ການປູກຈິດສຳນຶກຄວາມປອດໄພໄຊເບີ

Cyber Security Awareness

DO

DON'T

Cyber Security Awareness

“DO YOUR PART, BE CYBER SMART”

ຂໍ້ມູນອ້າງອີງຈາກ National Information Centre India

"ກະລຸນາຈື່ໄວ້ສະເໝີວ່າ ເມື່ອອິນເຕີເນັດໄດ້ຮັບຂໍ້ມູນສ່ວນຕົວທີ່ສຳຄັນ ຈະບໍ່ສາມາດຄວບຄຸມຂໍ້ມູນດັ່ງກ່າວໄດ້ ຂໍ້ມູນໃດກໍ່ຕາມທີ່ສາມາດໂພສລົງ ກໍ່ສາມາດຄົ້ນຫາ, ຄັດລອກ ແລະ ບັນທຶກໄວ້ໄດ້"

ກາມປຸກຈິດສຳນຶກຄວາມປອດໄພໄຊເບີ
ໂດຍ ກົມຄວາມປອດໄພໄຊເບີ
www.dcs.gov.la
admin@laocert.gov.la
ແປ, ຮຽບຮຽງ ແລະ ອອກແບບໂດຍ ພະແນກຄົ້ນຄວ້າ ແລະ ພັດທະນາ

ການປູກຈິດສຳນຶກຄວາມປອດໄພໄຊເບີ

ຄວາມປອດໄພທາງໄຊເບີແມ່ນຂະບວນການ ໃນການປ້ອງກັນ ແລະ ການກູ້ຄືນລະບົບຄອມພິວເຕີ, ເຄືອຂ່າຍ, ອຸປະກອນ ແລະ ໂປຣແກຣມ ຈາກທຸກປະເພດຂອງການໂຈມຕີທາງໄຊເບີ. ບັນດາມາດຕະການຄວາມປອດໄພໄຊເບີໄດ້ຮັບການອອກແບບ ເພື່ອຕໍ່ຕ້ານກັບໄພຄຸກຄາມໃນລະບົບເຄືອຂ່າຍ ແລະ ແອັບພີເຄຊັນ ບໍ່ວ່າໄພຄຸກຄາມຈະຢູ່ພາຍໃນ ຫຼື ພາຍນອກອົງກອນກໍ່ຕາມ.

ຄວາມປອດໄພໄຊເບີ ຈຶ່ງມີຄວາມສຳຄັນຢ່າງຍິ່ງ ໃນການປົກປ້ອງແຫຼ່ງຂໍ້ມູນ ແລະ ໂຄງລ່າງພື້ນຖານທີ່ສຳຄັນ. ການຖືກລັກຂໍ້ມູນໄປໃຊ້ໃນທາງທີ່ຜິດ ຊຶ່ງເປັນຂໍ້ມູນສຳຄັນ, ຂໍ້ມູນທາງການ, ຂໍ້ມູນລະບຸຕົວຕົນ, ຂໍ້ມູນສຸຂະພາບ ແລະ ຂໍ້ມູນການເງິນ ຈະເກີດຄວາມເສັຍຫາຍຢ່າງຫຼວງຫຼາຍ.

ຜູ້ໂຈມຕີຈະກຳນົດເປົ້າໝາຍ

- ຣາດແອ
- ຊອບແອ
- ຂໍ້ມູນ
- ອິນເຕີເນັດ/ເຄືອຂ່າຍ
- ການຢຸດສະງັກຂອງການບໍລິການ

ການສັ່ງລອມໄພຄຸກຄາມທີ່ໂຈມຕີມີ 6 ປະເພດຫລັກ ຄື:
ການປ່ຽນແປງໜ້າເວັບໄຊ, ໂປຣແກຣມປະສົງຮ້າຍ, ໄວຣັດຮຽກຄ່າໄຖ, ການຕົວະຍົວະຫຼອກລວງ, ຊ່ອງໂຫວ່ລະບົບ, ການໂຈມຕີໝາຍເລກໄອພີ.

1. ຄວນກວດ URL ກ່ອນກົດລິ້ງ ທີ່ຖືກສົ່ງມາກັບອີເມວ;
2. ຄວນລາຍງານກິດຈະກຳ ຫຼື ເຫດການ ທີ່ໜ້າສົງໄສທັນທີ;
3. ບັນຊີອີເມວທາງການ ຄວນໃຊ້ສະເພາະ ຈຸດປະສົງທາງການການເທົ່ານັ້ນ;
4. ບໍ່ສົ່ງຕໍ່ອີເມວທາງການໄປຫາອີເມວ ສ່ວນຕົວ.

1. ບໍ່ຄວນຕອບກັບອີເມວທີ່ບໍ່ຮູ້ຕົ້ນທາງ;
2. ບໍ່ຄວນກົດລິ້ງຈາກອີເມວທີ່ບໍ່ຮູ້ຈັກ ຫຼື ແຫຼ່ງທີ່ມາບໍ່ໜ້າເຊື່ອຖື;
3. ບໍ່ຄວນສົ່ງຂໍ້ມູນສ່ວນຕົວສຳຄັນ ເຊັ່ນ: ເລກບັດທະນາຄານ, ລະຫັດຜ່ານ ຫຼື ຂໍ້ມູນລະບຸຕົວຕົນຜ່ານທາງອີເມວ.

ອີເມວ

1. ຄວນປະຕິບັດຕາມມາດຕະຖານໃນການຕັ້ງລະຫັດຜ່ານຢ່າງເຂັ້ມແຂງ;
2. ຄວນໃຊ້ລະຫັດຜ່ານທີ່ຄາດເດົາໄດ້ຍາກ, ລະຫັດຜ່ານໃຊ້ຕັ້ງ 10 ໂຕຂຶ້ນໄປຄື: ອັກສອນໃຫຍ່, ອັກສອນນ້ອຍ, ຕົວເລກ ແລະ ສັນຍາລັກພິເສດ;
3. ຄວນປ່ຽນລະຫັດຜ່ານເປັນໄລຍະ;
4. ຄວນໃຊ້ລະຫັດຜ່ານແຕກຕ່າງທຸກບັນຊີ;
5. ບັນທຶກລະຫັດຜ່ານເປັນຄວາມລັບ;
6. ປ່ຽນລະຫັດຜ່ານທາກສົງໃສວ່າຖືກເປີດເຜີຍ;
7. ລະມັດລະວັງສະພາບແວດລ້ອມໃນຂະນະປ້ອນລະຫັດຜ່ານ.

1. ບໍ່ຄວນເປີດເຜີຍລະຫັດຜ່ານ;
2. ບໍ່ຄວນໃຊ້ລະຫັດຜ່ານທີ່ເຄີຍໃຊ້ກ່ອນໜ້ານີ້;
3. ບໍ່ຄວນໃຊ້ຊື່ສິ່ງຕ່າງໆທີ່ຢູ່ອ້ອມຂ້າງ;
4. ບໍ່ຄວນໃຊ້ຄຳສັບຈາກພົມຈະນານຸກົມ ເພາະຈະຄາດເດົາໄດ້ງ່າຍ.

ລະຫັດຜ່ານ

1. ຄວນລ໋ອກໜ້າຈໍເມື່ອຢຸດໃຊ້ງານ;
2. ຄວນເກັບຮັກສາໄວ້ບ່ອນປອດໄພ;
3. ຖ້າຫາກ Computer/ Laptop ຖືກລັກ ໃຫ້ແຈ້ງຄວາມເຈົ້າໜ້າທີ່ທັນທີ;
4. ຕິດຕັ້ງໂປຣແກຣມປ້ອງກັນໄວຣັດ ແລະ ອັບເດດເປັນປະຈຳ.

1. ບໍ່ຄວນຕິດຕັ້ງໂປຣແກຣມທີ່ບໍ່ໜ້າເຊື່ອຖື ຫຼື ທີ່ບ່ໄດ້ຮັບອະນຸຍາດ;
2. ບໍ່ຄວນເປີດເຄື່ອງປະໄວ້.

ຄອມພິວເຕີ

1. ຄວນລ໋ອກໜ້າຈໍເມື່ອຢຸດໃຊ້ງານ;
2. ຄວນເກັບຮັກສາໄວ້ບ່ອນປອດໄພ;
3. ຄວນປົກປ້ອງຂໍ້ມູນສຳຄັນ ແລະ ຫລີກລ່ຽງ ການຮ້ອງຂໍຂໍ້ມູນສຳຄັນຜ່ານມືຖື;
4. ມືຖືເສຍ ຫຼື ຖືກລັກ ແຈ້ງຫາເຈົ້າໜ້າທີ່;
5. ກວດສອບສິດທິການເຂົ້າເຖິງໃດແດ່ ເມື່ອ ຕິດຕັ້ງແອັບພິເຄຊັນ;
6. ກວດສອບປະຫວັດຂອງແອັບພິເຄຊັນ ກ່ອນການຕິດຕັ້ງ;
7. ລະມັດລະວັງການໃຊ້ບໍລິການລະບຸຕຳແໜ່ງ.

1. ບໍ່ຄວນຕອບກັບການຮ້ອງຂໍຂໍ້ມູນສຳຄັນ ທີ່ເປັນຄວາມລັບ;
2. ບໍ່ຄວນປະມືຖືຖິ້ມໄວ້;
3. ລະມັດລະວັງການຫລອກລວງເອົາຂໍ້ມູນ ໂດຍໂທປອມເປັນເຈົ້າໜ້າທີ່ທາງການ.

ໂທລະສັບມືຖື

1. ຄວນລ໋ອກ ແລະ ເກັບຮັກສາອຸປະກອນ ໄວ້ບ່ອນປອດໄພ;
2. ລຶບຂໍ້ມູນເມື່ອບໍ່ຈຳເປັນໃຊ້ງານແລ້ວ;
3. ຫ້າມນຳອຸປະກອນໃຊ້ງານທາງການ ຫຼື ເກັບຂໍ້ມູນທາງການ ແລະ ຫ້າມສົ່ງມອບ ອຸປະກອນໃຫ້ຜູ້ທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ;
4. ຫາກຈຳເປັນນຳໃຊ້ທາງການ ຫຼື ເກັບຂໍ້ມູນ ທາງການ ເກີດສູນຫາຍ ໃຫ້ລາຍງານທັນທີ.

1. ບໍ່ຄວນວາງອຸປະກອນໄວ້ບ່ອນລັກໄດ້ງ່າຍ;
2. ບໍ່ຄວນເຊື່ອມຕໍ່ອຸປະກອນ ໂດຍບໍ່ໄດ້ຮັບອະນຸ ຍາດອາດມີໄວຣັດ ຫຼື ຂໍ້ມູນອາດເສຍຫາຍ.

ອຸປະກອນສື່ແບບພົກພາ

1. ຄຳນຶງໄວ້ສະເໝີການເຊື່ອມຕໍ່ເຄືອຂ່າຍໄຮ້ສາຍ ແມ່ນບໍ່ມີຄວາມປອດໄພ;
2. ຫລີກລ່ຽງການເຊື່ອມຕໍ່ເຄືອຂ່າຍໄຮ້ສາຍ ສາທາລະນະ, ເມື່ອຈຳເປັນຕ້ອງເຊື່ອມຕໍ່ ຄວນນຳໃຊ້ VPN ເພື່ອປົກປ້ອງຂໍ້ມູນ ແລະ ອຸປະກອນໃຫ້ປອດໄພ;
3. ຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າອຸປະກອນ ກະຈາຍສັນຍານລະບົບເຄືອຂ່າຍໄຮ້ສາຍຖືກ ຕັ້ງຄ່າໄວ້ຄ່າເລີ່ມຕົ້ນ.

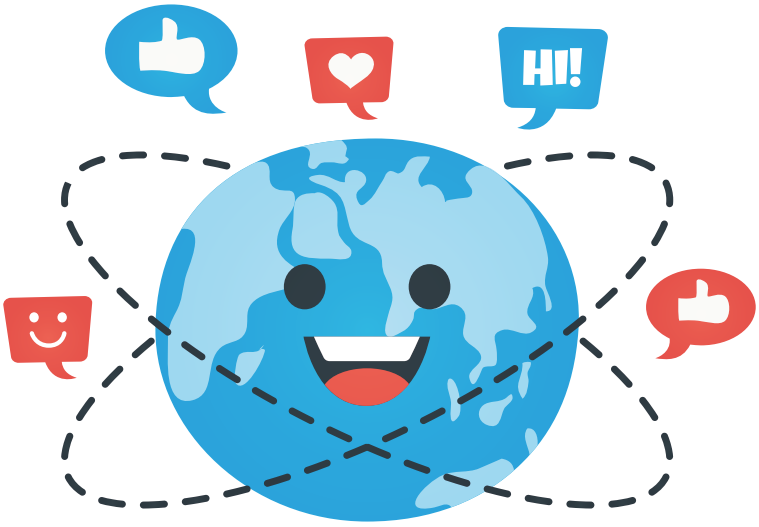
1. ບໍ່ຄວນເຊື່ອມຕໍ່ເຄືອຂ່າຍໄຮ້ສາຍ ຫຼື ບູທູດ ເມື່ອບໍ່ໃຊ້ງານແລ້ວ;
2. ບໍ່ຄວນເຂົ້າເວັບໄຊ ທີ່ມີການປ້ອນຂໍ້ມູນ ສ່ວນຕົວ ເມື່ອເຊື່ອມຕໍ່ເຄືອຂ່າຍໄຮ້ສາຍ ສາທາລະນະ.

ລະບົບເຄືອຂ່າຍໄຮ້ສາຍ

1. ຄວນໃຊ້ອິນເຕີເນັດບຣາວເຊີເວີຊັ່ນຫລ້າສຸດ;
2. ຄວນອອກຈາກລະບົບທຸກຄັ້ງ ຄື: ອີເມວ ເປັນຕົ້ນ ກ່ອນຈະອອກຈາກບຣາວເຊີ;
3. ຄວນປິດ web session ຫຼັງຈາກ ສຳເລັດບັນດາກິດຈະກຳຕ່າງໆ;
4. ຄວນອະນຸຍາດບັນທຶກ cookies ສະເພາະເວັບໄຊທີ່ໜ້າເຊື່ອຖືໄດ້.

1. ບໍ່ຄວນອະນຸຍາດບັນທຶກລະຫັດຜ່ານ ຫຼື ບັນທຶກແບບອັດຕະໂນມັດຂອງບຣາວເຊີ;
2. ບໍ່ຄວນດາວໂຫລດ ຫຼື ກະຈາຍໂປຣແກຣມ ປະສົງຮ້າຍ ຫຼື ເຄື່ອງມືທີ່ເປັນອັນຕະລາຍ;
3. ບໍ່ຄວນລະເມີດສິດທິ ຫຼື ໃບອະນຸຍາດ ໂດຍ ການດາວໂຫລດ ຫຼື ແຈກຍາຍເນື້ອຫາທີ່ໄດ້ ຮັບການຄຸ້ມຄອງ.

ການໃຊ້ງານອິນເຕີເນັດ



1. ຄວນກວດສອບລະບົບການບໍລິການ ໄດ້ກຳນົດຄ່າຈາກສ່ວນກາງໃນການຈັດການ ໂດຍຊອບແອ໊ປ້ອງກັນໄວຣັດ;
2. ຄວນກວດສອບຊອບແອ໊ປ້ອງກັນໄວຣັດ ແລະ ນາມສະກຸນຟາຍໄວຣັດມີການອັບເດດ;
3. ກໍລະນີທີ່ບໍ່ສາມາດລຶບໄວຣັດໄດ້ໃຫ້ລາຍງານຫາຜູ້ຮັບຜິດຊອບດ້ານຄວາມປອດໄພ.

ປອດໄພຈາກໄວຣັດ

1. ຄວນນຳໃຊ້ເວັບບຣາວເຊີເວີຊັ່ນຫລ້າສຸດ;
2. ຄວນລຶບປະຫວັດບຣາວເຊີຄື: cookies, temp file, history ແລະ activeX;
3. ຄວນປິດການສະໜັບສະໜຸນຂອງ JavaScript ຫຼື ActiveX ທັງໝົດ ກ່ອນການເຂົ້າເວັບໄຊທີ່ບໍ່ຮູ້ຈັກ.

1. ບໍ່ຄວນໃຫ້ຂໍ້ມູນສ່ວນຕົວໃນລິ້ງເວັບໄຊ ບໍ່ໜ້າເຊື່ອຖື;
2. ບໍ່ຄວນອະນຸຍາດໃຫ້ມີ pop-ups ແລະ plugins ໂດຍປິດການໃຊ້ງານທັງໝົດ ທີ່ຕັ້ງຄ່າບຣາວເຊີ.

ບຣາວເຊີ

ຄວນອັບເດດໃຫ້ເປັນເວີຊັ່ນຫລ້າສຸດຢ່າງເປັນປະຈຳ.

ແອັບພີເຄຊັນທີ່ຂຸມມາໃຊ້ງານເທິງເວັບບຣາວເຊີ

1. ຄວນເກັບຮັກສາຂໍ້ມູນສຳຄັນທີ່ພິມອອກ ໄວ້ບ່ອນປອດໄພ;
2. ຄວນລະມັດລະວັງສະພາບແວດລ້ອມ ເມື່ອພິມ ຫຼື ສົ່ງແຟັກຂໍ້ມູນສຳຄັນ;
3. ຄວນເອົາເອກະສານທີ່ພິມອອກ ຫຼື ໄດ້ຮັບ ແຟັກໃນທີ່ທັນ ປ້ອງກັນບໍ່ໃຫ້ບຸກຄົນອື່ນ ເຫັນເນື້ອໃນທີ່ສຳຄັນ.

1. ບໍ່ຄວນຖິ້ມເອກະສານທີ່ມີຂໍ້ມູນສຳຄັນ ທົ່ວໄປ ແຕ່ຄວນທຳລາຍຖິ້ມ;
2. ບໍ່ຄວນວາງເອກະສານຂໍ້ມູນໄວ້ທົ່ວໄປ.

ເຄື່ອງພິມ ຫຼື ແຟັກ

1. ຄວນຕັ້ງຄ່າຄວາມເປັນສ່ວນຕົວໃຫ້ກັບບັນຊີສື່ສັງຄົມອອນລາຍ ເພື່ອຈຳກັດການເຂົ້າເຖິງຂໍ້ມູນສ່ວນຕົວ;
2. ຄວນເພີ່ມໝູ່ເພື່ອນ ໃນສື່ສັງຄົມອອນລາຍສະເພາະຄົນທີ່ຮູ້ຈັກ;
3. ຄວນລະມັດລະວັງໃນການເພີ່ມໝູ່ເພື່ອນທີ່ແປກໜ້າໃນສື່ສັງຄົມອອນລາຍ;
4. ຄວນກວດສອບການຕັ້ງຄ່າຄວາມເປັນສ່ວນຕົວຂອງໂປຣຟາຍ ແລະ ກວດສອບວ່າຕັ້ງຄ່າໃນລະດັບທີ່ສູງ ຫຼື ການຢືນຢັນຕົວຕົນແບບສອງຊັ້ນ;
5. ເຖິງແມ່ນວ່າຈະຕັ້ງຄ່າຄວາມເປັນສ່ວນຕົວໃນສື່ສັງຄົມອອນລາຍ ແຕ່ກໍ່ ບໍ່ຮັບປະກັນຄວາມປອດໄພຂໍ້ມູນສ່ວນຕົວ ຄວນຄຳນຶງວ່າໃຜກໍ່ສາມາດເບິ່ງຂໍ້ມູນຫຼື ໂພສໄດ້.

1. ບໍ່ຄວນເກັບບັນຫາທີ່ປະເຊີນໄວ້ຄົນດຽວ;
2. ບໍ່ຄວນໂພສຂໍ້ມູນສ່ວນຕົວທີ່ສຳຄັນລົງສື່ສັງຄົມອອນລາຍ;
3. ບໍ່ຄວນແບ່ງປັ່ນຂໍ້ມູນສ່ວນຕົວເຊັ່ນ: ວັນເດືອນປີເກີດ, ຊື່ນາມສະກຸນແທ້, ຂໍ້ມູນກ່ຽວກັບບຸກຄົນອ້ອມຂ້າງ ຫຼື ສັດລ້ຽງ, ຂໍ້ມູນລະບຸຕຳແໜ່ງ ຫຼື ຕົວຕົນ, ຫລີກລ່ຽງການແບ່ງປັ່ນລົງສື່ສັງອອນລາຍ ເພາະອາດເຮັດໃຫ້ສະກົດຮອຍຕາມໄດ້.

ສື່ສັງຄົມອອນລາຍ

โดย ກົມຄວາມປອດໄພໄຊເບີ

LaoCERT
Lao Computer Emergency Response Team