapat gawin kung sakaling "mangyari sa inyong kumpanya ang mga pangyayaring inilalarawan".

Halimbawa ng isang hakbang

Gumawa ng isang manwal na naglalaman ng mga hakbang na dapat gawin sakaling may malantad o mapalabas, manakaw, o mawalang kritikal na impormasyon.

Bilang **25** sa diagnostic sheet ng kumpanya — Tungkol sa rule

Makikita sa diagnostic sheet na ito ng kumpanya ang halimbawa ng mga hakbang na isinasagawa upang makamit ang layunin ng B tulad ng "kung ginagawa ba ninyo ang mga hakbang na tulad ng A at iba pa." Ngunit sa pagkakataong ito, hindi ninyo alam na ang B ay talagang kinakailangan at kung ano ang dahilan kung bakit isinasagawa ang A. Kinakailangang linawin ang layunin at hakbang na kailangang isagawa. Ang mga hakbang na makikita dito ay naaangkop sa halimbawa na makikita sa A, ang mga hakbang na kailangan ay maaring maiba batay sa sitwasyon o kalagayan ng bawat kumpanya.

Halimbawa ng isang hakbang

Ilathala ang diagnostic sheet bilang 1 hanggang 24 sa bulletin board o intranet ng inyong kumpanya bilang hakbang laban sa banta sa information security.
2. Kung sa inyong palagay ay may problema ang kasalukuyang patakaran, baguhin ito at mas pagbutihin.

* Ang mga datos na ito ay independyenteng administratibong ahensya. Ang mga datos na ito ay mula sa Information Technology Promotion Agency security center, na matapos isalin ng pamahalaang ng Japan, ay ipapamahagi sa bawat bansa na kabilang sa ASEAN.
Higit sa rito, ang paggamit, pagbabago, pagkopya, pagpapadala, at pagsasahimpapawid ng mga datos upang pagkakitaan na walang sapat na pahintulot mula sa pamahalaan ng Japan ay mahigpit na ipinagbabawal.
(Para sa mga katanungan: Information Security Center, Kalihiman ng Gabinete) （NISC）〒100-0014 2-4-12 Nagata-cho poc@nisc.go.jp)

Diagnostic sheet ng kumpanya na ginawa sa

Limang minuto lang!

Ang diagnostic sheet ng kumpanya ay naglalayong ipabatid sa isang tao ang mga hakbang laban sa panganib sa information security

- Bago ang diagnosis, tingnan muna ang 1 sa likod.
- Basahin ang mga nilalaman ng diagnostic sheet at bilugan ang aytem sa kolumna na tumutugma sa inyong kasagutan.
- Kapag isinasagawa ng lahat ng empleyado , piliin ang "Isinasagawa ito".
- Ang sheet ay kinakailangang sagutan o punan ng mga tagapangasiwa o administrador.
- Kapag tapos na ang tsek, isulat ang kabuuang bilang sa pinakahuling bahagi.

Pangalan ng kumpanya

Pangalan ng sumulat

Petsa ng pagsagawa taon buwan araw

No	Diagnostic item	Nilalaman ng diagnostic	Check				Ito ay tumutugma sa diagnostic pamphlet ng kumpanya.
			Ang bahaging ito ay isinasagawa	Ang bahaging ito ay isinasagawa	Hindi ito isinasagawa	Hindi ko alam	
1	Tungkol sa pag-iimbak	Hindi ba kayo nag-iiwan ng anumang dokumento o kagamitan na naglalaman ng kritikal na impormasyon *1 sa mesa, sa halip, ito ay itinatago sa isang lalagyan o silid-aklatan na mayroong susian?	4	2	0	0	P1 No.1 Ginagamit itong sanggunian para sa pag-iimbak.
2	Tungkol sa paglalabas	. Kapag nagdadala kayo ng kritikal na impormasyon sa labas ng kumpanya, isinasagawa o sinusunod ba ninyo ang mga hakbang laban sa pagnanakaw o pagkawala ng file, tulad halimbawa ng paglalagay ng password?	4	2	0	0	P1 No.2 Ginagamit itong sanggunian para sa paglalabas.
3	Tungkol sa pagtatapon	Sa tuwing magtatapon ng mga importanteng dokumento tulad ng CD at iba pa, sinisigurado ba ninyo na hindi na mababasa pa ang kritikal na impormasyon na nilalaman ng mga ito sa pamamagitan ng paggamit ng shredder bago itapon ang mga ito?	4	2	0	0	P1 No.3 Ginagamit itong sanggunian para sa pagtatapon.
4		Kapag nagtatapon kayo ng personal computer o anumang data storage medium na naglalaman ng kritikal na impormasyon, gumagamit ba kayo ng software upang burahin ang mga datos na nilalaman ng mga ito o pinapabura ba ninyo ang electronic data sa isang espesyal na kontratista?	4	2	0	0	P1 No.4 Ginagamit itong sanggunian para sa pagtatapon.
5	Tungkol sa opisina	Kapag mayroong hindi kilalang tao sa loob ng opisina, tinatanong ba ninyo kung bakit siya naroroon at sinusubukan ba ninyong pigilin ang pagpasok niya mula sa mga lugar na hindi maaring pasukin ng mga hindi awtorisadong tao?	4	2	0	0	P2 No.5 Ginagamit itong sanggunian para sa opisina.
6		Isinasagawa ba ninyo ang mga hakbang upang maiwasan ang pagnanakaw, tulad halimbawa ng pagtatago ng mga kagamitan at notebook PC sa mga drawer ng inyong mesa, sa tuwing kayo ay aalis?	4	2	0	0	P2 No.6 Ginagamit itong sanggunian para sa opisina.
7		Ikinakandado ba ng huling taong umaalis ng opisina ang inyong opisina at inililista ba ninyo ang oras ng pag-alis (oras, pangalan ng taong umalis) mula sa opisina?	4	2	0	0	P2 No.7 Ginagamit itong sanggunian para sa opisina.
8	Tungkol sa personal computer	Sinisiguro ba ninyo na bago o updated ang inyong software, sa pamamagitan ng pagsasagawa ng Windows Update* 2?	4	2	0	0	P3 No.8 Ginagamit itong sanggunian para sa personal computer.
9		Ipinagbabawal ba ang paggamit o paglalagay ng mga delikadong software na maaring maging sanhi ng aksidenteng paglabas ng kritikal na impormasyon na tulad ng file trading software*3?	4	2	0	0	P3 No.9 Ginagamit itong sanggunian para sa personal computer.
10		Nilinaw ba ang tama at maling paggamit ng personal computer sa kumpanya, tulad halimbawa ng paggamit ng lisensyadong system ng kumpanya sa isang indibidwal na personal computer na ginagamit sa loob at labas ng kumpanya?	4	2	0	0	P3 No.10 Ginagamit itong sanggunian para sa personal computer.
11		Pinapatay ba ang power supply ng mga personal computer sa tuwing aalis ng opisina upang masiguro na hindi ito magamit ng iba?	4	2	0	0	P3 No.11 Ginagamit itong sanggunian para sa personal computer.
12	Tungkol sa password	Iniiwasan ba ang paggamit ng password na madaling hulaan, tulad halimbawa ng mga pangalan?	4	2	0	0	P4 No.12,13,14 Ginagamit itong sanggunian para sa password.
13		Hindi ba ninyo inilalagay o isinusulat ang password sa isang papel at idinidikit sa isang lugar?	4	2	0	0	P4 No.12,13,14 Ginagamit itong sanggunian para sa password.
14		Regular bang pinapalitan ang password upang masiguro na hindi ito mahuhulaan ng iba?	4	2	0	0	P4 No.12,13,14 Ginagamit itong sanggunian para sa password.
15	Tungkol sa virus	Isinagawa ba ninyo ang hakbang para protektahan ang personal computer mula sa virus na nagmumula sa kahina-hinalang website o E-mail sa pamamagitan ng paglalagay ng anti-virus software sa bawat personal computer?	4	2	0	0	P4 No.15 Ginagamit itong sanggunian para sa virus.
16		Sinisiguro ba ninyo na updated ang virus definition file sa pamamagitan ng paggamit ng automatic update ng inyong anti-virus software*4?	4	2	0	0	P4 No.16 Ginagamit itong sanggunian para sa virus.
17	Tungkol sa E-mail	Bago magpadala ng E-mail, sinisiguro ba ninyo na hindi ito maipapadala sa maling tao o address sa pamamagitan ng pagtse-tsek ng address na papadalhan?	4	2	0	0	P5 No.17 Ginagamit itong sanggunian para sa E-mail.
18		Sa tuwing magpapadala kayo ng pare-parehong E-mail sa iba' t-ibang tao, ginagamit ba ninyo ang BCC function ng E-mail upang masiguro na hindi nila makikita E-mail address ng isa' t-isa?	4	2	0	0	P5 No.18 Ginagamit itong sanggunian para sa E-mail.
19		Sa tuwing magpapadala kayo ng file na naglalaman ng kritikal na impormasyon sa pamamagitan ng E-mail, nilalagyan ba ninyo ng password ang file upang maprotektahan ang nilalaman nito?	4	2	0	0	P5 No.19 Ginagamit itong sanggunian para sa E-mail.
20	Tungkol sa backup	Isinasagawa ba ninyo ang hakbang laban sa aksidenteng pagkawala ng file nang dahil sa pagkasira ng system, maling pagkabura, at iba pa, sa pamamagitan ng regular na paggawa ng backup para sa mga files na naglalaman ng kritikal na impormasyon?	4	2	0	0	P5 No.20 Ginagamit itong sanggunian para sa backup.
21	Tungkol sa empleyado	Sinisiguro ba ninyo na pananatilihing lihim ng isang empleyado ang mga impormasyon tulad halimbawa ng mga impormasyon tungkol sa kaso ng pag-aampon?	4	2	0	0	P6 No.21 Ginagamit itong sanggunian para sa mga empleyad.
22		Regular ba ninyong ipinapaalala at ipinaliliwanag sa mga empleyado ang kahalagahan ng pag-kontrol sa mga impormasyon, at iba pa?	4	2	0	0	P6 No.22 Ginagamit itong sanggunian para sa mga empleyad.
23	Tungkol sa kasosyo	Pinapipirma ba ninyo ang mga kustomer sa isang kontrata kung saan nakasaad ang pagpapanatiling lihim ng mga impormasyon?	4	2	0	0	P6 No.23 Ginagamit itong sanggunian para sa mga kasosyo.
24	Tungkol sa aksidente	Mayroon ba kayong ginawang paghahanda tulad halimbawa ng pagbuo ng isang manwal na naglalaman ng mga dapat gawin sa panahon ng aksidente tulad ng aksidenteng paglabas, pagkawala, o pagkanakaw ng kritikal na impormasyon?	4	2	0	0	P6 No.24 Ginagamit itong sanggunian para sa panahon ng aksidente.
25	Tungkol sa alituntunin	Malinaw ba ang mga hakbang laban sa panganib sa information security tulad ng pagpapatupad ng patakaran ng kumpanya laban sa panganib sa information security (nasa itaas na 1~24, at iba pa)?	4	2	0	0	P6 No.25 Ginagamit itong sanggunian para sa alituntunin.
			A Kolumna para sa kabuuang puntos ng mga hakbang na isinasagawa	B Bahagi ng kolumna para sa pagkukuwenta ng kabuuang puntos ng mga hakbang na isinasagawa.	A+B Kabuuang puntos		
			Puntos	Puntos	Puntos		

※1 Mga kritikal na impormasyon na kung sakaling aksidenteng lumabas ay maaring maging sanhi ng kawalan ng tiwala sa kumpanya
Ito ay karaniwang mga datos ng kustomer, rehistro ng empleyado, mga plano, iskedyul o plano para sa pag-unlad, presyo ng binibiling gamit, halaga ng transaksyon, at iba pa.
※2 Programa na ibinibigay ng Microsoft Corp. na nagtatama sa mga kamalian o kahinaan ng Windows PC.
※3 Software na nagbibigay-daan sa pagpapalitan ng mga files sa pagitan ng marami at hindi tukoy na computers sa Internet, tulad halimbawa ng winny at Share.
※4 Tinatawag rin itong database file "pattern file" na ginagamit para sa pagtuklas ng mga computer virus.
※5 Function na nagtatago sa E-mail address ng tao mula sa ibang tao na kabilang sa listahan ng mga taong tatanggap ng parehong E-mail. Ito ay daglat para sa Blind Carbon Copy.

★Walang garantiya na ang mga hakbang na nakasaad sa diagnostic sheet ay sapat upang maprotektahan ang mga kritikal na impormasyon ng kumpanya.

1 Basahin muna ito bago isagawa ang diagnosis.

Ang paggamit.

Mayroong 25 na mga hakbang na kinikilala bilang minimong hakbang laban sa panganib sa information security na dapat ipatupad ng mga maliliit-at-katamtamang-laki na negosyo. Suriin kung ang mga hakbang na ito ay kasalukuyang ipinapatupad sa inyong kumpanya. Sumangguni sa kalakip na pamphlet para sa deskripsyon ng bawat hakbang at kung ano ang gagawin kung sakaling hindi pa ipinapatupad ang hakbang.

Ang layunin at halaga

- Sa pamamagitan nito, maaring matukoy ang problema at kung saan ito nagmumula.
- Sa pamamagitan ng pagtukoy sa problema, malalaman ang naaangkop na hakbang upang masolusyonan ito.

Pagbabasa ng "mga nilalaman ng diagnostic sheet"

Gumawa ng desisyon ukol sa aktwal na pangangailangan at huwag magpa-apekto lamang sa mga nilalaman ng diagnostic sheet. Halimbawa, ang pangunahing nilalaman ng bilang 6 sa diagnostic sheet ay tungkol sa kung "nagsasagawa ba kayo ng mga hakbang upang maiwasan ang pagnanakaw." Kung ang inyong kumpanya ay nagmamay-ari o gumagamit ng mga notebook PC, nagsasagawa ba kayo ng mga hakbang upang maiwasan ang pagkanakaw ng mga ito, tulad ng pagtatago ng mga ito sa kahon ng inyong mesa sa tuwing aalis kayo ng opisina? Kung ang inyong kumpanya naman ay walang notebook PC, nagsasagawa ba kayo ng mga hakbang tulad ng pagtatago at pag-iingat ng mga USB memory at external hard disk upang maiwasan ang pagnanakaw ng mga ito? Nagkakaroon ng pagkakaiba sa mga katanungan. Kung mayroong mga bagay na hindi malinaw para sa inyo o kung hindi kayo sigurado sa pangunahing punto ng katanungan, sumangguni sa pamphlet. Sa Sa isang kumpanya, ang mga ordinaryong impormasyon ay isa sa mga kritikal na impormasyon.

5		Kapag mayroong hindi kilalang tao sa loob ng opisina, tinatanong ba ninyo kung bakit siya naroroon at sinusubukan ba ninyong pigilin ang pagpasok niya mula sa mga lugar na hindi maaring pasukin ng mga hindi awtorisadong tao?
6	Tungkol sa opisina	Isinasagawa ba ninyo ang mga hakbang upang maiwasan ang pagnanakaw, tulad halimbawa ng pagtatago ng mga kagamitan at notebook PC sa mga drawer ng inyong mesa, sa tuwing kayo ay aalis?
7		Ikinakandado ba ng huling taong umaalis ng opisina ang inyong opisina at inililista ba ninyo ang oras ng pag–alis (oras, pangalan ng taong umalis) mula sa opisina?

Malamang sasabihin ninyo, walang "kritikal o importanteng impormasyon ang aming kumpanya", ngunit ang mga sumusunod ay halimbawa ng mga kritikal o importanteng impormasyon.

- Paraan ng pakikipag-ugnayan sa mga kustomer
- Impormasyon tungkol sa accounting ng kumpanya.
- Impormasyon ukol sa paglinang o paglikha ng bagong produkto at iba pa.
- Adres at impormasyon tungkol sa suweldo ng mga empleyado
- Rekord ng mga transaksyon at halaga ng mga ito ng bawat kustomer.
- Mga impormasyon na ipinag-utos ng mga kustomer na ingatan at pangalagaan.

2 Matapos ang diagnosis, basahin ito.

Mga direksyon na perpekto

Ang mga isinasagawang hakbang laban sa panganib sa information security ay perpekto na. pag-isipan ang pagpapataas ng antas.

→ Gumamit tayo ng patnubay sa seguridad at benchmark. → GOOD

Direksyon na may 70-99 puntos.

Halos lahat ay isinasagawa na ngunit mayroong ilang hakbang na hindi pa sapat.

Ang mga impormasyon ay maaring lumabas o malantad mula sa maliit na butas sa inyong seguridad. Ayusin na ang mga ito hangga't maaga pa.

Direksyon na may 50～69 puntos.

Kapansin-pansin na hindi masyadong binibigyang-pansin ang mga hakbang para sa pag-iingat.

Kung mababa ang marka ng isang aytem, isaayos ito. Simulan ang pagsasaayos sa madaling bahagi ng isang hakbang.

Direksyon na may 49 puntos pababa.

Talagang napakahirap kapag may nangyayaring mga aksidente na tulad ng aksidenteng paglabas ng impormasyon.

Kapag hindi nauunawaan ang bahagi o marka, lagyan ng tsek ang mababang aytem. Ipatupad na ang mga hakbang bago pa muling magkaroon ng aksidenteng paglabas ng impormasyon.

Alamin ang uri ng industriya na kinabibilangan ng kumpanya at "pag-aralan ang study tool para sa information security"* upang mas maunawaan ang posisyon at ranggo. Kapag mayroong ibang aytem na pinili maliban sa nasa kolumna na "isinasagawa", pag-aralan nang mahusay ang pamamaraan ng hakbang. Alamin ang "mga aytem na hindi isinasagawa" at piliting makaabot sa 100 puntos.

Sumagguni sa pagsusuri ng bisa o sa impormasyon tungkol sa pagpapabuti o muling pagsusuri. → Mabuti ang pagsasagawa ng pagpapabuti at muling pagsusuri.

Sumagguni sa impormasyon ukol sa mga hakbang at pagpa-plano o pagsusuri sa bisa. → Pagsusuri ng bisa / Pagsusuri ng bisa

Sumangguni sa stocks o sa impormasyon ukol sa mga hakbang at pagpa-plano. → Mga hakbang at pagpa-plano / Mga hakbang at pagpa-plano / Stocks

Ang diagnostic sheet na ito para sa mga kumpanya ay para sa mga kumpanya na mayroon ng mga sumusunod na katangian.

- Walang taong sadyang nakatalaga sa information system, o ang taong mamamahala sa system ay magiging karagdagang posisyon.
- Dahil sa limitado ang pinansiyal na kakayahan ng pangasiwaan, hindi gaanong ginagastusan ang mga hakbang na tinatalakay dito.

Saligan ng hakbang na ipinapakita sa halimbawa sa diagnosis sheet ng kumpanya.

- Maari itong makatulong sa pagbibigay ng direksyon at maaring ma-tsek ng kinatawan (tagapamahala) ang plano ng mga hakbang.
- Magkakakilala ang lahat ng mga empleyado.
- Ang server o kagamitan sa networking na pag-aari ng kumpanya ay hindi nangangailangan ng komplikadong setup

・Ang E-mail at homepage ay gumagamit ng server ng ISP. Samakatuwid, hindi ang kumpanya ang nagmamay-ari ng server na direktang nakakonekta sa Internet.
・Tanging mga commercial application software lamang ang ginagamit sa kumpanya, walang espesyal na software na nilikha na para lamang sa kumpanya.
・Kapag gumagamit ng indibidwal o sariling PC, huwag itong ikonekta sa network ng kumpanya, tulad halimbawa ng ISP at iba pa.
・(Walang WAN sa inyong kumpanya) Maliban sa Internet, wala nang ibang koneksyon na ginagamit sa loob ng network ng kumpanya.