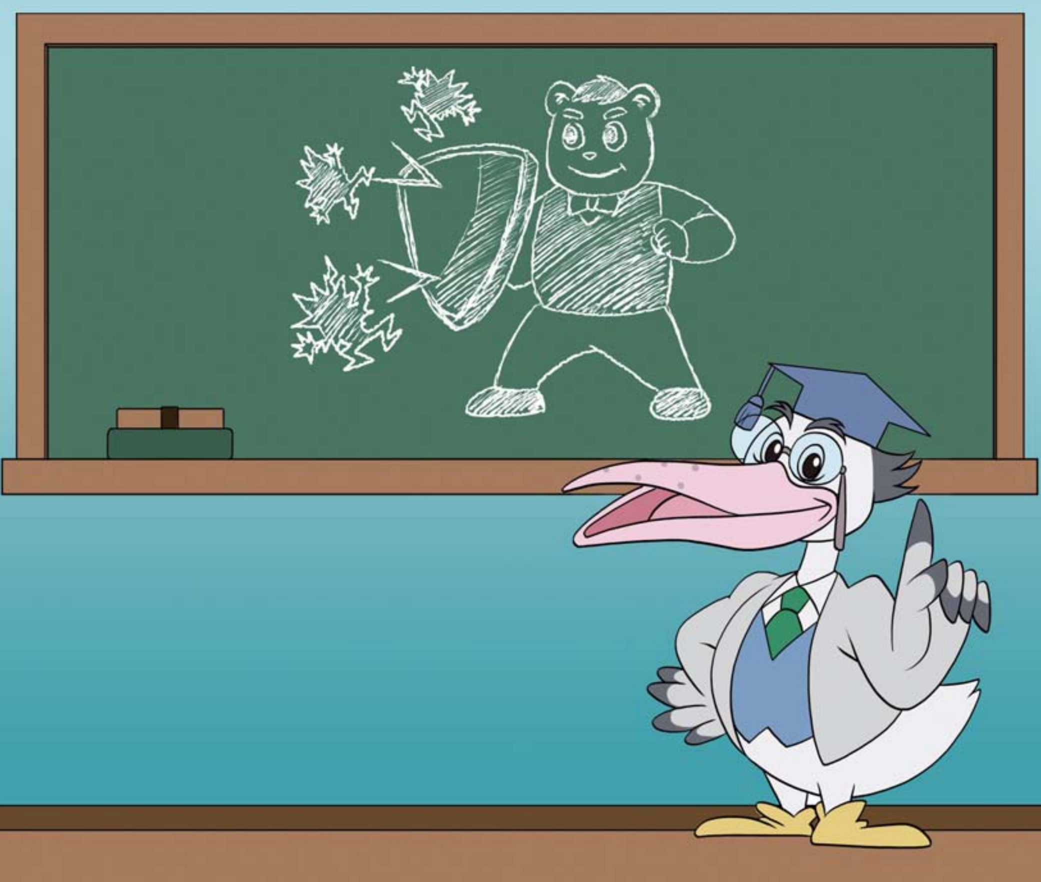
ມັງງະ

ເຮົາມາຮຽນຮູ້ການຮັກສາຄວາມ ປອດໄພທາງໄຊເບີກັນເທ໊າະ

ຮູ້ທັນ, ປ້ອງກັນ, ແລະ ລະມັດລະວັງ



ຄວາມປອດໄພໃນສະມາດໂຟນ

ພາກ 1

ມັນເກີດຫຍັງຂຶ້ນ?
ແຈ້ງເຕືອນ!
ສະມາດໂຟນຂອງທ່ານໄດ້ຖືກລ໋ອກໄວ້
ເພາະພວກເຮົາໄດ້ກວດພົບແອັບພິເຄ
ຊັ່ນທີ່ຜິດກົດໝາຍຢູ່ໃນສະມາດ
ໂຟນຂອງທ່ານ.
ເພື່ອປົດລ໋ອກສະມາດໂຟນຂອງທ່ານ,
ກະລຸນາຈ່າຍເງິນ 5,000,000 ກີບ
ພາຍໃນສາມມື້.
ສະມາດໂຟນຂອງທ່ານຈະຖືກລ໋ອກໄວ້
ຈົນກວ່າທ່ານຈະຈ່າຍເງິນ.
ຊວຍແລ້ວ! ສະມາດໂຟນຂອງ ຂ້ອຍໃຊ້ງານຫຍັງ ບໍ່ໄດ້ເລີຍ!
ຂ້ອຍຄວນຈະ ເຮັດແນວໃດດີ?
ການລະເມີດກົດໝາຍ
ຂ້ອຍບໍ່ຮູ້ວ່າຈະ ຕ້ອງໄປປຶກສາໃຜ
ດີລະ, ຂ້ອຍຈະຈ່າຍ ແລະ ຂ້ອຍຫວັງວ່າມັນຈະ ໃຊ້ງານໄດ້ຄືເກົ່າ.

ທະນາຄານ XX
ທຸກຢ່າງມັນກໍ່ດີໝົດຢູ່ດອກ. ແຕ່ວ່າມັ້ນຄື ມາແພງແທ້!
ເອົາລະ, ບາດນີ້ສະມາດໂຟນຂອງຂ້ອຍກໍຊິໃຊ້ງານໄດ້ປົກກະຕິແລ້ວ...
...ຮະ...
...ແມ່ນຫຍັງອີກແລ້ວ!?
ສະມາດໂຟນຂອງທ່ານບໍ່ສາມາດປົດລ໋ອກໄດ້.
ດ໋ອກເຕີ! ຊ່ວຍຂ້ອຍແດ່?
ເກີດຫຍັງຂຶ້ນກັບເຈົ້າ?
ຂ້ອຍຈ່າຍເງິນໄປແລ້ວ ແຕ່ສະມາດໂຟນຂອງຂ້ອຍມັນຍັງຕິດລ໋ອກຢູ່.
ມັນຕ້ອງແມ່ນການຫຼອກລວງຢ່າງແນ່ນອນ.
ໄວຣັສມັກຈະພົບເຫັນຢູ່ໃນແອັບພິເຄຊັ່ນຟຣີ.
ດັ່ງນັ້ນ, ເຈົ້າຈະຕ້ອງຕິດຕັ້ງຊ໋ອບແວປ້ອງກັນໄວຣັສ ແລະ ດາວໂຫຼດສະເພາະແອັບທີ່ມາຈາກແຫຼ່ງທີ່ນ່າເຊື່ອໄດ້ເທົ່ານັ້ນ.
ເຂົ້າໃຈແລ້ວ!

NO.1 [ສະຫຼູບ] ຄວາມປອດໄພໃນສະມາດໂຟນ

ລະມັດລະວັງ!

- ໄວຣັສບໍ່ພຽງແຕ່ມີຢູ່ໃນຄອມພິວເຕີເທົ່ານັ້ນ ແຕ່ມັນຍັງມີຢູ່ໃນສະມາດໂຟນອີກດ້ວຍ.
- ອຸປະກອນຂອງທ່ານ (ຄອມພິວເຕີ ຫຼື ສະມາດໂຟນ) ອາດຈະຕິດໄວຣັສ ຜ່ານທາງການດາວໂຫຼດ "ແອັບພິເຄຊັນຟຣີ".
- ຄອມພິວເຕີ ຫຼື ສະມາດໂຟນຂອງທ່ານ ອາດຈະຕິດໄວຣັສ ເມື່ອທ່ານບໍ່ປັບປຸງລະບົບປະຕິບັດການ ຫຼື ແອັບພິເຄຊັນ.

ມາດຕະການ

- ຕິດຕັ້ງຊອບແວປ້ອງກັນໄວຣັສໃນຄອມພິວເຕີ ແລະ ສະມາດໂຟນຂອງທ່ານ.
- ດາວໂຫຼດສະເພາະແອັບພິເຄຊັນທີ່ມາຈາກແຫຼ່ງທີ່ນ່າເຊື່ອຖື ໂດຍການກວດສອບຄໍາບັນຍາຍ, ຜູ້ເຜີຍແຜ່, ການມີຕົວຕົນຂອງບໍລິສັດ, ແງ່ມຸມຂອງຄໍາຄິດເຫັນ ແລະ ອື່ນໆ
- ປັບປຸງແອັບພິເຄຊັນ ແລະ ລະບົບປະຕິບັດການໃຫ້ຢູ່ໃນສະພາບໃໝ່ລ່າສຸດສະເໝີ.

ເລື່ອງງ່າຍໆ

- **Ransomware** (ເປັນເມົາແວຊະນິດໜຶ່ງທີ່ລອກໜ້າຈໍຂອງຄອມພິວເຕີ ແລະ ສະມາດໂຟນ ຫຼັງຈາກນັ້ນມັນຈະໃຫ້ທ່ານຈ່າຍເງິນເພື່ອປົດລອກ) ມັນເກີດຂຶ້ນມາແລ້ວໃນທົ່ວໂລກ
  ລະມັດລະວັງ **Ransomware** ບໍ່ພຽງແຕ່ພົບເຫັນຢູ່ຄອມພິວເຕີເທົ່ານັ້ນ ແຕ່ມັນຍັງເກີດຂຶ້ນຢູ່ໃນສະມາດໂຟນອີກດ້ວຍ
- ບໍ່ຄວນເປີດໄຟລ໌ທີ່ຄັດຕິດມາໃນອີເມວຂີ້ເຫຍື້ອ, ຖ້າບໍ່ດັ່ງນັ້ນອຸປະກອນຂອງທ່ານອາດຈະຕິດໄວຣັສນີ້.

ພາກ2

ຄວາມປອດໄພຂອງເຄືອຂ່າຍໄຮ້ສາຍ

ປັດຈຸບັນນີ້, ຂ້ອຍໄດ້ຮັບອີເມວ ຂີ້ເຫຍື້ອຢ່າງຫຼວງຫຼາຍ
ທ່ານໄດ້ຮັບອີເມວໃໝ່ 320 ອີເມວ
ມີສິ່ງແປກ ປະຫຼາດໄດ້ ເກີດຂຶ້ນອີກ
ມີສາຍໂທ ເຂົ້າມາ!
ມີສາຍໂທເຂົ້າມາ ອີກແລ້ວ 30 ສາຍ
ຍິ່ງໄປກວ່ານັ້ນ ...
ເຈົ້າແນ່ ໃຈຫວາ!?
ຂ້ອຍປະຫຼາດໃຈຫຼາຍ ເພາະວ່າຂ້ອຍໄດ້ເຫັນຮູບ ຂອງເຈົ້າຕອນທີ່ຫຼິ້ນ ອິນເຕີເນັດມື້ວານນີ້!
ແມ່ນຫຍັງນີ?
ຂ້ອຍບໍ່ເຄີຍໂພສຮູບນີ້ລົງໃນ ສື່ສັງຄົມອອນລາຍຈັກເທື່ອ.
ທ້າວ Anonymity
ເຮ້..., ເຈົ້າຄິດວ່າສາວນີ້ໜ້າຮັກບໍ່?

ອ້ະ ອ້າ ອ້າ....
ໂອ້ຍ...! ເກີດບັນຫານີ້ຂຶ້ນໄດ້ແນວໃດ?
ດ໋ອກເຕີ້! ຮູບພາບຂອງຂ້ອຍກຳລັງຖືກເຜີຍແຜ່ຢູ່ເທິງອິນເຕີເນັດ!
ໂອ ນາງເອີຍ! ເຈົ້າພົບບັນຫາທີ່ຮ້າຍແຮງແລ້ວ.
ມີສິ່ງແປກໆໄດ້ເກີດຂຶ້ນກັບຂ້ອຍມາຕະຫຼອດ, ຕັ້ງແຕ່ຂ້ອຍໄດ້ໄປຫຼິ້ນ ວາຍ-ຟາຍ ຟຣີ ຢູ່ສວນສາທາລະນະ.
ນີ້ແຫລະແມ່ນເຫດຜົນ. ມັນອັນຕະລາຍເມື່ອຫຼິ້ນອິນເຕີເນັດຜ່ານ ວາຍ-ຟາຍ ທີ່ບໍ່ຮູ້ແຫຼ່ງທີ່ມາ!
ສະນັ້ນ, ເຈົ້າຕ້ອງໃຊ້ ວາຍ-ຟາຍ ຈາກແຫຼ່ງທີ່ໜ້າເຊື່ອຖືໄດ້ເທົ່ານັ້ນ.
ຂ້ອຍບໍ່ຮູ້ວ່າມັນອັນຕະລາຍ. ຂ້ອຍໃຊ້ກໍ່ເພາະວ່າມັນຟຣີ.
ຕັ້ງແຕ່ນີ້ໄປ, ຂ້ອຍຈະລະມັດລະວັງໃຫ້ຫຼາຍຂຶ້ນ ຈະບໍ່ຫຼິ້ນ ວາຍ-ຟາຍ ຟຣີອີກ.

NO.2 [ສະຫຼຸບ] ຄວາມປອດໄພຂອງເຄືອຂ່າຍໄຮ້ສາຍ

ລະມັດລະວັງ!

- ວາຍ-ຟາຍ ບາງບ່ອນກໍ່ມີຈຸດປະສົງໃຫ້ຜູ້ຊົມໃຊ້ຕິດໄວຣັສ
- ໃຫ້ລະມັດລະວັງບາງຄົນອາດຈະດັກຈັບການສື່ສານຂອງທ່ານ ເມື່ອເວລາທ່ານເຂົ້ານຳໃຊ້ ວາຍ-ຟາຍ ທີ່ອັນຕະລາຍ
- ເຖິງວ່າທ່ານຈະໃຊ້ເຄືອຂ່າຍໄຮ້ສາຍສາທາລະນະຈາກຜູ້ໃຫ້ບໍລິການອິນເຕີເນັດທີ່ເຊື່ອຖືໄດ້ກໍ່ຕາມ, ການສື່ສານຂອງທ່ານກໍ່ຍັງຈະຖືກດັກຈັບ ຖ້າບໍ່ມີການເຂົ້າລະຫັດ.

ມາດຕະການ

- ບໍ່ຄວນ ເຊື່ອມຕໍ່ ວາຍ-ຟາຍ ສາທາລະນະທີ່ບໍ່ຮູ້ຈັກ/ບໍ່ໜ້າເຊື່ອຖື.
- ນຳໃຊ້ ວາຍ-ຟາຍ ທີ່ມີການເຂົ້າລະຫັດ, ຖ້າທ່ານຕ້ອງການເຊື່ອມຕໍ່ ວາຍ-ຟາຍ ສາທາລະນະ.

ເລື່ອງງ່າຍໆ

- ໃຫ້ລະມັດລະວັງການຕັ້ງຄ່າ ເມື່ອນຳໃຊ້ ວາຍ-ຟາຍ ສາທາລະນະ. ຂໍ້ມູນຂອງທ່ານສາມາດຖືກພົບເຫັນໄດ້ ໂດຍຜູ້ທີ່ໃຊ້ ວາຍ-ຟາຍ ດຽວກັນ, ຖ້າທ່ານເປີດໃຊ້ງານ"ການແບ່ງປັນຂໍ້ມູນ" ໃນຄອມພິວເຕີ ຫຼື ສະມາດໂຟນ.
- ໃຫ້ແນ່ໃຈວ່າ ວາຍ-ຟາຍ ຂອງທ່ານໃຊ້ລະຫັດຜ່ານທີ່ສະຫຼັບສັບຊ້ອນ. ບໍ່ຄວນ ອະນຸຍາດໃຫ້ຄົນແປກໜ້າເຂົ້າເຖິງມັນ.

ການຫຼອກລວງທາງອິນເຕີເນັດ.

ພາກ3

ທະນາຄານ XX
ຮຽບຮ້ອຍ! ຂ້ອຍໄດ້ຊຳລະເງິນ ແລ້ວ, ທີ່ເຫຼືອກໍ່ມີແຕ່ ລໍຖ້າເທົ່ານັ້ນ.
ຂ້ອຍໄດ້ຊື້ກະເປົ໋າທີ່ຂ້ອຍ ຕ້ອງການແລ້ວ ເຊິ່ງມີສ່ວນຫຼຸດເຖິງ 90%.
ໂອ້! ແທ້ຫວານິ?
ໜຶ່ງເດືອນຕໍ່ມາ.
ຮື໋...ກະເປົ໋າຍັງມາ ບໍ່ຮອດປານນີ້.
Pi
Pi
ເຂົ້າໄປກວດສອບ ຢູ່ເວັບໄຊຮ້ານຂາຍ ເຄື່ອງດີກວ່າ.
ໂອ້, ມັນເກີດ ຫຍັງຂຶ້ນນິ?
ໜ້າເວັບໄຊປິດແລ້ວ! ຂ້ອຍຕ້ອງໂທຫາຮ້ານຂາຍເຄື່ອງ!
404 Not Found.
ໜ້ານີ້ປະຈຸບັນ ບໍ່ໄດ້ນຳໃຊ້ແລ້ວ.

ຂ້ອຍໄດ້ຊື້ກະເປົ໋າຈາກຮ້ານຄ້າອອນລາຍຂອງເຈົ້າເດືອນກ່ອນ ແຕ່ຂ້ອຍຍັງບໍ່ໄດ້ຮັບເຄື່ອງປານນີ້.
ຂ້ອຍຂໍໂທດຫຼາຍໆເດີ້ ພວກເຮົາບໍ່ມີຮ້ານຄ້າອອນລາຍ.
ຂ້ອຍຢ້ານວ່າມັນຕ້ອງມີຫຍັງເຂົ້າໃຈຜິດກັນຢ່າງແນ່ນອນ...
ຫາ໋...!?
ດ໋ອກເຕີ!
ນັ້ນມັນແມ່ນການຫຼອກຫຼວງທາງອິນເຕີເນັດປະເພດໜຶ່ງ.
ການຫຼອກຫຼວງທີ່ມີຢູ່ໃນອິນເຕີເນັດ, ເຊັ່ນ: ການຊື້ສິນຄ້າອອນລາຍເພື່ອຕົວະເອົາເງິນຂອງເຈົ້າ
ເຈົ້າຕ້ອງກວດສອບວ່າທີ່ຢູ່ເວັບໄຊ ຫຼື ຜູ້ສົ່ງອີເມວແມ່ນຂອງແທ້ ຫຼື ຂອງປອມ.
ບໍ່ມີການຊື້ຂາຍທີ່ຖືກປານນີ້. ຈາກນີ້ໄປຂ້ອຍຈະກວດສອບກ່ອນທຸກຄັ້ງ.

NO.3 [ສະຫຼຸບ] ການຫຼອກລວງທາງອິນເຕີເນັດ.

ລະມັດລະວັງ!

- ທ່ານອາດຈະພົບເຈີກັບການຫຼອກລວງໃນອິນເຕີເນັດ ເມື່ອທ່ານນໍາໃຊ້ການຊື້ເຄື່ອງອອນລາຍ ຫຼື ການໃຊ້ບໍລິການຂອງທະນາຄານທາງອິນເຕີເນັດ.
- ການຫຼອກລວງຜູ້ໃຊ້ ໄປສູ່ເວັບໄຊປອມທີ່ມີຄວາມຄ້າຍຄືກັບເວັບໄຊຈິງ ເຊິ່ງກໍາລັງເພີ່ມຂຶ້ນເລື້ອຍໆ.
- ທ່ານອາດຈະຖືກຫຼອກລວງເຂົ້າສູ່ເວັບໄຊປອມ ຫຼື ຕິດໄວຣັສ ຖ້າທ່ານເປີດເວັບໄຊ ຫຼື ໄຟລ໌ທີ່ໄດ້ຄັດຕິດມານໍາອີເມວຂີ້ເຫຍື້ອ.

ມາດຕະການ

- ໃຫ້ກວດສອບຢ່າງລະມັດລະວັງວ່າ ທີ່ຢູ່ເວັບໄຊ ຫຼື ຜູ້ສົ່ງອີເມວ ມີຄວາມຖືກຕ້ອງ.
- ຢ່າເຂົ້າເວັບໄຊທີ່ໜ້າສົງໄສ ຊຶ່ງພາສາມີຄວາມຜິດພ້ຽນ ຫຼື ບໍ່ມີຂໍ້ມູນໃນການຕິດຕໍ່ (ຫຼື ເປັນຂໍ້ມູນການຕິດຕໍ່ປອມ) ແລະ ອື່ນໆ

ເລື່ອງງ່າຍໆ

- ລະມັດລະວັງເວັບໄຊຫຼອກລວງ ເຊັ່ນ ເວັບໄຊທະນາຄານປອມ. ເວັບໄຊເຫຼົ່ານີ້ກໍາລັງແຜ່ຫຼາຍ ແລະສາມາດລັກເອົາຊື່ຜູ້ໃຊ້ ຫຼື ລະຫັດຜ່ານ ເພື່ອຄວບຄຸມບັນຊີການເຄື່ອນໄຫວທຸລະກໍາທາງການເງິນຜ່ານອິນເຕີເນັດ (ລັກເອົາເງິນຂອງທ່ານ)

ຄຳແນະນຳສຳລັບການ ນຳໃຊ້ສື່ສັງຄົມອອນລາຍ

ພາກ4

SNS : Social Networking Service

ແຕ່ວ່າ,
ເປັນຫຍັງຄືເລືອກ
ສະຖານທີ່ແບບນີ້ນໍ້?
ຄືວ່າບໍ່ມີໃຜ
ຢູ່ນີ້ຈັກຄົນ.
ແປະ!
ໂອະ?
ສະບາຍດີ!
ໂອ້...
ເອົາເງິນ
ມາ!
ໂອ້, ບໍ່!

ພວກເຂົາເອົາເງິນຂ້ອຍໄປໝົດເລີຍ
ແລະ ຂ້ອຍໝົດໂຕແລ້ວຕອນນີ້..
ມື້ນີ້ຂ້ອຍບໍ່ຢາກເຮັດຫຍັງແລ້ວ..
ຮູ້ສຶກຜິດຫວັງແທ້ໆ...
ຂ້ອຍຕ້ອງຍົກ
ເລີກນັດມື້ນີ້.
ແມ່ນຫຍັງ.....!
ເປັນຫຍັງລາວ
ຄືອອກຈາກ
ລະບົບ?
ຫວັງວ່າເຮົາຊິໄດ້ພົບ
ກັນເນາະມື້ອື່ນ.
ຕົກລົງ!
ແລ້ວພົບກັນເນາະ!
ລັບບິດ ທາໂລ້ ໄດ້ອອກຈາກລະບົບ!.
ໂອ້, ເຈົ້າຮູ້ໂຕບໍ່ວ່າເຈົ້າຖືກຕົວະແລ້ວ
ຖືກຕົວະຫວາ?
ການລັກເອົາຂໍ້ມູນ
ສ່ວນຕົວເປັນເລື່ອງ
ທີ່ງ່າຍດາຍໃນ
ສື່ສັງຄົມອອນລາຍ.
ທ່ານອາດມີສ່ວນ
ກ່ຽວຂ້ອງໃນການກໍ່
ອາຊະຍາກຳໂດຍການ
ລັກເອົາຂໍ້ມູນສ່ວນຕົວ.
ທ່ານບໍ່ຄວນຕິດຕໍ່ກັບຄົນທີ່ທ່ານ
ບໍ່ຮູ້ຈັກ. ມັນເປັນໄປບໍ່ໄດ້ດອກ
ທີ່ຈະໄດ້ພົບກັບບຸກຄົນທີ່ບໍ່ຮູ້ຈັກ
ເຫຼົ່ານັ້ນໃນຊີວິດຈິງ.
ແມ່ນຫຍັງ ຂ້ອຍຖືກ
ຕົວະຫວານີ....,
ແຕ່ນີ້ຕໍ່ໄປຂ້ອຍ
ຈະລະມັດລະວັງໃນການ
ນຳໃຊ້ ສື່ສັງຄົມອອນລາຍ
ໃຫ້ຫຼາຍຂຶ້ນ.
ໂອ້, ຫຸ່ນຍົນ
ຈຳລອງ....

NO.4 [ສະຫຼຸບ] ຄຳແນະນຳສຳລັບການນຳໃຊ້ສື່ສັງຄົມອອນລາຍ

ລະມັດລະວັງ!

- ບຸກຄົນທີ່ບໍ່ຫວັງດີອາດປອມຕົວມາເປັນບຸກຄົນທີ່ທ່ານສົນໃຈ ໂດຍໃຊ້ຮູບພາບຂອງຄົນອື່ນ ເພື່ອຕິດຕໍ່ຫາທ່ານ.
- ບຸກຄົນທີ່ບໍ່ຫວັງດີອາດຈະເວົ້າວ່າ " ຂ້ອຍຢາກພົບເຈົ້າເປັນການສ່ວນຕົວ " ເຊິ່ງອາດຈະພາໄປສູ່ການເກີດອາຊະຍາກຳ.
- ໃນກໍລະນີທີ່ຮ້າຍແຮງໄປກວ່ານັ້ນ, ເຈົ້າອາດຈະມີສ່ວນພົວພັນກັບການກໍ່ອາຊະຍາກຳເຊັ່ນ: ການລັກພາຕົວ, ການຄ້າມະນຸດ ແລະ ອື່ນໆ.

ມາດຕະການ

- ບໍ່ຄວນຕິດຕໍ່ກັບບຸກຄົນທີ່ທ່ານບໍ່ຮູ້ຈັກ.
- ບໍ່ຄວນໄປພົບກັບບຸກຄົນທີ່ບໍ່ຮູ້ຈັກເປັນການສ່ວນຕົວ ເຖິງແມ່ນວ່າພວກເຂົາຢາກພົບທ່ານກໍ່ຕາມ.

ເລື່ອງງ່າຍໆ

- ຄົນແປກໜ້າຈະຕິດຕໍ່ຫາທ່ານເລື້ອຍໆ ເຊິ່ງອາດຈະນຳທ່ານໄປສູ່ການກໍ່ອາຊະຍາກຳ.
- ບໍ່ຄວນໃຫ້ຂໍ້ມູນສ່ວນຕົວກັບຄົນແປກໜ້າເຊັ່ນ: ຊື່, ຮູບ, ເບີໂທລະສັບ, ທີ່ຢູ່ ແລະ ອື່ນໆ.
- ລະວັງບາງຄັ້ງບຸກຄົນທີ່ບໍ່ຫວັງດີ ອາດປອມມາເປັນໝູ່ຂອງທ່ານ ດັ່ງນັ້ນ ໃຫ້ແນ່ໃຈວ່າບຸກຄົນນັ້ນແມ່ນຄົນທີ່ທ່ານຮູ້ຈັກແທ້.

ການນຳໃຊ້ອິນເຕີເນັດແມ່ນ ມີຄວາມສ່ຽງຫຼາຍ.
ຢ່າງໃດກໍ່ຕາມ, ພວກເຮົາສາມາດເຊື່ອມຕໍ່ກັບ ຜູ້ຄົນໃນທົ່ວໂລກໄດ້ ຖ້າພວກເຮົາໃຊ້ອິນເຕີເນັດ ຢ່າງຖືກຕ້ອງ!
ນຳໃຊ້ອິນເຕີເນັດໃຫ້ມີຄວາມປອດໄພໂດຍໃຊ້ ມາດຕະການຮັກສາຄວາມປອດໄພທາງໄຊເບີ

ຮູ້ທັນ, ປ້ອງກັນ, ແລະ ລະມັດລະວັງ

知る　守る　続ける

ASEAN · JAPAN
Information Security Awareness