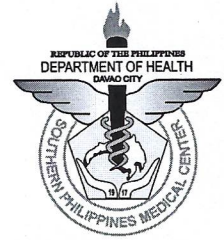




Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029



SPMC ADVISORY

Date: 5 June 2017
For: All SPMC Personnel, Volunteer and Visiting Consultants, Affiliates and Interns
Subject: Ransomware called "WannaCry"

In the last few weeks a massive cyber-attack has affected machines around the world by "WannaCry". This Ransomware locks users out of their own systems and demands a ransom payment to release files. In this heightened situation, we request everyone to stay alert while using your computers. When dealing with any emails from any unknown email address, do not click any link or open any unknown attachments. We request you to follow the best practices outlined below in checking your email through your computer, laptop and mobile devices to ensure the SPMC Computer network is not compromised. Please observe the following:


1. Do not open attachment in unsolicited e-mails even if they come from people in your contact list.
2. Do not click on any URLs contained in an unsolicited e-mail.
3. Report any suspicious emails or attachments to the IHOMP Office at local number 5043
4. Do not download suspicious software, videos, MP3s or any audio files, Torrents, Psiphone and others.
5. Ensure that your antivirus is updated and running in any machine you are using.
6. Backup your critical data periodically.

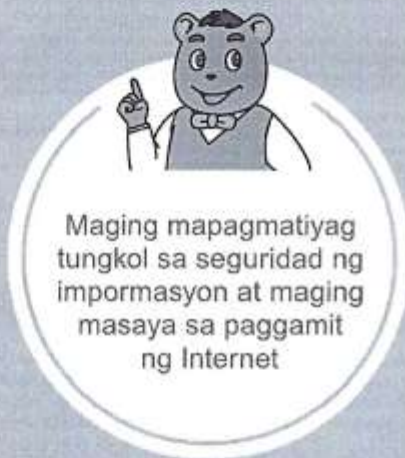
If in case of actual infection do the following:

- a) Immediately call IHOMP Office (Local 5043) or try to disconnect your machine from the network by pulling the LAN cable out of the port in your computer.
- b) Do not try to restore any data on your own.

Everyone is encouraged to help in protecting SPMC systems and network infrastructure.

Thank you for your understanding,


RICARDO SD. JUSTOL, MARE, MPA
Chief Administrative Officer



Hatid sa inyo ng:



Information and Communications
Technology Office
Department of Science and Technology

at



ASEAN • JAPAN
Information Security Awareness



ASEAN • JAPAN
Information Security Awareness



Alamin, Siguruhin
at Maging Mapagmatiyag

Seguridad ng Impormasyon

Gamitin ang Internet ng may Kompiyansa



Seguridad ng mga Smartphone

Ang mga Smartphone ay kinagigiliwan ng maraming tao sa buong mundo at ang porsyento ng benta ng mga smartphone, bilang bahagi ng kabuuang benta ng maliliit at portabl na radyo telepono, ay lalo pang tumataas.

Ang mga Smartphone ay kasama sa sobrang makabagong mga kagamitan kung ikukumpara sa tradisyonal na maliliit at portabl na radyo telepono. Sila ay nagbibigay kakayahan upang ating makita ang mga website na idinesenyo para sa mga PC at may iba't ibang uri ng aplikasyon ang maaaring ilipat dito at malayang magamit.

Ang naaayong bersiyon ng OS¹ at aplikasyon² sa mga Smartphone ay karaniwang inilalaan. Ang mga pagbabagong ito ay maaaring magbigay ng mas maraming pwedeng gawin at madagdagan ang sopistikasyon ng mga Smartphone o kaya ay madagdagan pa lalo ang kanyang seguridad.

¹ - OS ay ang pinaikling anyo ng Operating System o kaya ay ang programa at iba pang impormasyong nagpapatakbo o may kontrol sa PC o smartphone. Halimbawa sa mga PC, ang OS ay ang namamahala sa iba't-ibang gawain tulad ng sa I/O (Input/Output) na siyang namamahala sa mga ipinapasok gamit ang kibord, o kaya ay ang mga resulta na kailangan ilantad sa kasangkapang nagpapakita ng datos o kaya ay sa aparato sa paglilimbag.

² - Ang aplikasyon ay isang programa at iba pang impormasyong nagpapatakbo ng computer na may espesipikong isyuni, katulad ng sistemang pang-computer na nakaprograma para sa mabilis, mahusay na produksiyon at pag-edit ng mga papeles, ulat, rekord sa negosyo at iba pang katulad o kaya ay ang pagmanipula at makuha ang mga datos na nasa talahanayan. Ang mga laing gumagamit ay maaaring pumili ng aplikasyon na kailangan nila, at gamitin ang mga aplikasyon pagkatapos isasayos ang mga ito sa OS na siyang may pundamental na gawain.

³ - Ang Update ay nangangahulugan ng menor na pagbabago ng programa at iba pang impormasyong nagpapatakbo ng computer upang itama ang kamalian o kaya ay upang pahasayin ang ibang gawain nito. Sa pamamagitan ng paglagay sa kanila, ang mga taong gumagamit ay maaari nilang mapanatili na nasa tama ang kanilang programa. Mahalaga din na mapanatili sa tama ang mga programa na may kinalaman sa seguridad ng impormasyon.



Mga Panganib at Mga Banta

1 Ang bilang ng mga masamang programa na pinipili ang mga Smartphone ay lalong dumadami. Kapag ang iyong Smartphone ay magkaroon ng masamang programa, ang nilalaman ng iyong listahan ng mga tirahan at iba pang personal na impormasyon ay masaring maipadala sa isang panlabas na aparato na nangangasiwa sa pangmadlang serbisyo ng magkakabit na mga makinang elektroniko o kaya ay ang hindi awtorisadong pagsingil ng bayarin ay maaaring mangyari.

2 Maliban sa pagkakaroon ng masamang programa, habang naglilipat ng mga aplikasyon, ang isang aplikasyon ay maaaring humingi ng karapatan na gamitin ang impormasyon ng isang aparato o kaya ay hilingin na ang nilalaman ng listahan ng mga tirahan ay ipadala sa isang panlabas na aparato na nangangasiwa sa pangmadlang serbisyo ng magkakabit na mga makinang elektroniko. Bilang halimbawa, mayroong isang aplikasyon na nag-aangkin na ito ay nakadiseno na nagpapahaba ng buhay ng baterya, ngunit sa katotohanan ito ay susubuk na ipadala ang impormasyon na ang laman ay listahan ng mga tirahan na wala namang kabuluhan sa pag-gamit ng aplikasyon, sa isang panlabas na laptop.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Panatilihin ang OS, mga aplikasyon at programang panlaban sa iba pang programa na nagdudulot ng pinsala sa mga Smartphone ay palaging nakasunod sa pinakabagong bersiyon. Sa kadahilanang ang mga Smartphone ay nagtataglay ng listahan ng mga tirahan at iba pang sensitibong impormasyon, ang mas ibayo pang pag-iingat ay kinakailangan.
- Kung ikaw ay maglipat ng aplikasyon, siguruhin na ang website ay puwedeng mapagkatiwalaan at pati na din ang nagbigay ng aplikasyon. Kapag ikaw ay maglipat ng aplikasyon, siguruhin na iyong surin ang kasunduan na nagbibigay pahintulot at/o kaya ay ang mga termino ng serbisyo para sa mga impormasyon na kinukuha at kung paano ito maaaring gamitin, bago pa man ibigay ang pahintulot o kaya ay gamitin ang aplikasyon.

Seguridad ng Wireless LAN

Sa nagdaang mga taon, ang mga Laptop ay lalo pang gumaan ang kanilang timbang at ang mga Smartphone ay lalong kinagigiliwan, na lalo pang nagpabilis sa paggamit ng "Wireless LAN" upang magkaroon ng paraang maka-konekta sa Internet sa pamamagitan ng komunikasyon na hindi gumagamit ng kable sa loob o labas ng kabahayan o opisina.

Bilang karagdagan sa mga serbisyo may bayad, ang paggamit ng libreng Wi-Fi na pang-publiko na inilaan sa mga paliparan, estasyon ng tren at mga gusali para sa kalakalan ay dumami pa lalo.



Mga Panganib at Mga Banta

1 Sa kadahilanang ang Wireless LAN sa bahay o opisina ay maaaring kumonekta ng libre sa nasasakupang lugar ng along-radyo, ang komunikasyong ito ay puwedeng maharag kapag walang tamang seguridad na nakalagay. Pati na din ang hindi awtorisadong paraan ng pagkonekta sa Wireless LAN ay maaaring magdulot sa paglabas ng impormasyong personal o sikreto ng kumpanya o maging dahilan upang maging daan ng pag-atake sa aparato na nangangasiwa sa pangmadlang serbisyo ng magkakabit na mga makinang elektroniko.



2 Kapag gumagamit ng isang pang-publikong serbisyo ng Wireless LAN, ang iyong Laptop o Smartphone ay maaaring kumonekta sa isang huwad na pook. Kung gayon, ang iyong komunikasyon ay maaaring mapakinggan kahit na ang gamit mo na Wireless LAN ay gumagamit ng encryption.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Gumamit ng Wireless LAN sa bahay o opisina pagkatapos mailagay ang data encryption (WPA2: Wi-Fi Protected Access 2, atbp.) ng sa gayun ang pangkaraniwang komunikasyon ay hindi mahaharag at upang maiwasan ang hindi awtorisadong pagpasok. Kapag mano-mano ang paglagay ng data encryption, gumamit ng mahabang hanay ng mga karakter na hindi mo akalain na ito ang encryption key.
- Kapag gumagamit ng isang pang-publikong serbisyo ng Wireless LAN, gamitin lang ang website na encrypted sa pamamagitan ng SSL⁴ (ang URL ay nagsisimula sa "https://") at siguruhin na hindi gumagana ang File Sharing sa Laptop bago pa man gumamit ng serbisyo ng Wireless LAN.

⁴ - Ang SSL ay ang pinaikling anyo ng Secure Socket Layer na isang protokol para sa pag-encrypt ng impormasyon na ipinapadala sa isang sistemang hypertext na tumatakbo sa Internet.

Pandaraya sa Pamamagitan ng Isang Pindot

Ang pandaraya gamit ng isang pindot ay tungkol sa pandaraya sa pera sa pamamagitan ng paglabas ng iskrin para sa pagbayad ng pagsali o kaya ay bayad sa serbisyo pagkatapos pindutin ang isang litrato o sine sa isang website.



Sa ngayon, mayroon isang pandaraya gamit ng isang pindot na ang gamit ay aplikasyon ng Smartphone at Social Networking Services¹ o kaya ay Blog².

Maliban sa mga kasong "one-click", ang iskrin sa paniningil ay maaaring maglabas pagkatapos ng ilang pindot, ng impormasyon tungkol sa pagpatunay ng edad at iba pa. Sa ibang pagkakataon ang gamit na pamamaraan ay lalong nagiging mapanlinlang at sopistikado. Ang iskrin ng paniningil ay hindi nawawala kahit na patayin pa ang aparato.

¹ - Ang SNS ay ang pinaikling anyo ng Social Networking Service na naglalaman ng koleksiyon ng magkakaugnay na dokumento o pintungan ng impormasyon sa isang sistemang hypertext na tumatakb sa Internet na may madaming puwedeng pag-gamitan katulad ng pagbukas ng ating diary o aklat ng mga litrato sa publiko, o kaya ay gumawa ng komunidad na kung saan ang mga gumagamit nito ay puwedeng malayang magpalitan ng mga pananaw.

² - Ang Blog ay ang pinaikling anyo ng Weblog na kung saan ang mga gumagamit ay maaaring sumulat ng kanilang pananaw o kaya ay impresyon katulad ng talaarawan, at ang mga bumabasa nito ay matayang makapagbibigay ng kanilang komento.

Mga Panganib at Mga Banta

1 Ang pagpindot sa mga libreng litrato o sine na napakainteresado sa gumagamit ay maaaring magdulot ng hindi awtorisadong paniningil o mapunta ka sa isang mapanlinlang na website.

2 Mayroong mga pagkakataon na ang IP address³ o impormasyon ng nagbibigay ng serbisyo ay nakalista sa iskrin ng paniningil upang magbigay takot at palabasin na ang gumagamit ay nakilala na.



³ - Ang IP address ay numero para sa identipikasyon na maaaring awtomatikong italaga sa mga instrumento o computer kapag sila ay ikakabit sa Internet.

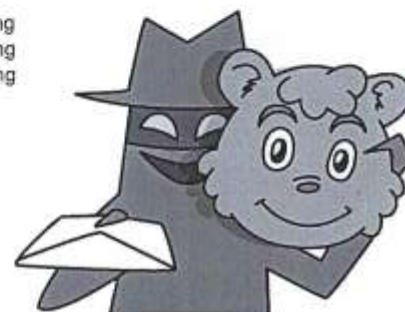


Mga Hakbang Laban sa mga Panganib at mga Banta

- Harangan ang mga pagtatangka na kumonekta sa mga malisyosong website sa pamamagitan ng paggamit ng filtering software o mga makabagong software sa seguridad. Siguruhin din na mag download lamang ng mga aplikasyon para sa smartphone mula sa mga mapagkakatiwalaang website.
- Maging maalam kapag gumagamit ng computer na ang isang pagpindot ay hindi nangangahulugan na ikaw ay makikilala agad, kaya huwag sumagot sa mga pagtatangka na ikaw ay singilin. Sa mga gumagamit ng smartphone, maging maingat sa mga aplikasyon, ano mang impormasyon na nakalagay sa aparato katulad ng iyong impormasyon o iba pa na nakalagay sa listahan ng mga tirahan ay maaaring maisiwalat.
- Kung magkataon na ikaw ay mapunta sa isang malisyosong website, ang hindi awtorisadong paniningil ay magpapatuloy o makatanggap ka ng utos mula sa korte, kumunsulta muna sa awtoridad para sa nararapat na payo.

Pagpunteryang Atake Gamit ang Email a.k.a. Atake Gamit ang Spear Phishing

Ang pagpunteryang atake gamit ang e-mail ay ang pagpadala ng e-mail na kunwari ay galing sa isang kakilala. Ang e-mail ay maaaring may malisyosong nakalagay at kapag mabigyan daan, ito ay manghawa ng virus or maglagay ng trojan.



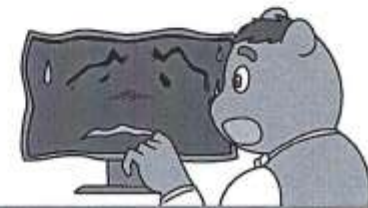
Ang isang halimbawa ng ganitong uri ng pagpunterya ay ang pag-atake sa isang espesipikong organisasyon o kaya ay indibidwal. Ang isang e-mail na may nakalagay na virus ay ipinapadala mula sa isang nagpapanggap na partido o isang kasamahan sa organisasyon.

May mga naiulat na mga kaso kung saan ang lihim na salita ay nanakaw o kaya ay nagkaroon ng pagkahawa ng virus at iba pa, na ang pinagmulan ng atake ay ang pagpunterya gamit ang e-mail.

Mga Panganib at Mga Banta

1 Sa kamakailang mga atake, ang mga pamamaraan na ginamit upang magpanggap bilang isang pinagkakatiwalaang e-mail ay nagiging sopistikado at adelantado. Ang pangalan ng mga kagawaran at/o kaya ay mga tunay na indibidwal ay ginamit, bilang karagdagan sa mga nilalaman o kaya ay impormasyon na tanging ang mga nakaka-alam lamang ay iyong piling lapian.

2 Kung may nakalagay na virus, ang kinalabasan ng pagbukas nito ay ang awtomatikong pagkonekta sa panlabas na server at anumang impormasyon ang nasa computer ay lalabas ng walang pahintulot.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Huwag buksan ang anumang kahina-hinalang kalakip sa e-mail o URL.
- Kung mangyaring nakapagbukas ka ng kahina-hinalang e-mail, huwag kang mataranta at huwag patayin ang aparato. Tanggaliin ang kable para sa network at humingi ng tulong mula sa system administrator.
- Maglagay ng programa laban sa computer virus at siguruhin na ito ay palaging nasasaayong bersiyon.
- Tuwinang ilagay ang mga pagbabago sa mga aplikasyon maliban duon sa OS.

Mga Atake Gamit ang DDoS

Ang pag-atake gamit ang DDoS ay pagpapadala sa isang espesipikong server ng packets mula sa maraming mga computer na nakompromiso na mula sa ibat-ibang mga network, hanggang ang linya ng komunikasyon ay nag-uumpaw na at ang server ay huminto na sa gawain nito.

DDoS: Distributed Denial of Service / Nakapamahaging pagkait ng serbisyo



Mga Panganib at Mga Banta

1 Ang umaatake ay palihim na naglalagay ng malisyosong programa upang gawin ang pag-atake sa pamamagitan ng mga computers na walang kaugnayan sa totoong bibiktimahin na server. Samakatuwid, ang isang gumagamit ng computer ay maaaring umatake sa isa pa ng hindi niya nalalaman.

2 Ang computer na nakompromiso na ay maaaring magsagawa ng iba pang mga pag-atake katulad ng paghawa ng computer virus, pagpapadala ng mga walang silbing e-mail o kaya ay ang pagsira sa itsura ng website imbes na ang tunay na umaatake ang gumawa nito.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Panatilihin ang OS sa computer, smartphone o iba pang aparato na kumukonekta sa Internet ay palaging may naaayon at pinaka-bagong bersiyon.
- Maglagay ng programa laban sa computer virus at siguruhin na ito ay may naaayon at pinaka-bagong bersiyon.
- Tuwinang ilagay ang mga pagbabago sa mga aplikasyon maliban duon sa OS.

Tuntunin ng Mabuting Asal Kapag Gumagamit ng Internet

Dahil sa pagdami ng maaaring gamit ng SNS (social networking service), maraming mga isyu sa Internet, na hindi naisip nuon, ay nagsilabasan.

Mayroong mga kaso na kung saan ang mga indibidwal ay naglalagay ng mga nilalaman sa Internet na maaaring makilala ang siniraang puri o kaya ay nangangailangang magbigay ng pang-publikong paumanhin ang mga kumapanya.



Mga Panganib at Mga Banta

1 Mayroong posibilidad na ang karaniwang paglagay ng impormasyon sa SNS ay magdulot ng paglahad ng pansariling impormasyon o kaya ay ang lumabag sa pagiging pribado.



2 Ang kaswal na paglagay ng impormasyon sa Internet ay maaaring magdulot ng demanda para sa pagbabayad sa kasiraan na nangyari, masidhing pagkastigo ng batas o kaya ay ang ma-aresto ka.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Maging maingat na huwag mabunyag ang anumang hindi kinakailangan personal na impormasyon sa Internet sa pamamagitan ng SNS, blog o miniblog at iba pa. Ang paglagay ng mga larawan ay maaaring magbunyag ng impormasyon tungkol sa mga lugar na dapat ay pinag-iingatan.
- Kahit sa Internet, siguruhin na iyong isaalang-alang ang pagiging pribado at dignidad ng ibang tao at suriin ang nilalaman bago maglagay ng impormasyon.

Angkop na Pagkapwesto at Pamamahala ng ID at Lihim na Salita

Upang magamit ang e-mail, pamimili sa Internet, pagbangko sa Internet at iba pang mga serbisyo sa Internet ng ligtas, may maraming ibat-ibang tipo ng pagpapatotoo, habang ang isa sa pinakasikat ay ang kumbinasyon ng ID at lihim na salita.

Kamakailan lang ay nagkaroon ng pagtaas sa mga pag-atake na ang punterya ay ang impormasyon tungkol sa taong gumagamit katulad ng ID at ang lihim na salita.



Mga Panganib at Mga Banta

1 Ang malisyosong ika-tatlong partido ay maaaring gayahin ang isang taong gumagamit at ibunyag ang impormasyon o kaya ay maging sanhi ng pagbabayad sa pinsala kapag ang ID at lihim na salita ay lubhang napakapayak na kumbinasyon (tulad ng 4 na numero ng kaarawan or "9999" at iba pa) o kaya ay dahil sa walang pag-iingat na pamamahala. Halimbawa, ang lihim na salita ay isulat at iwanan sa idinidikit na post-it-note sa kasangkapan na nagpapakita ng mga datos.

2 Kapag gumagamit ng parehong kumbinasyon ng ID at lihim na salita para sa ibat-ibang mga website at ang impormasyon ay lumabas mula sa isang website, ang posibilidad na maging biktima ng hindi awtorisadong pagpasok sa iba pang website ay tataas.

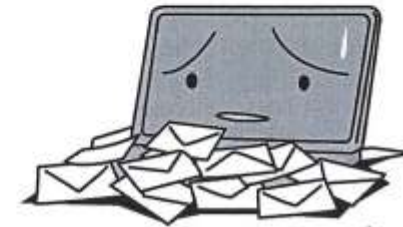


Mga Hakbang Laban sa mga Panganib at mga Banta

- Itakda ang lihim na salita kasama ang mahirap mabatid na hanay na mayroong hindi baba sa 8 karakter na naglalaman ng mga bilang, malaki at maliit na letra at piling mga simbolo. Gayunpaman ay baguhin ang lihim na salita palagi.
- Huwag ipamahagi ang lihim na salita sa ibang tao o kaya ay gamitin ang kaparehong lihim na salita para sa ibat-ibang website. Kung ang website na iyong gamit ay magbigay impormasyon na ang iyong lihim na salita ay lumabas ng walang pahintulot, palitan ang lihim na salita para sa website na iyun at para na din duon sa iba pang mga website na gamit mo ang kaparehong lihim na salita.
- Iwasan ang paglagay ng pangsariling impormasyon sa mga computer na bukas sa buong publiko katulad ng Internet Cafe at iba pang mga katulad na lugar.

Mga Walang Silbing E-mails ¹

Ang e-mail ay mabuti sa pangangailangan na gamit para sa komunikasyon kung saan ang pagpadala at pagtanggap ay puwedeng gawin na walang isinasalang-alarig kung nasaan ang tatanggap o kaya ay kung gaano kalayo sila. Subalit, mula sa panahaw ng makatatanggap ay maaaring marami ang hindi kinakailangan na e-mail, walang silbing mga e-mail, na ipinapadala at natatanggap.



Dahil sa malaking bilang ng walang silbing mga e-mail na ipinapadala, nagkaroon ng mga isyu na kung saan ang mga kagamitan ng nagkakaloob ng pasilidad ay maaaring lumabis na sa kakayanan nito at humantong sa pagka-antala ng pagpadala o pagtanggap ng mga mensahe.

Mga Panganib at Mga Banta

1 May mga kaso na ang computer ay lilikha ng walang kaayusan na malaking bilang ng mga e-mail addresses at magpapadala ng mga mensahe. Samakatuwid, ang pag-gamit ng mga maikling e-mail address at sikat na pangalan ay maaaring magresulta sa mataas na posibilidad na makatanggap ng mga walang silbing e-mail.



2 Ang ilan sa mga balidong e-mail address para makapagpadala ng walang silbing e-mail ay nakolekta sa pamamagitan ng pagrehistro sa isang libreng huwad na serbisyo o kaya ay sa pamamagitan ng walang katotohanang paraan ng pagpatigil ng suskripsiyon. Dagdag pa dito, ang pagbukas ng nakalakip na impormasyon sa isang e-mail o kaya ay pagbukas sa isang kawing sa loob ng e-mail ay maaaring magdulot ng pagpunta sa isang hindi awtorisadong website o kaya ay magdulot ng pagkahawa ng computer virus.

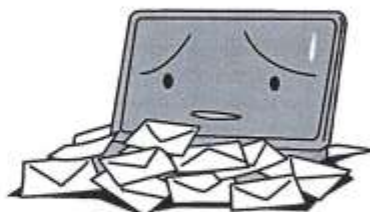


Mga Hakbang Laban sa mga Panganib at mga Banta

- Ang mga e-mail address ay dapat mayroong malaking bilang ng mga karakter at isama ng walang kaayusan ang mga numero upang gawin itong mahirap mahulaan.
- Huwag maglagay ng padalos-dalos ng iyong e-mail address sa isang website o kaya ay ilagay sa website ang iyong e-mail address kung hindi naman kinakailangan.
- Kung kinakailangan na gumamit ng website na hindi mapagka-katiwalaan, maaaring mas epektibo na gumamit ng libreng e-mail address kaysa gamitin ang e-mail address na ipinamahagi mula sa nagbibigay ng serbisyo.

Mga Walang Silbing E-mails 2

Ang mga walang silbing e-mail ay hindi lamang puwedeng magdulot ng hindi ikatutuwa ng makakatanggap o kaya ay makaabala pa sa trabaho, ngunit ang mga pamamaraan ay lalong nagiging malisyoso at mapanlikha, na maaaring magdulot sa pagpunta sa isang hindi awtorisadong website kung saan ang iyong pera ay puwedeng manakaw, o kaya ay mapunta sa isang puwesto para salain ang mga walang silbing e-mail.



Ang mga Smartphone ay maaaring mahawaan ng computer virus na nakapaloob sa mga walang silbing e-mail, na minamanipula mula sa malayong lugar upang magpadala ng malaking bilang ng mga walang silbing e-mail na hindi alam ng gumagamit.

1 Mga Panganib at Mga Banta

1 May mga kaso na ang computer ay lilikha ng walang kaayusan na malaking bilang ng mga e-mail address at magpapadala ng mga mensahe. Samakatuwid, ang pag-gamit ng mga maikling e-mail address at sikat na pangalan ay maaaring magresulta sa mataas na posibilidad na makatanggap ng mga walang silbing e-mail.



2 Ang ilan sa mga balidong e-mail address para makapagpadala ng walang silbing e-mail ay nakolekta sa pamamagitan ng pagrehistro sa isang libreng huwad na serbisyo o kaya ay sa pamamagitan ng walang katotohanang paraan ng pagpatigil ng suskripsiyon. Dagdag pa dito, ang pagbukas ng nakalakip na impormasyon sa isang e-mail o kaya ay pagbukas sa isang kawing sa loob ng e-mail ay maaaring magdulot ng pagpunta sa isang hindi awtorisadong website o kaya ay magdulot ng pagkahawa ng computer virus.



Mga Hakbang Laban sa mga Panganib at mga Banta

- Subukan na harangan ang mga walang silbing e-mail sa pamamagitan ng paggamit sa serbisyo ng mga hakbang laban sa mga walang silbing e-mail katulad ng pagtanggap o kaya ay panlaban sa panggagaya mula sa mga nagbibigay ng serbisyo para sa Internet o kaya ay programa na pangsala.
- Kung ikaw ay makatanggap ng mga walang silbing e-mail, burahin agad ito bago pa man buksan. Gayundin, huwag buksan ang anumang nakalakip sa e-mail o kaya ay buksan ang kawing mula sa mga kahina-hinalang e-mail. Maaari din naman maging epektibo na ipadala ang mga walang silbing e-mail sa nagbibigay serbisyo sa inyo ng Internet o kaya ay sa pampublikong ahensiya na may kinalaman dito.
- Gumawa ng iba pang mga hakbangin para sa mga smartphone at gayun din naman sa PC.

Protektahan ang inyong smartphone at computer.

Ang mga Smartphone at mga computer ay mga nakabubuting kagamitan. Ngunit sila ay may maraming kinakaharap na panganib katulad ng pagkakaroon ng mga computer virus. Alalahanin na sundin ang tatlong pinakamataas na tulong para sa seguridad ng impormasyon para maasahan ang kaligtasan at seguridad kapag gumagamit ng mga computer at mga smartphone.



Tatlong pinakamataas na patnubay para sa seguridad ng impormasyon

Hawakan ang mga mahalagang impormasyon kaugnay sa isang tao ng may ibayong pag-iingat.

Protektahan ang iyong computer sa pamamagitan ng mga makabagong seguridad.

Huwag puntahan o kaya ay buksan ang mga kahina-hinalang website o kaya ay hindi pamilyar na ipinapadalang mga email.

Ang mga seguridad para sa impormasyon ay maaaring ihalimbawa sa pagkabit ng sinturong pangkaligtasan kapag magbyahe gamit ang kotse, at ito ay isang bagay na hindi natin dapat makalimutan kapag tayo ay gumagamit ng smartphone o kaya ay computer.

