ASEAN · JAPAN
Information Security Awareness

ຮູ້ທັນ ປ້ອງກັນ ລະມັດລະວັງ

ຮັກສາຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ

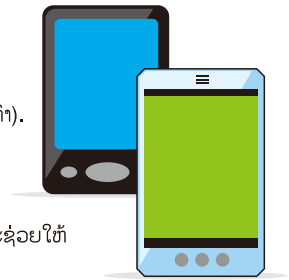
ໃຊ້ອິນເຕີເນັດດ້ວຍຄວາມໝັ້ນໃຈ

ລະມັດລະວັງ
ຮັກສາຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ
ແລະ ມ່ວນຊື່ນ
ກັບການນຳໃຊ້ອິນເຕີເນັດ

LaoCERT
Lao Computer Emergency Response Team

http://www.laocert.gov.la

ການຮັກສາຄວາມປອດໄພສະມາດໂຟນ



ສະມາດໂຟນໄດ້ກາຍມາເປັນທີ່ນິຍົມກັນຫຼາຍຂຶ້ນທົ່ວທຸກມຸມໂລກ
ແລະ ຍອດຂອງການຂາຍສະມາດໂຟນກໍ່ໄດ້ມີອັດຕາສ່ວນເພີ່ມຂຶ້ນ.

ສະມາດໂຟນເປັນອຸປະກອນທີ່ທັນສະໄໝເມື່ອທຽບກັບໂທລະສັບມືຖືແບບດັ້ງເດີມ(ລຸ້ນເກົ່າ).
ເຊິ່ງຊ່ວຍໃຫ້ເຮົາສາມາດເບິ່ງເວັບໄຊຕ່າງໆໄດ້ຄືກັນກັບຄອມພິວເຕີທົ່ວໄປ ແລະ
ໂປຼແກຼມປະເພດຕ່າງໆສາມາດດາວໂຫຼດ ແລະ ໃຊ້ງານໄດ້ຢ່າງເປັນອິດສະລະ.

ການປັບປຸງລະບົບປະຕິບັດການ ແລະ ໂປຼແກຼມເທິງສະມາດໂຟນຢ່າງເປັນປົກກະຕິຈະຊ່ວຍໃຫ້
ອຸປະກອນກາຍເປັນເຄື່ອງມືທີ່ມີຄວາມທັນສະໄໝ ແລະ ປອດໄພຫຼາຍຂຶ້ນກວ່າເກົ່າ.

※1 OS ແມ່ນຄຳຫຍໍ້ຂອງລະບົບປະຕິບັດການເຊິ່ງແມ່ນຊ່ອບແວຊຸດໜຶ່ງທີ່ຄວບຄຸມຄອມພິວເຕີ ຫຼື ສະມາດໂຟນ.
ຕົວຢ່າງເຊັ່ນ: ໃນຄອມພິວເຕີ, ລະບົບປະຕິບັດການມີໜ້າທີ່ຈັດການກັບບັນດາຟັງຊັ່ນປະເພດຕ່າງໆເຊັ່ນ: I/O(ເຂົ້າ/
ອອກ) ຫຳໜ້າທີ່ເປັນຕົວປະມວນຜົນ ຮັບຄຳສັ່ງຈາກແປ້ນພິມ ແລ້ວມັນຈະສົ່ງໄປສະແດງທີ່ໜ້າຈໍ ຫຼື ພິມອອກມາ

※2 ໂປຼແກຼມແມ່ນ ຊ່ອບແວທີ່ມີວັດຖຸປະສົງສະເພາະເຊັ່ນ: ການປະມວນຜົນຄຳສັ່ງ ຫຼື ທຳການຄິດໄລ່. ຜູ້ຊົມໃຊ້
ສາມາດເລືອກໄດ້ຕາມຄວາມຕ້ອງການ ພາຍຫຼັງທີ່ໂປຼແກຼມໄດ້ຕິດຕັ້ງລົງໄປໃນລະບົບປະຕິບັດການແລ້ວ ເຊິ່ງມັນກໍ່ມີຟັງຊັ່ນ
ພື້ນຖານທີ່ນຳໃຊ້ໃນຊ່ອບແວທົ່ວໄປ.

※3 ອັບເດດແມ່ນໝາຍເຖິງ ການປັບປຸງ ຫຼື ແກ້ໄຂເລັກນ້ອຍຂອງຊ່ອບແວ ເພື່ອແກ້ໄຂຂໍ້ບົກຜ່ອງ ຫຼື ປັບປຸງໜ້າທີ່
ການທຳງານຂອງຊ່ອບແວນັ້ນໃຫ້ດີຂຶ້ນ ເຊິ່ງຜູ້ໃຊ້ສາມາດປັບປຸງໄດ້ຕາມໄລຍະທີ່ມັນໄດ້ແກ້ໄຂສຳເລັດເພາະຊ່ອບແວທີ່ໄດ້
ຮັບການປັບປຸງນັ້ນມັນຈະມີຄວາມປອດໄພຂຶ້ນຕື່ມ

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ຈຳນວນເປົ້າໝາຍການໂຈມຕີຂອງ ເມົາແວ(malware) ຕໍ່ກັບສະມາດໂຟນໄດ້ເພີ່ມຂຶ້ນເລື້ອຍໆ. ຖ້າຫາກວ່າອຸປະກອນ
ຂອງທ່ານຕິດເຊື້ອແລ້ວ, ຂໍ້ມູນທີ່ສຳຄັນອາດຈະຖືກສົ່ງໄປຫາເຄື່ອງແມ່ຂ່າຍພາຍນອກ ຫຼື ການລັກໂອນເງິນໃນບັນຊີຂອງ
ທ່ານອາດຈະເກີດຂຶ້ນໂດຍທີ່ບໍ່ຮູ້ໂຕ.

2 ນອກຈາກຈະຕິດເຊື້ອໂດຍເມົາແວ(malware)ແລ້ວ, ເມື່ອເວລາທີ່ມີການດາວໂຫຼດໂປຼແກຼມຕ່າງໆ,
ໂປຼແກຼມອາດຈະຂໍໃຫ້ຜູ້ໃຊ້ງານສະໜອງຂໍ້ມູນ ຫຼື ຂໍ້ມູນບັນຊີທະນາຄານ
ກໍ່ຈະຖືກສົ່ງໄປຫາເຄື່ອງແມ່ຂ່າຍພາຍນອກ. ຍົກຕົວຢ່າງ ໃນກໍລະນີ
ຂອງໂປຼແກຼມທີ່ອ້າງວ່າໄດ້ຮັບການອອກແບບມາເພື່ອເພີ່ມແບັດຕາລີໄດ້,
ແຕ່ແທ້ຈິງແລ້ວມັນພະຍາຍາມທີ່ຈະສົ່ງຂໍ້ມູນບັນຊີ
ທະນາຄານທີ່ບໍ່ໄດ້ກ່ຽວຂ້ອງກັບການໃຊ້ງານຂອງໂປຼແກຼມໄປຫາບຸກຄົນພາຍນອກ(ພາກສ່ວນອື່ນ).

ມາດຕະການຕອບໂຕ້

- ປັບປຸງລະບົບປະຕິບັດການ, ໂປຼແກຼມ ແລະ ຊ່ອບແວປ້ອງກັນໄວຣັດສເທິງສະມາດໂຟນໃຫ້ຢູ່ໃນສະພາບລຸ້ນໃໝ່ລ້າສຸດ
ເປັນປະຈຳ. ເມື່ອທຽບກັບເຄື່ອງຄອມພິວເຕີແລ້ວ ສະມາດໂຟນກໍ່ສາມາດເກັບຮັກສາຂໍ້ມູນບັນຊີທະນາຄານ ແລະ ຂໍ້
ມູນທີ່ສຳຄັນອື່ນໆໄດ້, ສະນັ້ນເຮົາກໍ່ຄວນໃຫ້ຄວາມລະມັດລະວັງຫຼາຍຂຶ້ນ ເຊິ່ງເປັນສິ່ງທີ່ຈຳເປັນໃນປະຈຸບັນ.

- ໃນເວລາທີ່ມີການດາວໂຫຼດໂປຼແກຼມຕ່າງໆ, ຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າເວັບໄຊ ແລະ ຜູ້ສະໜອງໂປຼແກຼມດັ່ງກ່າວວ່າ
ແມ່ນສາມາດເຊື່ອຖືໄດ້. ນອກຈາກນັ້ນເວລາທີ່ດາວໂຫຼດ, ຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າມີການຕົກລົງເຫັນດີ ຫຼື ເງື່ອນໄຂ
ຂອງການບໍລິການຂໍ້ມູນທີ່ເກັບລວບລວມ ແລະ ວິທີການທີ່ຈະນຳມາໃຊ້ ກ່ອນທີ່ຈະຕົກລົງເຫັນດີ ຫຼື ການນຳໃຊ້ໂປຼແກຼມ
ນັ້ນ.

ການຮັກສາຄວາມປອດໄພອາຍເລັສແລນ(ເຄືອຂ່າຍໄຮ້ສາຍ)

ໃນຊຸມປີມໍ່ໆມານີ້, ຄອມພິວເຕີສ່ວນບຸກຄົນໄດ້ກາຍມາເປັນເຄື່ອງທີ່ມີນ້ຳໜັກເບົາ ແລະ
ສະມາດໂຟນກໍ່ເປັນທີ່ນິຍົມກັນ
ຫຼາຍຂຶ້ນ, ເຊິ່ງມັນໄດ້ເພີ່ມຄວາມວ່ອງໄວຂອງການນຳໃຊ້ເຄືອຂ່າຍໄຮ້ສາຍ
ເຮັດໃຫ້ການເຂົ້າເຖິງອິນເຕີເນັດຜ່ານການສື່ສານ
ໄຮ້ສາຍນັ້ນບໍ່ວ່າຈະຢູ່ນອກບ້ານ ຫຼື ຫ້ອງການກໍ່ມີຄວາມສະດວກສະບາຍ.

ນອກຈາກການຊຳລະຄ່າໃຊ້ຈ່າຍໃຫ້ແກ່ຜູ້ໃຫ້ບໍລິການແລ້ວ, ບໍລິການຟ້ອາຍ-ຟາຍ (Wi-Fi)
ໄດ້ສະໜອງໃຫ້ຕາມສະຖານທີ່ສາທາລະນະເຊັ່ນ: ສະໜາມບິນ, ສະຖານນີລົດໄຟ ແລະ
ຕຶກອາຄານການຄ້າຕ່າງໆກໍ່ໄດ້ເພີ່ມຂຶ້ນເຊັ່ນກັນ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ເນື່ອງຈາກເຄືອຂ່າຍໄຮ້ສາຍສາມາດເຊື່ອມຕໍ່ໄດ້ຢ່າງອິດສະລະ
ພາຍໃນເຂດພື້ນທີ່ປົກຄຸມດ້ວຍຄື້ນວິທະຍຸ, ການສື່ສານໃນ
ຮູບແບບນີ້ອາດຈະຖືກດັກຈັບ
ເວັ້ນເສຍແຕ່ວ່າມາດຕະການຮັກສາຄວາມປອດໄພທີ່ເໝາະສົມຈະຖືກນຳມາບັງຄັບໃຊ້

2 ເຊັ່ນດຽວກັນກັບການລັກເຂົ້າໄປຫາເຄືອຂ່າຍໄຮ້ສາຍອາດຈະນຳໄປສູ່ການຮົ່ວໄຫຼຂອງຂໍ້ມູນສ່ວນບຸກຄົນ
ຫຼື ນຳຄອມພິວເຕີໃນເຄືອຂ່າຍມາໃຊ້ເປັນການໂຈມຕີເຊີເວີ.

3 ເມື່ອເວລານຳໃຊ້ບໍລິການເຄືອຂ່າຍໄຮ້ສາຍສາທາລະນະ, ຄອມພິວເຕີ ຫຼື ສະມາດໂຟນຂອງທ່ານອາດຈະເຊື່ອມຕໍ່ເຂົ້າຫາເຄືອ
ຂ່າຍປອມ. ໃນກໍລະນີນັ້ນ, ການສື່ສານຂອງທ່ານອາດຈະຖືກດັກສະກັດເອົາຂໍ້ມູນໄດ້ ເຖິງແມ່ນວ່າການນຳໃຊ້ລະບົບເຄືອ
ຂ່າຍໄຮ້ສາຍໄດ້ເຂົ້າລະຫັດແລ້ວກໍ່ຕາມ.

ມາດຕະການຕອບໂຕ້

- ນຳໃຊ້ເຄືອຂ່າຍໄຮ້ສາຍຢູ່ທີ່ບ້ານ ຫຼື ຫ້ອງການພາຍຫຼັງທີ່ໄດ້ຕັ້ງຄ່າການເຂົ້າລະຫັດຂໍ້ມູນ (WPA2: Wi-Fi Protected
Access 2, etc.) ເພື່ອເຮັດໃຫ້ການສື່ສານໃນຮູບແບບນີ້ບໍ່ສາມາດຖືກດັກຈັບໄດ້ ແລະ ກໍ່ເພື່ອປ້ອງກັນການເຂົ້າເຖິງທີ່ບໍ່ໄດ້
ຮັບອານຸຍາດ. ເມື່ອເຮົາຕັ້ງຄ່າການເຂົ້າລະຫັດຂໍ້ມູນ, ກຳນົດໃຫ້ມີຕົວອັກສອນທີ່ຍາວພຽງພໍ ແລະ ບໍ່ໃຫ້ສາມາດເດົາໄດ້ວ່າ
ເປັນການເຂົ້າລະຫັດ.

- ເມື່ອມີການໃຊ້ບໍລິການເຄືອຂ່າຍໄຮ້ສາຍສາທາລະນະ, ໃຊ້ເວັບໄຊເຂົ້າລະຫັດໂດຍ SSL (ເວັບໄຊທີ່ມີ URL ເລີ່ມຕົ້ນຈາກ
“https://”) ເທົ່ານັ້ນ ແລະ ກວດສອບຄອມພິວເຕີທີ່ທ່ານກຳລັງໃຊ້ງານຢູ່ນັ້ນຖ້າມີການໃຊ້ໄຟລຮ່ວມກັນກໍ່ໃຫ້ປິດໄວ້
ກ່ອນໃນຊ່ວງໄລຍະທີ່ໃຊ້ບໍລິການດັ່ງກ່າວ.

※4 SSL ແມ່ນຄຳສັບຫຍໍ້ຂອງ Secure Socket Layer ເຊິ່ງແມ່ນໂປຼໂຕໂຄນໜຶ່ງທີ່ໃຊ້ໄວ້ເຂົ້າລະຫັດຂໍ້ມູນ ເພື່ອສົ່ງຜ່ານເວັບໄຊ

ໜຶ່ງ-ຄຼິກ ສໍ້ໂກງ

ໜຶ່ງ-ຄຼິກ ສໍ້ໂກງ ໝາຍເຖິງການຂໍ້ລັກ(ສໍ້ໂກງ)ເງິນໂດຍການສະແດງໜ້າຈໍເພື່ອຮຽກຮ້ອງເກັບເງິນຄ່າລົງທະບຽນ ຫຼື ຄ່າທຳນຽມໃນການໃຊ້ບໍລິການຫຼັງຈາກການກົດທີ່ຮູບພາບ ຫຼື ວິດີໂອໃດໜຶ່ງທີ່ຢູ່ເທິງເວັບໄຊ

ເມື່ອມໍ່ໆມານີ້, ໄດ້ມີການສໍ້ໂກງ, ເຊິ່ງນຳໃຊ້ໂປຼແກຼມສະມາດໂຟນ ແລະ ບໍລິການສື່ສັງຄົມອອນລາຍເຊັ່ນ: ການໃຊ້ບູລອ / ບໍລິການເຄືອຂ່າຍສັງຄົມ SNS.

ນອກຈາກນີ້ໃນກໍລະນີ “ໜຶ່ງ-ຄຼິກ“, ໜ້າຈໍການຮຽກເກັບເງິນອາດຈະປະກົດຫຼັງຈາກການກົດບໍ່ພໍ່ເທົ່າໃດເຊັ່ນ: ການກວດ ສອບອາຍຸ ແລະ ອື່ນໆ. ສ່ວນໃນກໍລະນີອື່ນ ບາງເທື່ອນິກທີ່ນຳໃຊ້ມີຫຼາກຫຼາຍຂຶ້ນຄິດຄ້ຽວແລະສະຫຼັບຊັບຊ້ອນ, ເຖິງ ແມ່ນວ່າເຮົາຈະໄດ້ປິດອຸປະກອນໄປແລ້ວກໍ່ຕາມແຕ່ໜ້າຈໍການຮຽກເກັບຄ່າບໍລິການກໍ່ບໍ່ໄດ້ຫາຍໄປ.

※1 ປຸ່ອກແມ່ນຄຳສັ້ນຂອງເວັບປຸ່ອກທີ່ຢູ່ເທິງເວັບໄຊ ເຊິ່ງຜູ້ໃຊ້ສາມາດຂຽນຄວາມຄິດເຫັນຂອງຕົນເອງລົງໄດ້ ຫຼື ຄວາມຮູ້ສຶກຂອງຕົນເອງ ແລະ ຜູ້ທີ່ມາຢ້ຽມຊົມກໍ່ສາມາດໃຫ້ຄວາມຄິດເຫັນຂອງເຂົາໄດ້ເຊັ່ນດຽວກັນ

※2 SNS ແມ່ນຄຳສັບຫຍໍ້ຂອງບໍລິການເຄືອຂ່າຍສັງຄົມ ເຊິ່ງສະໜອງເວັບໄຊທີ່ມີຫຼາຍຟັງຊັນເຊັ່ນ: ການສະແດງສະໝຸດຮູບພາບໃຫ້ສາທາລະນະໄດ້ຊົມ ຫຼື ການສື່ສານພາຍໃນຊຸມຊົນ ເຊິ່ງຜູ້ຊົມໃຊ້ສາມາດແລກປ່ຽນຄວາມຄິດເຫັນຂອງຕົນໄດ້ຢ່າງອິດສະລະ

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ການກົດໄປທີ່ຟຼີຮູບພາບ ຫຼື ວິດີໂອຕ່າງໆທີ່ໜ້າສົນໃຈນັ້ນທ່ານຜູ້ໃຊ້ບໍລິການອາດນຳໄປສູ່ການຮຽກເກັບເງິນໂດຍບໍ່ໄດ້ຮັບອານຸຍາດ ຫຼື ໄປທີ່ເວັບໄຊຫຼອກຫຼວງ.

2 ມີບາງກໍລະນີທີ່ຢູ່ IP ※3 ຫຼື ຜູ້ສະໜອງຂໍ້ມູນໃຫ້ບໍລິການແມ່ນໄດ້ລະບຸໃບບິນໄວ້ເທິງໜ້າຈໍເພື່ອສ້າງຄວາມຢ້ານກົວໂດຍການເຮັດໃຫ້ເມັນເບິ່ງຄ້າຍຄືວ່າບຸກຄົນດັ່ງກ່າວໄດ້ຖືກລະບຸໄວ້.

※3 ທີ່ຢູ່ IP ແມ່ນໝາຍເລກທີ່ໄດ້ກຳນົດໃຫ້ຄອມພິວເຕີໂດຍອັດຕະໂນມັດ ເມື່ອເວລາມັນໄດ້ເຊື່ອມຕໍ່ເຂົ້າກັບອິນເຕີເນັດ

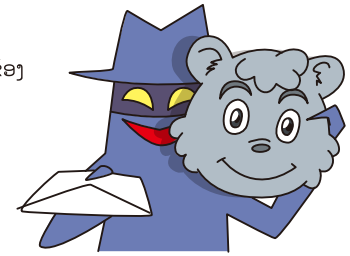
ມາດຕະການຕອບໂຕ້

- ໃຫ້ພະຍາຍາມປ້ອງກັນການເຊື່ອມຕໍ່ກັບເວັບໄຊທີ່ເປັນອັນຕະລາຍໂດຍໃຊ້ຊ່ອບແວໃນການກັ່ນກອງ ຫຼື ຊ່ອບແວຮັກສາຄວາມປອດໄພໃໝ່ລ່າສຸດ. ນອກຈາກນີ້ຈະຕ້ອງແນ່ໃຈວ່າການດາວໂຫຼດໂປຼແກຼມສະມາດໂຟນແມ່ນຈະຕ້ອງມາຈາກເວັບໄຊທີ່ໜ້າເຊື່ອຖືໄດ້ເທົ່ານັ້ນ.
- ຄວນຮັບຮູ້ວ່າເມື່ອເວລານຳໃຊ້ຄອມພິວເຕີ, ການກົດພຽງຄັ້ງດຽວຈະບໍ່ໄດ້ລະບຸຕົວຕົນຂອງທ່ານ, ສະນັ້ນບໍ່ຄວນຕອບສະໜອງຕໍ່ຄວາມພະຍາຍາມທີ່ຈະສໍ້ລະຄ່າໃຊ້ຈ່າຍນັ້ນ, ສຳລັບສະມາດໂຟນແລ້ວ ການນຳໃຊ້ໂປຼແກຼມນັ້ນເຮົາຄວນລະມັດລະວັງໃຫ້ຫຼາຍຂຶ້ນ, ເພາະຂໍ້ມູນທີ່ໄດ້ເກັບໄວ້ໃນອຸປະກອນແມ່ນຂໍ້ມູນຕິດຕໍ່ສະເພາະຂອງທ່ານເອງ ຫຼື ຂໍ້ມູນອື່ນໆທີ່ຢູ່ໃນສະໝຸດບັນຊີນັ້ນອາດຈະຖືກເປີດເຜີຍໄດ້.
- ຖ້າມີຫຍັງເກີດຂຶ້ນຄວນຕິດຕໍ່ມາໜຶ່ງໃນສະຖານທີ່ເຫຼົ່ານີ້, ຖ້າວ່າການຮຽກເກັບເງິນຍັງສືບຕໍ່ ຫຼື ຖ້າວ່າທ່ານໄດ້ຮັບຄຳສັ່ງສານ, ໃຫ້ປຶກສາອົງການທີ່ກ່ຽວຂ້ອງ (ໃຫ້ປຶກສາຜູ້ບໍລິຫານລະບົບ ຫຼື ທາງດ້ານກົດໝາຍ ແລະ ອື່ນໆ) ເພື່ອຂໍຄຳແນະນຳ.

ການໂຈມຕີທາງອີເມລທີ່ກຳນົດເປົ້າໝາຍ

ການໂຈມຕີທາງອີເມລທີ່ກຳນົດເປົ້າໝາຍແມ່ນການໂຈມຕີທີ່ໄດ້ສົ່ງອີເມລອອກໄປເພື່ອຫຼອກລວງຄ້າຍຄືກັບວ່າອີເມລດັ່ງກ່າວມາຈາກຄົນທີ່ເຮົາຮູ້ຈັກ, ເຊັ່ນເອກະສານຄັດຕິດທີ່ໄດ້ສົ່ງໄປຫານັ້ນເພື່ອໃຫ້ເຄື່ອງຂອງຜູ້ໃຊ້ງານຕິດເຊື້ອໄວຣັດສ.

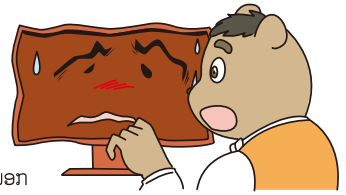
ຕົວຢ່າງທົ່ວໄປຂອງການໂຈມຕີແມ່ນເຈາະຈົງໄປທີ່ອົງການຈັດຕັ້ງໃດໜຶ່ງ ຫຼື ສະເພາະບຸກຄົນໃດໜຶ່ງ. ໄວຣັດສທີ່ໄດ້ຄັດຕິດ ມາກັບອີເມລແມ່ນຖືກສົ່ງມາຈາກຜູ້ທີ່ໂຈມຕີທີ່ອ້າງໂຕວ່າເປັນພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ຫຼື ເພື່ອນຮ່ວມງານຂອງອົງການຈັດຕັ້ງດຽວກັນ.



ກໍລະນີທີ່ໄດ້ຮັບລາຍງານວ່າລະຫັດຜ່ານຖືກລັກ ຫຼື ການຕິດເຊື້ອໄວຣັດສ, ແລະ ອື່ນໆ, ແມ່ນສາເຫດມາຈາກການໂຈມຕີ ທາງອີເມລທີ່ກຳນົດເປົ້າໝາຍ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ໃນການໂຈມຕີທີ່ຜ່ານມາ, ໄດ້ນຳໃຊ້ວິທີການປອມຕົວເປັນອີເມລທີ່ເຊື່ອຖືໄດ້, ເຊິ່ງໄດ້ເພີ່ມຄວາມຊັບຊ້ອນ ແລະ ທັນສະໄໝຂຶ້ນຢູ່ເລື້ອຍໆ ໂດຍການນຳໃຊ້ຊື່ຂອງກົມ/ພະແນກ ຫຼື ບຸກຄົນທີ່ມີຢູ່ຈິງ, ນອກເໜືອໄປຈາກນັ້ນຍັງໄດ້ມີການນຳໃຊ້ເນື້ອ ໃນ ຫຼື ຂໍ້ມູນທີ່ມີພຽງແຕ່ພາກສ່ວນທີ່ກ່ຽວຂ້ອງເທົ່ານັ້ນທີ່ຈະຮູ້.



2 ຖ້າໄວຣັດສໄດ້ຖືກຄັດຕິດມາ, ການເປີດເອກະສານທີ່ແນບມານັ້ນຈະສົ່ງຜົນໃນການຕິດຕໍ່ໄປຫາເຄື່ອງແມ່ຂ່າຍພາຍນອກ ໂດຍອັດຕະໂນມັດ ແລະ ຂໍ້ມູນຢູ່ພາຍໃນຄອມພິວເຕີກໍ່ຈະຖືກຮົ່ວໄຫຼອອກໄປ.

ມາດຕະການຕອບໂຕ້

- ຢ່າເປີດອີເມລ ຫຼື URL ທີ່ໜ້າສົງໃສຄັດຕິດມາ.
- ຖ້າຫາກວ່າທ່ານຫຼົງເປີດອີເມລທີ່ໜ້າສົງໃສ, ບໍ່ຕ້ອງຕົກໃຈພຽງແຕ່ປິດການທຳງານຂອງອຸປະກອນ. ຖອດສາຍເຊື່ອມຕໍ່ເຄືອຂ່າຍອອກ ແລະ ຂໍຄວາມຊ່ວຍເຫຼືອຈາກຜູ້ບໍລິຫານລະບົບ.
- ຕິດຕັ້ງໂປຼແກຼມປ້ອງກັນໄວຣັດສ ແລະ ໃຫ້ແນ່ໃຈວ່າມັນໄດ້ປັບປຸງຢ່າງສະໝ່ຳສະເໝີ.
- ນອກຈາກການປັບປຸງລະບົບປະຕິບັດການເປັນແຕ່ລະໄລຍະແລ້ວ ໂປຼແກຼມກໍ່ຕ້ອງໄດ້ປັບປຸງເຊັ່ນດຽວກັນ.

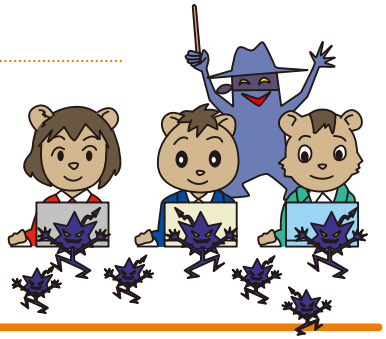
ການໂຈມຕີແບບ DDoS

ການໂຈມຕີແບບ DDoS ແມ່ນໜຶ່ງໃນການໂຈມຕີທີ່ເຈາະຈົງໄປຫາເຄື່ອງແມ່ຂ່າຍສະເພາະ ເຊິ່ງຈະຖືກໂຈມຕີໂດຍເຄື່ອງຄອມພິວເຕີທີ່ຮຸກຮານຜ່ານຫຼາຍໆເຄືອຂ່າຍພ້ອມກັນ, ຈົນເຮັດໃຫ້ສາຍການສື່ສານຄັບຄາແອອັດ ແລະ ໃນທີ່ສຸດເຄື່ອງແມ່ຂ່າຍກໍ່ຢຸດການທຳງານ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ຜູ້ບຸ່ຍຫວັງດີຈະເຊື່ອງຊ້ອນຕິດຕັ້ງໂປຼແກຼມທີ່ປະສົງຮ້າຍເພື່ອດຳເນີນການໂຈມຕີຄອມພິວເຕີທີ່ບໍ່ໄດ້ກ່ຽວຂ້ອງກັບເປົ້າໝາຍ (ເຄື່ອງແມ່ຂ່າຍ). ດັ່ງນັ້ນຜູ້ໃຊ້ອາດໂຈມຕີເຄື່ອງອື່ນໂດຍບໍ່ຮູ້ໂຕ.

2 ຄອມພິວເຕີທີ່ຖືກບຸກລຸກອາດດຳເນີນການໂຈມຕີອື່ນໆ ນອກເໜືອຈາກການໂຈມຕີແບບ DDoS ເຊັ່ນການຕິດເຊື້ອໄວຣັດສຕໍ່ກັບຄອມພິວເຕີອື່ນໆ, ການສົ່ງສະແປມອີເມລ ຫຼື ການເຮັດໃຫ້ເວັບໄຊຫຼົ້ມໃນຖານະຜູ້ໂຈມຕີ.



ມາດຕະການຕອບໂຕ້

- ຮັກສາລະບົບປະຕິບັດການຂອງເຄື່ອງຄອມພິວເຕີ, ສະມາດໂຟນ ຫຼື ອຸປະກອນອື່ນໆ ທີ່ເຊື່ອມຕໍ່ກັບອິນເຕີເນັດເພື່ອປັບປຸງໃຫ້ເປັນລຸ້ນລ່າສຸດຢູ່ສະເໝີ.
- ຕິດຕັ້ງໂປຼແກຼມປ້ອງກັນໄວຣັດສ ແລະ ໃຫ້ແນ່ໃຈວ່າມັນໄດ້ປັບປຸງຢ່າງສະໝ່ຳສະເໝີ.
- ນອກຈາກການປັບປຸງລະບົບປະຕິບັດການເປັນແຕ່ລະໄລຍະແລ້ວ ໂປຼແກຼມກໍ່ຕ້ອງໄດ້ປັບປຸງເຊັ່ນດຽວກັນ.

ມາລະຍາດເມື່ອນຳໃຊ້ອິນເຕີເນັດ

ເນື່ອງຈາກການໃຊ້ງານທີ່ໄດ້ເພີ່ມຂຶ້ນຂອງບໍລິການສັງຄົມອອນລາຍ, ບັນຫາທາງອິນເຕີເນັດທີ່ບໍ່ໄດ້ຄິດກ່ອນອາດມີຜົນຕາມມາ.

ມີຫຼາຍກໍລະນີທີ່ຜູ້ຊົມໃຊ້ອິນເຕີເນັດໄດ້ໂຟສ(ສົ່ງ)ຂໍ້ຄວາມເນື້ອຫາເພື່ອໃສ່ຮ້າຍປ້າຍສີເຮັດໃຫ້ບຸກຄົນ ຫຼື ບໍລິສັດໃດໜຶ່ງຕ້ອງໄດ້ອອກມາຂໍອະໄພຕໍ່ສາທາລະນະຊົນ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ມີຄວາມເປັນໄປໄດ້ວ່າການເຜີຍແຜ່ດ້ານບໍລິການເຄືອຂ່າຍສັງຄົມອາດຈະນຳໄປສູ່ການເປີດເຜີຍຂໍ້ມູນສ່ວນຕົວ ຫຼື ການໝິ່ນປະໝາດ ຫຼື ການລ່ວງລະເມີດຄວາມເປັນສ່ວນຕົວຂອງບຸກຄົນອື່ນ

2 ການໃສ່ຮ້າຍປ້າຍສີເທິງອິນເຕີເນັດອາດຈະສົ່ງຜົນໃຫ້ມີການຮ້ອງຟ້ອງຄ່າເສຍຫາຍ, ກ່າວຕຳນິຕິເຕືອນໂດຍລະບຽບກົດໝາຍ ຫຼື ກ້າວໄປເຖິງການຈັບກຸມ.

ມາດຕະການຕອບໂຕ້

- ລະມັດລະວັງບໍ່ໃຫ້ເປີດເຜີຍຂໍ້ມູນສ່ວນຕົວທີ່ບໍ່ຈຳເປັນໃນອິນເຕີເນັດໂດຍຜ່ານການບໍລິການເຄືອຂ່າຍສັງຄົມ (SNS) ບຼ໊ອກ ຫຼື ອື່ນໆ. ຮູບພາບທີ່ໂພສອາດຈະເປີດເຜີຍຂໍ້ມູນສະຖານທີ່ ດັ່ງນັ້ນທ່ານຄວນຈະລະມັດລະວັງ.
- ເຖິງແມ່ນວ່າຈະຢູ່ໃນອິນເຕີເນັດກໍ່ຕາມ, ເຮົາຄວນພິຈາລະນາສິດທິຄວາມເປັນສ່ວນຕົວຂອງຜູ້ອື່ນ ແລະ ກວດກາເບິ່ງເນື້ອໃນກ່ອນທີ່ຈະເຜີຍແຜ່ຂໍ້ມູນສູ່ສັງຄົມອອນລາຍ.

ການຕັ້ງຄ່າທີ່ເໝາະສົມຂອງລະຫັດປະຈຳຕົວ ແລະ ລະຫັດຜ່ານ

ເພື່ອທີ່ຈະນຳໃຊ້ອີເມລ, ອິນເຕີເນັດຊ່ອນປົ່ງ, ອິນເຕີເນັດແບ້ງຄິງ ແລະ ບໍລິການອື່ນໆທາງອິນເຕີເນັດຢ່າງປອດໄພ, ລະບົບ ກວດສອບຄວາມຖືກຕ້ອງມີຫຼາຍປະເພດ, ໃນຂະນະທີ່ເປັນທີ່ນິຍົມຫຼາຍທີ່ສຸດອີກອັນໜຶ່ງແມ່ນການປະສົມປະສານຂອງ ລະຫັດປະຈຳຕົວ ແລະ ລະຫັດຜ່ານ

ເມື່ອມໍ່ໆມານີ້ມີການໂຈມຕີເພີ່ມຂຶ້ນໃນໂລກໄຊເບີ ເຊິ່ງເປົ້າໝາຍແມ່ນຂໍ້ມູນບັນຊີຜູ້ໃຊ້ເຊັ່ນ: ລະຫັດປະຈຳຕົວ ແລະ ລະຫັດຜ່ານ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ບຸກຄົນທີສາມທີ່ເປັນອັນຕະລາຍອາດປອມຕົວເປັນຜູ້ໃຊ້ ແລະ ເປີດເຜີຍຂໍ້ມູນ ຫຼື ກໍ່ໃຫ້ເກີດຄວາມເສຍຫາຍທາງດ້ານການເງິນຖ້າລະຫັດປະຈຳຕົວ ແລະ ລະຫັດຜ່ານໃຊ້ແບບງ່າຍດາຍ(ເຊັ່ນ:ໝາຍເລກ 4 ຫຼັກ, ວັນເກີດ, ຫຼື "9999" ແລະ ອື່ນໆ) ຫຼື ຖ້າມັນຖືກປ່ອຍປະລະເລີຍ. (ຍົກຕົວຢ່າງເຊັ່ນ: ລະຫັດຜ່ານຕິດປະໄວ້ເທິງໜ້າຈໍ ແລະ ອື່ນໆ).

2 ຖ້າໃຊ້ລະຫັດປະຈຳຕົວ ແລະ ລະຫັດຜ່ານອັນດຽວກັນສຳລັບຫຼາຍໆເວັບໄຊ ແລະ ຂໍ້ມູນໄດ້ຖືກຮົ່ວໄຫຼຈາກເວັບໄຊໜຶ່ງ, ຄວາມເປັນໄປໄດ້ຂອງການຕົກເປັນເຫຍື່ອຈາກການໂຈມຕີໃນໂລກໄຊເບີຕໍ່ເວັບໄຊອື່ນໆກໍ່ຈະເພີ່ມຂຶ້ນ.

ມາດຕະການຕອບໂຕ້

- ຕັ້ງລະຫັດຜ່ານທີ່ຄາດເດົາບໍ່ໄດ້ ຈຳນວນຕົວອັກສອນທີ່ນຳໃຊ້ຢ່າງໜ້ອຍແມ່ນຍາວ 8 ຕົວ ປະສົມຕົວເລກ, ຕົວອັກສອນ ແລະ ສັນຍາລັກຕ່າງໆ ນອກຈາກນີ້ກໍ່ຄວນປ່ຽນລະຫັດຜ່ານເປັນປະຈຳ.
- ຢ່າເປີດເຜີຍລະຫັດຜ່ານໃຫ້ກັບບຸກຄົນອື່ນຮູ້ ຫຼື ໃຊ້ລະຫັດຜ່ານຊ້ຳກັນ(ຄືກັນ)ກັບຫຼາຍບໍລິການ. ຖ້າເວັບໄຊທີ່ທ່ານກຳລັງໃຊ້ງານຢູ່ນັ້ນແຈ້ງວ່າລະຫັດຜ່ານຂອງທ່ານຮົ່ວໄຫຼແມ່ນໃຫ້ປ່ຽນໃໝ່ທັນທີ.
- ຫຼີກລ້ຽງການປ້ອນຂໍ້ມູນສ່ວນຕົວ ຫຼື ຂໍ້ມູນທີ່ສຳຄັນໃສ່ຄອມພິວເຕີເມື່ອເວລາໃຊ້ຕາມສະຖານທີ່ສາທາລະນະເຊັ່ນ: ຮ້ານອິນເຕີເນັດຄາເຟ ແລະ ສະຖານທີ່ອື່ນໆ.

ສະແປມເມລ 1

ອີເມລແມ່ນອີກເຄື່ອງມືໜຶ່ງທີ່ຄ່ອນຂ້າງສື່ສານສະດວກສະບາຍໂດຍການສົ່ງ-ຮັບ ສາມາດດຳເນີນການໄດ້ໂດຍບໍ່ຕ້ອງຄຳນຶງວ່າສະຖານທີ່ຜູ້ຮັບນັ້ນຢູ່ໃສ ຫຼື ໄກປານໃດ. ເຖິງແນວໃດກໍ່ຕາມ, ຈາກຄວາມຄິດຂອງຜູ້ຮັບມັນອາດຈະມີຂໍ້ຄວາມອີເມລ ແລະ ສະແປມເປັນຈຳນວນຫຼວງຫຼາຍທີ່ຕິດມານຳໃນເວລາສົ່ງ ແລະ ຮັບ.

ເນື່ອງຈາກຂໍ້ຄວາມຂອງສະແປມເມລມີຈຳນວນຫຼວງຫຼາຍໄດ້ຖືກສົ່ງໄປນັ້ນ, ມັນກໍ່ໃຫ້ເກີດມີປັນຫາຢູ່ບ່ອນວ່າອຸປະກອນທີ່ໃຫ້ບໍລິການອຳນວຍຄວາມສະດວກນັ້ນອາດຈະເຮັດວຽກໜັກເກີນໄປ ເຊິ່ງອາດຈະນຳໄປສູ່ການສົ່ງແລະຮັບອີເມລລ່າຊ້າ.

ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ມີຫຼາຍກໍລະນີທີ່ເຄື່ອງຄອມພິວເຕີຈະສຸ່ມສ້າງທີ່ຢູ່ອີເມລອອກມາເປັນຈຳນວນຫຼວງຫຼາຍ ແລະ ກໍ່ສົ່ງຂໍ້ຄວາມອີເມລ. ດັ່ງນັ້ນ ອາດຈະສົ່ງຜົນໃຫ້ຄວາມເປັນໄປໄດ້ຂອງການຮັບສະແປມ ການໃຊ້ທີ່ຢູ່ອີເມລສັ້ນ ແລະ ຊື່ທີ່ນິຍົມໃນການຕັ້ງເປັນອີເມລນັ້ນ ນັ້ນເພີ່ມຂຶ້ນ.

2 ບາງສ່ວນຂອງການທຳນິດທີ່ຢູ່ອີເມລໃນການສົ່ງສະແປມເມລໄດ້ຖືກເກັບລວບລວມຜ່ານການລົງທະບຽນຄຳບໍລິການ ຫຼື ຜ່ານຂັ້ນຕອນການຍົກເລີກທີ່ສະແປມເມລສ້າງຂຶ້ນ.

3 ນອກຈາກນີ້ການເປີດໄຟລທີ່ແນບມາກັບອີເມລ ຫຼື ການເຂົ້າລິ້ງທີ່ມາກັບອີເມລນັ້ນອາດນຳໄປສູ່ການເບິ່ງເວັບໄຊທີ່ບໍ່ໄດ້ຮັບອານຸຍາດ ຫຼື ນຳໄປສູ່ການຕິດເຊື້ອໄວຣັດ.

ມາດຕະການຕອບໂຕ້

- ທີ່ຢູ່ອີເມລຄວນຈະມີທັ້ງຈຳນວນຕົວເລກ ແລະ ອັກສອນລວມກັນເພື່ອເຮັດໃຫ້ຍາກຕໍ່ການຄາດເດົາ.
- ຢ່າປ້ອນທີ່ຢູ່ອີເມລຂອງທ່ານເຂົ້າເວັບໄຊ ຫຼື ສະແດງທີ່ຢູ່ອີເມລຂອງທ່ານໄວ້ໃນເວັບໄຊ, ຖ້າບໍ່ຈຳເປັນ.
- ຖ້າມີຄວາມຈຳເປັນທີ່ຈະນຳໃຊ້ເວັບໄຊທີ່ອາດຈະບໍ່ໜ້າເຊື່ອຖືໄດ້ທັງໝົດນັ້ນ, ມັນອາດຈະມີປະສິດທິພາບໃນການນຳໃຊ້ທີ່ຢູ່ອີເມລທີ່ໃຊ້ໄດ້ຢ່າງມີອິດສະລະເມື່ອທຽບກັບການໃຊ້ອີເມລທີ່ຜູ້ໃຫ້ບໍລິການສະໜອງໃຫ້.

ສະແປມເມລ 2

ສະແປມເມລບໍ່ພຽງແຕ່ກໍ່ໃຫ້ເກີດຄວາມລຳຄານຕໍ່ກັບຜູ້ຮັບ ຫຼື ລົບກວນວຽກງານແລ້ວ, ແຕ່ຍັງເປັນວິທີທີ່ເຮັດໃຫ້ເປັນອັນຕະລາຍເພີ່ມຂຶ້ນ ແລະ ແນບນຽນອີກດ້ວຍ, ມັນອາດຈະນຳຜູ້ໃຊ້ເຊື່ອມໂຍງໄປຫາເວັບໄຊທ໌ທີ່ບໍ່ໄດ້ຮັບອານຸຍາດ ເຊິ່ງເປັນບ່ອນທີ່ເງິນອາດຈະຖືກລັກໄດ້ ຫຼື ໄປຜ່ານການຕັ້ງຄ່າຕົວກັ່ນກອງສະແປມເມລ.

ສະມາດໂຟນອາດຈະຕິດເຊື້ອໄວຣັດສທີ່ມາພ້ອມກັບສະແປມເມລ, ໂດຍທີ່ມີການເຄື່ອນຍ້າຍຈາກສະຖານທີ່ທີ່ຫ່າງໄກໃນການສົ່ງສະແປມເມລທີ່ມີຈຳນວນຫຼວງຫຼາຍເຂົ້າໄປໂດຍທີ່ຜູ້ໃຊ້ບໍ່ຮູ້ຕົວ.

! ຄວາມສ່ຽງ ແລະ ໄພຂົ່ມຂູ່

1 ມີຫຼາຍກໍລະນີທີ່ເຄື່ອງຄອມພິວເຕີຈະສຸ່ມສ້າງທີ່ຢູ່ອີເມລອອກມາເປັນຈຳນວນຫຼວງຫຼາຍ ແລະ ກໍ່ສິ່ງຂໍ້ຄວາມອີເມລ. ດັ່ງນັ້ນ ການໃຊ້ທີ່ຢູ່ອີເມລສັ້ນ ແລະ ຊື່ທີ່ນິຍົມໃນການຕັ້ງເປັນອີເມລນັ້ນ ອາດຈະສົ່ງຜົນໃຫ້ຄວາມເປັນໄປໄດ້ຂອງການຮັບສະແປມ ນັ້ນເພີ່ມຂຶ້ນ.

2 ບາງສ່ວນຂອງການກຳນົດທີ່ຢູ່ອີເມລໃນການສົ່ງສະແປມເມລໄດ້ຖືກເກັບລວບລວມຜ່ານການລົງທະບຽນຄ່າບໍລິການ ຫຼື ຜ່ານຂັ້ນຕອນການຍົກເລີກທີ່ສະແປມເມລສ້າງຂຶ້ນ.

3 ນອກຈາກນີ້ການເປີດໄຟລທີ່ແນບມາກັບອີເມລ ຫຼື ການເຂົ້າລິ້ງທີ່ມາກັບອີເມລນັ້ນອາດນຳໄປສູ່ການເບິ່ງເວັບໄຊທ໌ທີ່ບໍ່ໄດ້ຮັບອານຸຍາດ ຫຼື ນຳໄປສູ່ການຕິດເຊື້ອໄວຣັດສ.

ມາດຕະການຕອບໂຕ້

- ພະຍາຍາມທີ່ຈະປິດກັ້ນສະແປມເມລໂດຍການໃຊ້ບໍລິການຕອບໂຕ້ເຊັ່ນ: ຟັງຊັນປະຕິເສດເມລ ຫຼື ຟັງຊັນປ້ອງກັນການປອມແປງໂດຍຜູ້ໃຫ້ບໍລິການອິນເຕີເນັດ ຫຼື ຊ໋ອບແອກັ່ນກອງສະແປມເມລນັ້ນ.
- ຖ້າວ່າທ່ານໄດ້ຮັບສະແປມເມລ, ໃຫ້ລຶບຖິ້ມໂດຍບໍ່ຕ້ອງເປີດມັນ. ເຊັ່ນດຽວກັນກໍ່ບໍ່ຄວນເປີດໄຟລທີ່ແນບມາ ຫຼື ເຂົ້າຫາລິ້ງທີ່ມາກັບອີເມລທີ່ໜ້າສົງໃສ. ມັນອາດຈະສົ່ງຕໍ່ໄປຫາຜູ້ໃຫ້ບໍລິການ ຫຼື ໜ່ວຍງານຂອງລັດຖະບານ.
- ໃຊ້ມາດຕະການຕອບໂຕ້ໃຫ້ກັບສະມາດໂຟນເຊັ່ນດຽວກັນກັບຄອມພິວເຕີ.

ປ້ອງກັນຄອມພິວເຕີ ແລະ ສະມາດໂຟນດ້ວຍຕົວຂອງທ່ານເອງ

ສະມາດໂຟນ ແລະ ຄອມພິວເຕີ ແມ່ນເຄື່ອງມືທີ່ເປັນປະໂຫຍດ, ແຕ່ອີກດ້ານໜຶ່ງພວກມັນປະເຊີນກັບອັນຕະລາຍຫຼາຍຢ່າງເຊັ່ນ: ການຕິດເຊື້ອໄວຣັດສຄອມພິວເຕີ.
ຢ່າລືມປະຕິບັດຕາມສາມເຄັດລັບສຸດຍອດຂອງຄວາມປອດໄພຂໍ້ມູນຂ່າວສານເພື່ອໃຫ້ແນ່ໃຈວ່າມີຄວາມປອດໄພເມື່ອເວລາໃຊ້ຄອມພິວເຕີ ແລະ ສະມາດໂຟນ.

ສາມເຄັດລັບສຸດຍອດຂອງຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ

ບໍລິຫານຂໍ້ມູນສ່ວນຕົວທີ່ສຳຄັນດ້ວຍຄວາມເອົາໃຈໃສ່.

ປົກປ້ອງຄອມພິວເຕີຂອງທ່ານດ້ວຍການປັບປຸງຄວາມປອດໄພໃຫ້ໃໝ່ລ່າສຸດ.

ຢ່າເຂົ້າຫາເວັບໄຊທ໌ທີ່ໜ້າສົງໃສ ຫຼື ອີເມລທີ່ບໍ່ຄຸ້ນເຄີຍ.

ມາດຕະການຮັກສາຄວາມປອດໄພແມ່ນບໍ່ພຽງແຕ່ປະຕິບັດໄດ້ເມື່ອເຮົານຳໃຊ້ຄອມພິວເຕີ ຫຼື ສະມາດໂຟນເທົ່ານັ້ນ
ການຂັບຍານພາຫະນະກໍ່ເຊັ່ນດຽວກັນເຮົາຄວນໃສ່ສາຍຮັດນິລະໄພໄວ້ເພື່ອປ້ອງກັນຕົນເອງ
ສິ່ງທີ່ບໍ່ຄວນລືມ