ນຳໃຊ້ອິນເຕີເນັດໃຫ້ປອດໄພ

- ໂພສເຕີລາວເຊີດ
- ປ້ອງກັນໂຕເອງບໍ່ໃຫ້ຕົກເປັນເຫຍື່ອທາງອິນເຕີເນັດ
- ການປ້ອງກັນລະຫັດຜ່ານ
- ໄພຄຸກຄາມຕ່າງໆ ທາງອິນເຕີເນັດ
- ສື່ສັງຄົມອອນລາຍ
- ການນຳໃຊ້ສະມາດໂຟນ

“ ຮູ້ທັນ, ປ້ອງກັນ ແລະ ລະມັດລະວັງໄພທາງອິນເຕີເນັດ “

ໂພສເຕີ ລາວເຊີດ

ຢ່າປ່ອຍໃຫ້ຕົວທ່ານ ຕົກເປັນເຫຍື່ອທາງອິນເຕີເນັດ

Don't Fall Into Cyber Trap

ການປ້ອງກັນສາມາດເຮັດໄດ້ດ້ວຍຕົວທ່ານເອງ

You are your own protection

LaoCERT
Lao Computer Emergency Response Team

ຮັກສາຂໍ້ມູນໃຫ້ມີຄວາມປອດໄພ

- ຄວາມປອດໄພສະມາດໂຟນ
- ວາຍເລັສແລນ (ເຄື່ອຂ່າຍໄຮ້ສາຍ)
- ໜຶ່ງ-ຄຼິກ ສໍ້ໂກງ
- ການໂຈມຕີທາງອີເມລ
- ການໂຈມຕີແບບ DDoS
- ມາລະຍາດເມື່ອນຳໃຊ້ອິນເຕີເນັດ
- ການຕັ້ງຄ່າທີ່ເໝາະສົມຂອງລະຫັດຜ່ານ
- ສະແປມເມລ

LaoCERT
Lao Computer Emergency Response Team

ປ້ອງກັນໂຕເອງຈາກການຕົກເປັນເຫຍື່ອທາງອິນເຕີເນັດ

- ອັບເດດລະບົບປະຕິບັດການ ແລະ ໂປຼແກຼມແອນຕີ້ໄວຣັສເປັນປະຈຳ
- ຄວນສະແກນອຸປະກອນເກັບຂໍ້ມູນທຸກຄັ້ງກ່ອນຈະນຳມາໃຊ້ວຽກ ເຊັ່ນວ່າ : ກາດຄວາມຈຳ ຫຼື Flash Drive, External Harddisk ແລະ ອື່ນໆ .
- ຕິດຕັ້ງ Firewall ເພື່ອປ້ອງກັນການໂຈມຕີຈາກ Hacker ແລະ ເປັນການປ້ອງກັນການຮັບ-ສົ່ງ ຂໍ້ມູນທີ່ເຮົາບໍ່ຕ້ອງການ ລວມທັງ ສະປາຍແວ ຫຼື program ອື່ນໆທີ່ອາດຈະເປັນການເປີດຊ່ອງໂຫວໃນການໂຈມຕີ
- ລະມັດລະວັງໃນການຫຼິ້ນອິນເຕີເນັດເພີ່ມຂຶ້ນ ໂດຍການເຂົ້າເວັບໄຊ໌ດ້ວຍ Https
- ສ້າງໂຕເອງໃຫ້ເປັນຄົນຮອບຄອບ ແລະ ຄິດຢູ່ສະເໝີວ່າ "ປອດໄພໄວ້ກ່ອນ"
- ຕິດຕາມຂ່າວສານ ຮູບແບບການໂຈມຕີໃຫມ່ໆຢູ່ສະເໝີ ເພື່ອທີ່ຈະໄດ້ລະມັດລະວັງ ແລະ ຫາທາງປ້ອງກັນໄພທີ່ອາດຈະເກີດຂຶ້ນໄດ້.

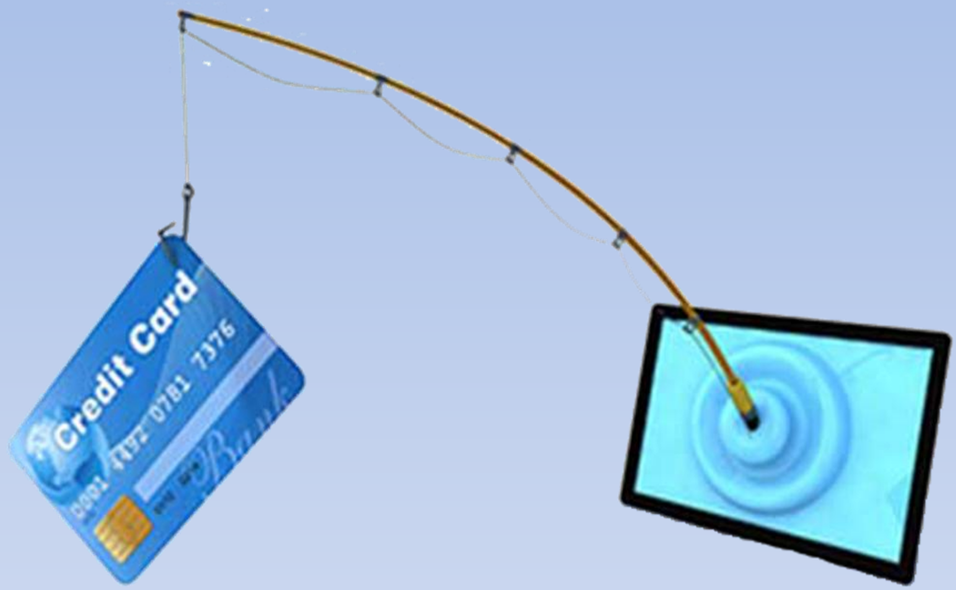
LaoCERT
Lao Computer Emergency Response Team

ການປ້ອງກັນລະຫັດຜ່ານ

1. ຄວນໃຊ້ລະຫັດຜ່ານທີ່ແຂງແກ່ນ ໂດຍການປະສົມຂອງບັນດາຕົວອັກສອນໃຫຍ່,ນ້ອຍ,ຕົວເລກ ແລະ ອັກສອນພິເສດ ເຊັ່ນ: L@oCeRT_20!3, XXXXXXXX
2. ຢ່າເປີດເຜີຍລະຫັດຜ່ານໃຫ້ຜູ້ອື່ນຮູ້.
3. ບໍ່ຄວນໃຊ້ລະຫັດຜ່ານທີ່ງ່າຍເກີນໄປເຊັ່ນ:9999, 1234, aaaa, abcd ຫຼື ເບີໂທລະສັບ,ວັນເດືອນປີເກີດ ແລະ ຄຳສັບຢູ່ໃນພົດຈະນານຸກົມ.
4. ບໍ່ຄວນກຳນົດຄວາມຍາວຂອງລະຫັດຜ່ານນ້ອຍກວ່າ 8 ຕົວອັກສອນ.
5. ຫ້າມເປີດເຜີຍລະຫັດຜ່ານທາງອີເມລ, ທາງໂທລະສັບ ຫຼື ຂຽນປະໄວ້ຊະຊາຍ.
6. ຄວນປ່ຽນລະຫັດຜ່ານເປັນປະຈຳ.
7. ຄວນເກັບຮັກສາລະຫັດຜ່ານໄວ້ໃຫ້ເປັນຄວາມລັບຢູ່ສະເໝີ.

LaoCERT
Lao Computer Emergency Response Team

ລະວັງຈະຕົກເປັນເຫຍື່ອຂອງການຫຼອກລວງ (ໜຶ່ງ-ລຶກ ສໍ້ໂກງ)



1. ຫ້າມ ຕອບອີເມລທີ່ຖາມເຖິງຂໍ້ມູນສ່ວນຕົວ ຫຼື ຂໍ້ມູນທາງການເງິນ.
2. ຫ້າມ Click link ທີ່ຢູ່ໃນອີເມລ.
3. ຄວນໃຊ້ໂປຼແກຼມປ້ອງກັນ Virus & Firewall ໃໝ່ຢູ່ສະເໝີ.
4. ຄວນລຶບຂໍ້ມູນທີ່ຄັດຕິດມານຳອີເມລອອກທັນທີ.

Phishing ແມ່ນການຫຼອກລໍ້ໃຫ້ເຫຍື່ອເປີດເຜີຍຂໍ້ມູນສ່ວນຕົວເຊັ່ນ : ລະຫັດບັດເຄຼດິດ, ຂໍ້ມູນບັນຊີທະນາຄານ, ອື່ນໆ. ດ້ວຍຮູບແບບຂອງ Email,Popup SMS ແລະ Web ຕ່າງໆ.

LaoCERT
Lao Computer Emergency Response Team

ການປ້ອງກັນສະແປມເມລ

1. ຫ້າມ ເປີດອ່ານອີເມລທີ່ບໍ່ຮູ້ແຫຼ່ງທີ່ມາ.
2. ຫ້າມ Click Link ທີ່ມານຳອີເມລ.
3. ຫ້າມ ຕອບກັບ ຫຼື ສົ່ງຕໍ່ສະແປມອີເມລ.
4. ຫ້າມ ເປີດອ່ານສະແປມອີເມລ.
5. ຫ້າມ ສົ່ງຕໍ່ອີເມລທີ່ບໍ່ຮູ້ທີ່ໄປທີ່ມາ.
6. ໃຫ້ ລຶບສະແປມອີເມລຖິ້ມທັນທີ.
7. ໃຫ້ ເປີດໃຊ້ Anti Spam Email.

ສາມາດດາວໂຫຼດໂປຼແກຼມນີ້ໄດ້ຈາກ:

http://software.thaiware.com/7893-AntiSPAM_Guard.html

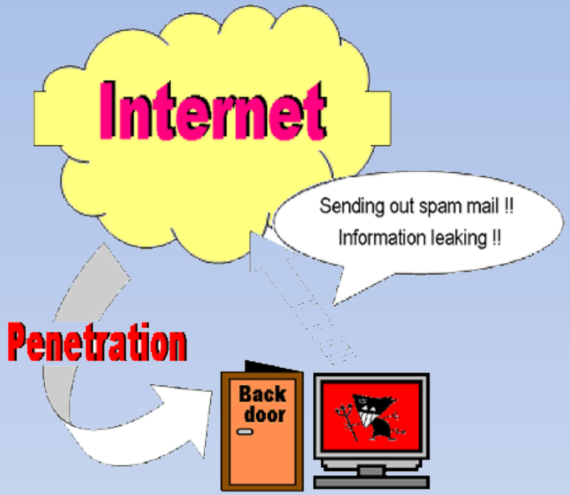
http://www.spamfighter.com/SPAMfighter/Lang_TH/Product_Info.asp

Spam Mail ແມ່ນອີເມລທີ່ເຮົາບໍ່ຕ້ອງການ ແລະ ສົ່ງມາຈາກຄົນທີ່ເຮົາບໍ່ຮູ້ຈັກກັນເຊັ່ນ : ຈົດໝາຍ, ຈົດໝາຍຫຼອກລວງຕ່າງໆ ທີ່ແອບແຝງຕິດມານຳ Spam ຄື: Virus, Spyware & Bots.

LaoCERT
Lao Computer Emergency Response Team

BackDoor ແລະ Botnets

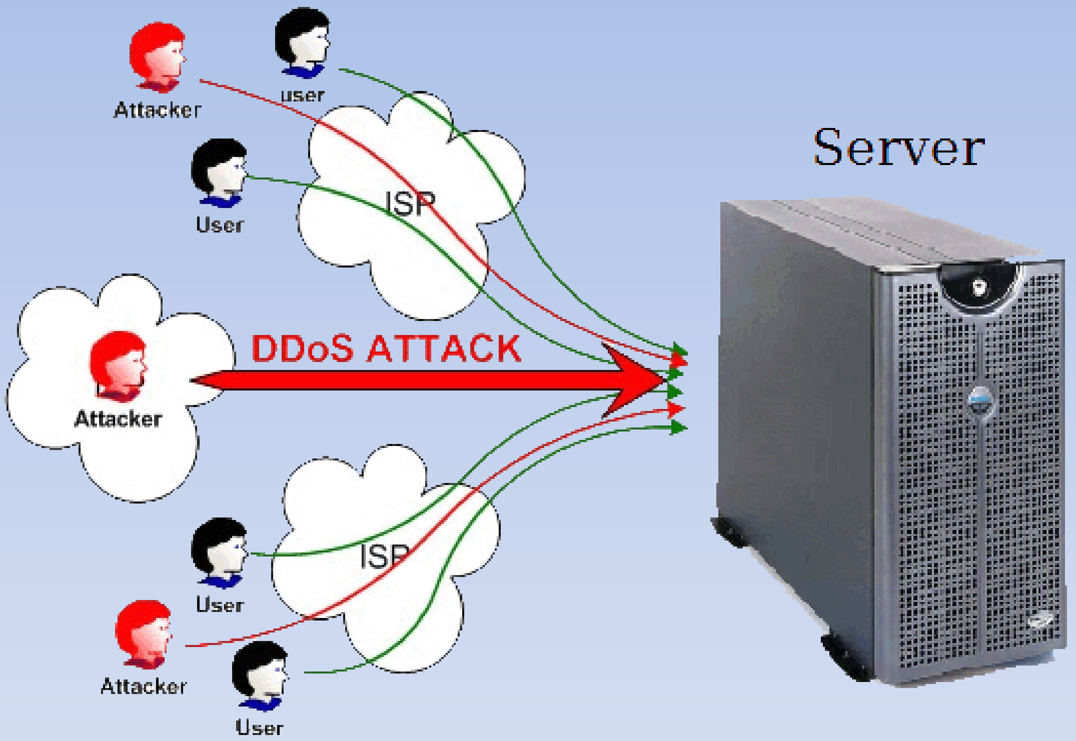
- Backdoor ເຮັດໜ້າທີ່ເປີດທາງໃຫ້ຜູ້ບໍ່ປະສົງດີ ສາມາດຣີໂໝດເຂົ້າໄປຫາເຄື່ອງຄອມພິວເຕີຂອງເຮົາ ໄດ້. ສ່ວນຫຼາຍຈະມາກັບການຕິດຕັ້ງ Application ຫຼື ໂປຼແກຼມທີ່ຜິດກົດໝາຍ.



- ຄອມພິວເຕີທີ່ຖືກບັນດາ Hacker ເຂົ້າຄວບຄຸມ ເຄື່ອງເປັນທີ່ຮຽບຮ້ອຍແລ້ວ ນັ້ນເອີ້ນວ່າ “Botnets” ເຊິ່ງກາຍເປັນເຄືອຂ່າຍຂອງ Hacker ເພື່ອໃຊ້ໃນ ການກະທຳຜິດ ເຊັ່ນ : ສົ່ງສະແປມເມລ ຫຼື ເປັນຖານ ໃນການໂຈມຕີເປົ້າໝາຍແບບ DDoS ເປັນຕົ້ນ

LaoCERT
Lao Computer Emergency Response Team

ການໂຈມຕີແບບ DDoS



- ເປັນການໂຈມຕີ ທີ່ເຈາະຈົງໄປຫາເຄື່ອງແມ່ຂ່າຍ ຫຼື ເຄື່ອງເຊີເວີ ເຊິ່ງຈະໂຈມຕີໂດຍເຄື່ອງຄອມພິວເຕີທີ່ຮຸກຮານ ຜ່ານຫຼາຍໆເຄື່ອຂ່າຍພ້ອມກັນ
- ເຮັດໃຫ້ເກີດຄວາມແອອັດໃນສາຍການສື່ສານ
- ໃນທີ່ສຸດເຄື່ອງແມ່ຂ່າຍກໍ່ຢຸດທຳງານ

LaoCERT
Lao Computer Emergency Response Team

ສື່ສັງຄົມອອນລາຍແມ່ນຫຍັງ?

- ແມ່ນຊ່ອງທາງໃນການຕິດຕໍ່ສື່ສານຜ່ານລະບົບອິນເຕີເນັດ ທີ່ບຸກຄົນທົ່ວໄປສາມາດນຳສະເໜີຂໍ້ມູນ, ຮູບພາບ, ວິດີໂອ, ຂໍ້ຄວາມ ຫຼື ເຫດການຕ່າງໆ ໄດ້ດ້ວຍຕົວເອງ ອອກສູ່ສາທາລະນະໂດຍໃຊ້ໂທລະສັບມືຖື ຫຼື ອຸປະກອນສື່ສານປະເພດຕ່າງໆ.
- ທຸກທີ່ທຸກເວລາສິ່ງຕໍ່ຂ່າວສານໄດ້ວ່ອງໄວ, ມີທັງດ້ານດີ ແລະ ດ້ານຫຍໍ້ທໍ້ ປຽບສະເໝືອນມີດສອງຄົມ ໃຊ້ດີກໍ່ເປັນປະໂຫຍດ ໃຊ້ບໍ່ຖືກກໍ່ທຳລາຍຕົນເອງ.
- ເປັນການປ່ຽນສະພາບຈາກຄົນອ່ານຂ່າວ, ຟັງຂ່າວ, ເບິ່ງຂ່າວ ເປັນນັກຂ່າວ, ນັກວິເຄາະ ແລະ ນັກວິຈານ ປະກົດການລັກສະນະນີ້ກຳລັງເປັນແນວໂນ້ມໃໝ່ຂອງສື່ສານມວນຊົນຍຸກອິນເຕີເນັດ.

LaoCERT
Lao Computer Emergency Response Team

10 ອັນດັບທີ່ມັກໃຊ້ຫຼາຍໂດຍທົ່ວໄປ

1. facebook.com
2. twitter.com
3. Google
4. linkedIn.com
5. Youtube.com
6. flickr.com
7. myspace.com
8. Wikipedia.org
9. bing.com
10. livejournal.com

ຂໍ້ດີ

- ສາມາດແລກປ່ຽນຂໍ້ມູນ, ຂ່າວສານຕ່າງໆ ໄດ້ຢ່າງວ່ອງໄວ.
- ເປັນຄັງຂໍ້ມູນຄວາມຮູ້ຂະໜາດນ້ອຍເພາະເຮົາສາມາດສະເໜີຄວາມຄິດເຫັນ ແລກປ່ຽນຄວາມຮູ້ ຫຼື ຕັ້ງຄຳຖາມໃນເລື່ອງຕ່າງໆ ເພື່ອໃຫ້ບຸກຄົນອື່ນທີ່ສົນໃຈໄດ້ຊ່ວຍກັນຕອບ.
- ປະຫຍັດຄ່າໃຊ້ຈ່າຍໃນການຕິດຕໍ່ສື່ສານກັບຄົນອື່ນ ສະດວກ ແລະ ວ່ອງໄວ.
- ເປັນສື່ໃນການນຳສະເໜີຜົນງານຂອງຕົວເອງເຊັ່ນ:ງານຂຽນ, ຮູບພາບ, ວີດີໂອ ຕ່າງໆ ເພື່ອໃຫ້ຜູ້ອື່ນໄດ້ເຂົ້າມາຮັບຊົມ ແລະ ສະແດງຄວາມຄິດເຫັນ.
- ໃຊ້ເປັນສື່ໃນການໂຄສະນາ ປະຊາສຳພັນ ສິນຄ້າ ຫຼື ບໍລິການລູກຄ້າສຳລັບບໍລິສັດ ແລະ ອົງກອນຕ່າງ ໆ ຊ່ວຍສ້າງຄວາມເຊື່ອມັ່ນໃຫ້ລູກຄ້າ.
- ຫາເພື່ອນທີ່ຮູ້ໃຈ, ສ້າງຄວາມສຳພັນທີ່ດີຈາກເພື່ອນສູ່ເພື່ອນ.

LaoCERT Lao Computer Emergency Response Team

ຂໍ້ເສຍ

- Social Network ເປັນສັງຄົມອອນໄລທີ່ກວ້າງ ຫາກຜູ້ໃຊ້ຮູ້ເທົ່າບໍ່ເຖິງການ ຫລື ຂາດວິຈາລະນະຍານ ອາດຈະຖືກຫຼອກລວງໄດ້(ດັ່ງນັ້ນ, ຕ້ອງປະຕິບັດຕາມຄຳແນະນຳຢ່າງເຄັ່ງຄັດ).
- ອາດມີຄົນນຳຮູບ ຫຼື ຂໍ້ມູນສ່ວນຕົວຕ່າງໆຂອງເຮົາໄປໃຊ້ໃນທາງທີ່ຜິດ.
- ໃນເຄືອຂ່າຍອິນເຕີເນັດ ເປັນແຫຼ່ງເຜີຍແຜ່ໄວຣັສ ໄດ້ເປັນຢ່າງດີ.
- ອາດມີຄົນລັກລອບເອົາບັນຊີຂອງເຮົາໄປແອບອ້າງ ກະທຳຜິດຕ່າງໆ ຈົນເກີດຜົນເສຍຫາຍໄດ້
- ຖ້າໃຊ້ຊີວິດຢູ່ກັບ Social network ຫຼາຍເກີນໄປອາດເຮັດໃຫ້:
  - ເສຍການຮຽນ.
  - ຜົນການປະຕິບັດວຽກງານ ບໍ່ໄດ້ດີ.
  - ເສຍເວລາ.
  - ເສຍສຸຂະພາບ.

ໃຊ້ເຄືອຂ່າຍສັງຄົມອອນລາຍແນວໃດຈຶ່ງຈະປອດໄພ

1. ບໍ່ຄວນ ເປີດເຜີຍຂໍ້ມູນສ່ວນຕົວຫຼາຍເກີນໄປ.
2. ບໍ່ຄວນ Post ຂໍ້ມູນສ່ວນຕົວຂອງຜູ້ອື່ນ, ຊຶ່ງອາດເຮັດໃຫ້ຜູ້ອື່ນໄດ້ຮັບຄວາມເສຍຫາຍ ແລະ ນຳຜົນສະທ້ອນຄືນສູ່ຕົນ.
3. ຄວນ ຈຳໄວ້ວ່າທຸກຢ່າງທີ່ Post ຂຶ້ນໄປແລ້ວນັ້ນຄວາມເປັນສ່ວນຕົວຈະໝົດໄປທັນທີ.
4. ຄວນ ລຶບທຸກຂໍ້ຄວາມທີ່ບໍ່ເໝາະສົມອອກ.
5. ຄວນ ລະມັດລະວັງໃຫ້ຫຼາຍກ່ຽວກັບຄຳຖາມຂໍ້ມູນສ່ວນຕົວໃນເວລາສົນທະນາກັບຄົນທີ່ຫາກໍ່ຮູ້ຈັກກັນ.
6. ຄວນ ເພີ່ມບຸກຄົນທີ່ຮູ້ຈັກກັນດີເທົ່ານັ້ນເຂົ້າມາເປັນເພື່ອນ.
7. ຄວນ ກວດສອບລະບຽບການຕ່າງໆໃນການນຳໃຊ້ເຄືອຂ່າຍສັງຄົມອອນລາຍ ເຊັ່ນ: Facebook, Youtube,...ກ່ອນນຳໃຊ້.

LaoCERT
Lao Computer Emergency Response Team

Chat ແນວໃດຈຶ່ງຈະປອດໄພ

- ຫ້າມໃຫ້ຜູ້ອື່ນຮູ້ກ່ຽວກັບຂໍ້ມູນທີ່ສຳຄັນຂອງຕົນເອງ.
- ຫ້າມ ເລືອກ Option “Remember Password” ໃນການພິມຊື່ ແລະ ລະຫັດຜ່ານເຂົ້າເຄື່ອງອິນເຕີເນັດສາທາລະນະ.
- ຄວນໃຊ້ຊື່ຫຼິ້ນ ແທນ ຊື່ແທ້.
- ຄວນ ລະມັດລະວັງໃນການນັດພົບກັບຄົນແປກໜ້າ ທີ່ຮູ້ຈັກກັນໃນການ Chat.
- ຄວນ ເປີດ Files ໃນການ Chat ສະເພາະຄົນທີ່ຮູ້ຈັກກັນດີເທົ່ານັ້ນ.

LaoCERT
Lao Computer Emergency Response Team

ພຶດຕິກຳການນຳໃຊ້ສະມາດໂຟນ

ນຳໃຊ້ໂທລະສັບມືຖືໃຫ້ປອດໄພ.

- ບໍ່ຄວນບອກເລກໂທລະສັບຂອງຕົນເອງສູ່ຜູ້ອື່ນ, ບໍ່ຄວນລົມໂທລະສັບ, ແຊັດ ກັບຄົນທີ່ບໍ່ຮູ້ຈັກກັນ.
- ຄວນຮູ້ຈັກການຕອບປະຕິເສດການຮັບໂທລະສັບຈາກບຸກຄົນທີ່ບໍ່ຮູ້ຈັກ.
- ເມື່ອເຮັດໂທລະສັບມືຖືເສຍ ຫຼື ຖືກລັກຄວນແຈ້ງໃຫ້ຕຳຫຼວດ ຫຼື ບໍລິສັດທີ່ໃຫ້ການບໍລິການໂທລະສັບມືຖືນັ້ນໂດຍດ່ວນ.
- ບໍ່ຄວນນຳເອົາໂທລະສັບມືຖືຂອງຕົນເອງຖ່າຍຮູບ ຫຼື ຖ່າຍວິດີໂອກ່ອນໄດ້ຮັບອະນຸຍາດຈາກບຸກຄົນທີ່ກ່ຽວຂ້ອງ.
- ບໍ່ຄວນປ່ອຍໃຫ້ບຸກຄົນອື່ນຖ່າຍຮູບ ຫຼື ຖ່າຍວິດີໂອຂອງຕົນເອງໂດຍທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດຈາກຕົນເອງກ່ອນ, ຮູບ ຫຼື ວິດີໂອທີ່ຖ່າຍນັ້ນອາດຖືກນຳໄປເຜີຍແຜ່ລົງທາງອິນເຕີເນັດ.
- ປັບປຸງລະບົບປະຕິບັດການ, ໂປຼແກຼມຕ່າງໆ ໃຫ້ຢູ່ໃນສະພາບໃໝ່ລ່າສຸດ.
- ເວລາດາວໂຫລດໂປຼແກຼມຕ່າງໆ ໃຫ້ກວດສອບໃຫ້ແນ່ໃຈວ່າເວບໄຊ,ໂປຼແກຼມນັ້ນສາມາດເຊື່ອຖືໄດ້.

LaoCERT
Lao Computer Emergency Response Team

ພະແນກ ສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ

ຕິດຕໍ່ ລາວເຊີດ ໄດ້ທີ່ : www.laocert.gov.la

LaoCERT
Lao Computer Emergency Response Team