# ເຄັດລັບໃນການຮັກສາຄວາມປອດໄພອຸປະກອນອິນເຕີເນັດຂອງສິ່ງຂອງທ່ານ

ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕຣາລີໄດ້ພັດທະນາຂໍ້ມູນນີ້ເພື່ອຊ່ວຍໃຫ້ຊຸມຊົນຊື້ ແລະ ໃຊ້ງານອຸປະກອນອິນເຕີເນັດຂອງສິ່ງຕ່າງໆ (IoT) ຢ່າງປອດໄພ. ອຸປະກອນ IoT ເປັນສິ່ງຂອງໃນຊີວິດປະຈຳວັນທີ່ມີການເຊື່ອມຕໍ່ອິນເຕີເນັດ. ຕົວຢ່າງຂອງອຸປະກອນ IoT ປະກອບມີເຄື່ອງຕິດຕາມເດັກ, ໂດຣນ, ກ້ອງວົງຈອນປິດ, ໂທລະທັດອັດສະລິຍະ ແລະ ອິນເວີເຕີພະລັງງານແສງຕາເວັນ. ອຸປະກອນ IoT ພາຍໃນບ້ານ ແລະ ທຸລະກິດໂດຍທົ່ວໄປແລ້ວຈະໃຊ້ Wi-Fi ຫຼື ເຄືອຂ່າຍມືຖື ເຊັ່ນ: 4G ຫຼື 5G ເພື່ອເຊື່ອມຕໍ່ອິນເຕີເນັດ.

ອຸປະກອນ IoT ຈຳນວນຫຼາຍທີ່ພົບເຫັນທົ່ວໄປໃນຄົວເຮືອນ ແລະ ທຸລະກິດໃນອົດສະຕາລີບໍ່ໄດ້ຖືກອອກແບບດ້ວຍຄວາມປອດໄພ. ອັນນີ້ເຮັດໃຫ້ອຸປະກອນມີຄວາມສ່ຽງຕໍ່ການປະນີປະນອມຜ່ານທາງອິນເຕີເນັດ. ເຫດການດັ່ງກ່າວອາດເຮັດໃຫ້ຜູ້ກໍ່ອາດຊະຍາກຳທາງໄຊເບີສາມາດເຂົ້າເຖິງອຸປະກອນ ແລະ ຂໍ້ມູນສ່ວນຕົວຂອງທ່ານເພື່ອຈຸດປະສົງທີ່ເປັນອັນຕະລາຍໄດ້.

# ກ່ອນທີ່ຈະຊື້ ອຸປະກອນ IoT

ການຄົ້ນຄ້ວາອຸປະກອນກ່ອນທີ່ຈະຕັດສິນໃຈຊື້ເປັນສິ່ງສຳຄັນ, ເນື່ອງຈາກຜູ້ຜະລິດກຳນົດລະດັບຄວາມປອດໄພທີ່ແຕກຕ່າງກັນ. ກ່ອນທີ່ຈະຊື້ອຸປະກອນ, ຄວນປຽບທຽບອຸປະກອນທີ່ຊື້ຄ້າຍຄືກັນທີ່ຂາຍໂດຍຜູ້ຜະລິດທີ່ແຕກຕ່າງກັນ. ສິ່ງທີ່ຄວນພິຈາລະນາໄດ້ແກ່:

1. **ອຸປະກອນນີ້ຜະລິດໂດຍບໍລິສັດທີ່ມີຊື່ສຽງ ແລະ ຈຳໜ່າຍໂດຍຮ້ານຄ້າທີ່ມີຊື່ສຽງ ຫຼື ບໍ?** ບໍລິສັດທີ່ມີຊື່ສຽງ ແລະ ເປັນທີ່ຮູ້ຈັກມັກຈະຜະລິດອຸປະກອນທີ່ຄຳນຶງເຖິງຄວາມປອດໄພ. ຮ້ານຄ້າທີ່ມີຊື່ສຽງ ແລະ ເປັນທີ່ຮູ້ຈັກມັກຈະຂາຍອຸປະກອນຈາກບໍລິສັດທີ່ມີຊື່ສຽງເທົ່ານັ້ນ ແລະ ມີລະບົບຕ່ອງໂສ້ສະໜອງທີ່ເຂັ້ມງວດກວ່າ ເພື່ອໃຫ້ແນ່ໃຈວ່າອຸປະກອນຈະມາຮອດທ່ານຕາມຈຸດປະສົງຂອງຜູ້ຜະລິດ.

2. **ມັນສາມາດປ່ຽນລະຫັດຜ່ານໄດ້ບໍ?** ການປ່ຽນລະຫັດຜ່ານເປັນສິ່ງທີ່ດີສະເໝີ. ຢ່າງໃດກໍຕາມ, ຖ້າອຸປະກອນຖືກຈັດສົ່ງໂດຍມີລະຫັດຜ່ານຄ່າເລີ່ມຕົ້ນທີ່ອ່ອນແອ, ສິ່ງນີ້ຈະກາຍເປັນສິ່ງທີ່ສຳຄັນກວ່າ. ອຸປະກອນທີ່ມີຄວາມປອດໄພທີ່ດີຄວນມີລະຫັດຜ່ານທີ່ບໍ່ຄືໃຜ, ບໍ່ສາມາດຄາດເດົາໄດ້, ສະລັບສັບຊ້ອນ ແລະ ບໍ່ສາມາດຄາດເດົາລະຫັດຜ່ານໄດ້, ເນື່ອງຈາກລະຫັດຜ່ານຄ່າເລີ່ມຕົ້ນທີ່ອ່ອນແອເປັນວິທີທີ່ງ່າຍທີ່ສຸດໃນການໂຈມຕີອຸປະກອນ.

3. **ຜູ້ຜະລິດຄວນມີການອັບເດດໃຫ້ຫຼືບໍ?** ສິ່ງສຳຄັນຕ່າງໆທີ່ບໍລິສັດຈະຕ້ອງສະເໜີໃຫ້ການອັບເດດ ເພື່ອແກ້ໄຂຈຸດອ່ອນຂອງອຸປະກອນທັນທີພວກເຂົາຖືກຄົ້ນພົບ. ຕົວຢ່າງ, ຖ້າຊອບແວຢູ່ໃນອຸປະກອນມີຊ່ອງໂຫວ່ທີ່ຮູ້ຈັກ ຫຼື ແຮກເກີພັດທະນາວິທີໃໝ່ໆໃນການບຸກລຸກອຸປະກອນຂອງທ່ານ, ຈຳເປັນຕ້ອງມີການອັບເດດເພື່ອການແກ້ໄຂບັນຫາ.

4. **ອຸປະກອນຈະເກັບກຳຂໍ້ມູນອັນໃດ ແລະ ຂໍ້ມູນນັ້ນຈະຖືກແບ່ງປັນກັບໃຜ?** ຂໍ້ມູນກ່ຽວກັບຂໍ້ມູນທີ່ຈະເກັບກຳ ແລະ ວິທີການທີ່ໃຊ້ງານຄວນສາມາດເຂົ້າເຖິງໄດ້ງ່າຍໃນເວັບໄຊທ໌ຂອງຜູ້ຜະລິດ ຫຼື ນະໂຍບາຍຄວາມເປັນສ່ວນຕົວຂອງເຂົາເຈົ້າ. ສິ່ງສຳຄັນແມ່ນຕ້ອງພິຈາລະນາຂໍ້ມູນຂ່າວສານທີ່ແອັບພລິເຄຊັນອອນລາຍ ຫຼື ມືຖືເກັບກຳຢູ່ສະເໝີ.

5. **ອຸປະກອນນີ້ເຮັດສະເພາະສິ່ງທີ່ທ່ານຕ້ອງການເທົ່ານັ້ນຫຼືບໍ?** ການຊື້ອຸປະກອນທີ່ໄດ້ເກີນກວ່າສິ່ງທີ່ທ່ານຕ້ອງການ, ລວມທັງການເຊື່ອມຕໍ່ອິນເຕີເນັດ, ອາດຈະເຮັດໃຫ້ຄວາມປອດໄພຂອງທ່ານຫຼຸດລົງ. ຄວາມສາມາດຂອງອຸປະກອນທີ່ທ່ານບໍ່ໄດ້ໃຊ້ສາມາດເພີ່ມຄວາມສ່ຽງຕໍ່ການໂຈມຕີຂອງອຸປະກອນໄດ້ໂດຍບໍ່ກໍ່ໃຫ້ເກີດຜົນປະໂຫຍດໃດໆແກ່ທ່ານ.

# ອຸປະກອນ IoT

ຈົ່ງຈື່ຈຳຄຳຖາມງ່າຍໆຈຳນວນໜຶ່ງໃນຂະນະທີ່ຕັ້ງຄ່າອຸປະກອນຂອງທ່ານ, ເພື່ອຊ່ວຍໃຫ້ທ່ານຮັກສາເຄືອຂ່າຍ ແລະ ຂໍ້ມູນຂອງທ່ານໃຫ້ປອດໄພຍິ່ງຂຶ້ນ.

1. **ອຸປະກອນຈຳເປັນຕ້ອງເຊື່ອມຕໍ່ກັບອິນເຕີເນັດບໍ?** ພຽງເພາະມັນສາມາດເຊື່ອມຕໍ່ໄດ້ ບໍ່ໄດ້ໝາຍຄວາມວ່າມັນຄວນເຊື່ອມຕໍ່ດ້ວຍ. ອຸປະກອນທີ່ບໍ່ໄດ້ເຊື່ອມຕໍ່ກັບອິນເຕີເນັດ ມີໂອກາດສ່ຽງຕໍ່ການຖືກບຸກລຸກໜ້ອຍລົງຫຼາຍ. ຖ້າທ່ານບໍ່ໄດ້ຈະນຳໃຊ້ຄຸນສົມບັດທີ່ຕ້ອງໃຊ້ການເຊື່ອມຕໍ່ອິນເຕີເນັດທ່ານຄວນພິຈາລະນາວ່າຈຳເປັນຕ້ອງເຊື່ອມຕໍ່ຫຼືບໍ່.

2. **ອຸປະກອນຢູ່ໃນສະຖານທີ່ທີ່ປອດໄພບໍ?** ຖ້າບໍ່ຈຳເປັນຕ້ອງຕິດຕັ້ງອຸປະກອນຢູ່ໃນພື້ນທີ່ທີ່ບໍ່ປອດໄພ, ການຕິດຕັ້ງຢູ່ໃນສະຖານທີ່ທີ່ປອດໄພຈະຫຼຸດຜ່ອນຄວາມສ່ຽງຕໍ່ການບຸກລຸກທາງດ້ານຮ່າງກາຍໄດ້.

3. **ຂ້າພະເຈົ້າຈະປ່ຽນຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານຄ່າເລີ່ມຕົ້ນບໍ?** ສິ່ງສຳຄັນແມ່ນທ່ານຕ້ອງໃຊ້ລະຫັດຜ່ານ ຫຼື ລະຫັດຜ່ານທີ່ເດົາຍາກ. ຖ້າອຸປະກອນຂອງທ່ານບໍ່ໄດ້ຖືກຈັດສົ່ງດ້ວຍລະຫັດຜ່ານທີ່ບໍ່ຊ້ຳກັນ, ບໍ່ສາມາດຄາດເດົາໄດ້, ສະລັບສັບຊ້ອນ ແລະ ບໍ່ສາມາດຄາດເດົາໄດ້ ຈຳເປັນຕ້ອງປ່ຽນລະຫັດຜ່ານນີ້. ຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານເລີ່ມຕົ້ນຈະຖືກເກັບກຳ ແລະ ໂພສທາງອອນລາຍ, ເຮັດໃຫ້ອຸປະກອນຂອງທ່ານມີຄວາມສ່ຽງຕໍ່ການໂຈມຕີ.

4. **ການຕັ້ງຄ່າເຄືອຂ່າຍ Wi-Fi ຂອງຂ້າພະເຈົ້າປອດໄພຫຼືບໍ່ ແລະມີລະຫັດຜ່ານທີ່ປອດໄພຫຼືບໍ?** ຮັກສາຄວາມປອດໄພກັບເຄືອຂ່າຍ Wi-Fi ແລະ ເຣົ້າເຕີຂອງທ່ານ ເພື່ອເຮັດໃຫ້ການໂຈມຕີເຂົ້າເຖິງອຸປະກອນ ແລະ ເຄືອຂ່າຍຂອງທ່ານໄດ້ຍາກ.

### ໄປໃຫ້ໄກກວ່ານັ້ນ

ຕັ້ງຄ່າເຄືອຂ່າຍ Wi-Fi ເພີ່ມເຕີມໃນເຣົ້າເຕີຂອງທ່ານສຳລັບອຸປະກອນ IoT ເທົ່ານັ້ນ. ເຣົ້າເຕີ Wi-Fi ຂອງທ່ານອາດຈະຊາບສິ່ງນີ້ວ່າເປັນເຄືອຂ່າຍ 'ແຂກ'. ຖ້າອຸປະກອນ IoT ຂອງທ່ານບໍ່ຈຳເປັນຕ້ອງມີການສື່ສານລະຫວ່າງກັນ ແລະ ກັນ, ໃຫ້ເປີດໃຊ້ຄຸນສົມບັດ 'ການແຍກລູກຄ້າ'. ການແຍກອຸປະກອນ IoT ຂອງທ່ານອອກຈາກຂໍ້ມູນທີ່ລະອຽດອ່ອນຂອງທ່ານຈະຊ່ວຍໃຫ້ໝັ້ນໃຈວ່າການບຸກລຸກອຸປະກອນ IoT ບໍ່ອະນຸຍາດໃຫ້ເຂົ້າເຖິງອຸປະກອນ ຫຼື ຂໍ້ມູນອື່ນຂອງທ່ານໄດ້.

5. **ຄຸນສົມບັດອຸປະກອນທີ່ບໍ່ຈຳເປັນຖືກປິດໄວ້ຫຼືບໍ?** ຖ້າອຸປະກອນຂອງທ່ານມີຄຸນສົມບັດທີ່ບໍ່ຕ້ອງການ ຫຼື ບໍ່ຈຳເປັນ (ເຊັ່ນ: ກ້ອງຖ່າຍຮູບ ຫຼື ໄມໂຄຣໂຟນ), ຄວນປິດການໃຊ້ງານຄຸນສົມບັດເຫຼົ່ານີ້ໃນບ່ອນທີ່ເປັນໄປໄດ້.

### ໄປໃຫ້ໄກກວ່ານັ້ນ

ຊອກຫາການຕັ້ງຄ່າທີ່ກ່າວເຖິງການເປີດໃຊ້ງານການເຂົ້າເຖິງໄລຍະໄກໄປຍັງອິນເຕີເຟດການດູແລລະບົບເວັບຂອງອຸປະກອນຈາກ LAN ຫຼື WAN/ອິນເຕີເນັດພາຍໃນເຄື່ອງ. ກວດສອບໃຫ້ແນ່ໃຈວ່າໄດ້ຕັ້ງຄ່າເປັນ LAN ໃນທ້ອງຖິ່ນ, ເວັ້ນເສຍແຕ່ທ່ານຈະຕ້ອງການການເຂົ້າເຖິງຈາກໄລຍະໄກດ້ວຍຕົວເອງ.

# ການບຳລຸງຮັກສາ ອຸປະກອນ IoT

ມີສິ່ງສຳຄັນບາງປະການທີ່ຕ້ອງຈື່ໄວ້ເມື່ອທ່ານຕັ້ງຄ່າ ແລະ ໃຊ້ງານອຸປະກອນ IoT ແລ້ວ. ສິ່ງເຫຼົ່ານີ້ລວມມີ:

1. **ປິດເປີດອຸປະກອນຄືນໃໝ່ຂອງທ່ານເປັນປະຈຳ.** ອາດຈະມີໄວຣັສຢູ່ຖ້າອຸປະກອນ IoT ເລີ່ມຊ້າລົງ ຫຼື ໃຊ້ງານບໍ່ໄດ້. ມັນແວສ່ວນໃຫຍ່ຈະຖືກເກັບໄວ້ໃນໜ່ວຍຄວາມຈຳ ແລະ ບໍ່ສາມາດລຶບອອກໄດ້ຢ່າງງ່າຍດາຍໂດຍການປິດເປີດອຸປະກອນຄືນ, ນັ້ນແມ່ນການປິດ ແລະ ເປີດອຸປະກອນ. ຖ້າອຸປະກອນຍັງຄົງເຮັດວຽກຊ້າ ຫຼື ໃຊ້ງານບໍ່ໄດ້ຫຼັງຈາກປິດເປີດເຄື່ອງໃໝ່, ໃຫ້ລອງຣີເຊັດເປັນຄ່າໂຮງງານ ແຕ່ການເຮັດສິ່ງນີ້ອາດລຶບຂໍ້ມູນຜູ້ໃຊ້ ແລະ ການຕັ້ງຄ່າສ່ວນບຸກຄົນທັງໝົດຂອງທ່ານ.

2. **ໃຊ້ການອັບເດດເປັນປະຈຳ.** ອຸປະກອນບາງຢ່າງຈະໃຊ້ການອັບເດດໂດຍອັດຕະໂນມັດ. ສຳລັບຜູ້ທີ່ບໍ່ໄດ້ເຮັດ, ໃຫ້ກວດສອບກັບຜູ້ຜະລິດເປັນປະຈຳ ແລະ ອັບເດດເມື່ອມີການອັບເດດ. ເມື່ອອຸປະກອນຂອງທ່ານບໍ່ສາມາດອັບເດດໄດ້ອີກຕໍ່ໄປ, ໃຫ້ພິຈາລະນາອັບເກຣດເປັນອຸປະກອນທີ່ໃໝ່ກວ່າທີ່ສາມາດອັບເດດໄດ້. ອຸປະກອນທີ່ບໍ່ມີການເຂົ້າເຖິງການອັບເດດຄວາມປອດໄພຈະບໍ່ໄດ້ຮັບການປົກປ້ອງຖ້າຄົ້ນພົບຊ່ອງໂຫວ່ໃໝ່ໆ ແລະ ອຸປະກອນເຫຼົ່ານີ້ອາດຈະກາຍເປັນຄວາມສ່ຽງຕໍ່ເຄືອຂ່າຍ, ຄວາມເປັນສ່ວນຕົວ ແລະ ຂໍ້ມູນຂອງທ່ານ.

3. **ປິດອຸປະກອນຂອງທ່ານເມື່ອບໍ່ໄດ້ໃຊ້ງານ.** ການປະໃຫ້ອຸປະກອນທີ່ບໍ່ໄດ້ໃຊ້ງານ ແລະ ບໍ່ໄດ້ຮັບການກວດສອບໃຫ້ເປີດຢູ່ ແລະ ເຊື່ອມຕໍ່ກັບເຄືອຂ່າຍ Wi-Fi ເປັນໄລຍະເວລາທີ່ຍາວນານ ອາດເພີ່ມໂອກາດທີ່ອຸປະກອນຂອງທ່ານຈະຖືກໂຈມຕີ. ຕົວເລືອກໜຶ່ງໃນການເຮັດໃຫ້ສຳເລັດໂດຍອັດຕະໂນມັດແມ່ນການໃຊ້ເຄື່ອງຈັບເວລາສຽບໄຟ ເພື່ອຈ່າຍໄຟໃຫ້ກັບອຸປະກອນສະເພາະໃນຊ່ວງເວລາທີ່ລະບຸເທົ່ານັ້ນ.

4. **ລະວັງການເພີ່ມຂຶ້ນຢ່າງຫຼວງຫຼາຍຂອງການໃຊ້ອິນເຕີເນັດ ຫຼື ໃບບິນລາຍເດືອນຂອງທ່ານ.** ການເພີ່ມຂຶ້ນຂອງການໃຊ້ອິນເຕີເນັດ ຫຼື ຄ່າໃບບິນທີ່ເພີ່ມຂຶ້ນຢ່າງຫຼວງຫຼາຍສາມາດຊີ້ບອກວ່າອຸປະກອນຂອງທ່ານຖືກບຸກລຸກ. ເວັ້ນແຕ່ວ່າຝ່າຍ IT ຂອງທຸລະກິດຂອງທ່ານຈະກວດສອບເລື່ອງນີ້, ຄວນຣີເຊັດເປັນຄ່າໂຮງງານ (ຢ່າງໃດກໍຕາມ, ໃຫ້ຮູ້ວ່າການເຮັດສິ່ງນີ້ອາດຈະລຶບຂໍ້ມູນຜູ້ໃຊ້ ແລະ ການຕັ້ງຄ່າສ່ວນບຸກຄົນທັງໝົດ), ຈາກນັ້ນຈຶ່ງປ່ຽນລະຫັດຜ່ານຂອງທ່ານ.

# ການກຳຈັດ ອຸປະກອນ IoT

ການກຳຈັດອຸປະກອນ (ໂດຍການຖິ້ມ ຫຼື ຂາຍ) ອາດຈະເຮັດໃຫ້ບຸກຄົນອື່ນເຂົ້າເຖິງຂໍ້ມູນສ່ວນຕົວ ຫຼື ຂໍ້ມູນຂອງທ່ານໄດ້ງ່າຍ. ວິທີການປ້ອງກັນປະກອບມີ:

1. **ລຶບຂໍ້ມູນ ແລະ ຂໍ້ມູນສ່ວນຕົວທັງໝົດ.** ຜູ້ຜະລິດຄວນກຳນົດວິທີການລຶບຂໍ້ມູນ ແລະ ຂໍ້ມູນສ່ວນບຸກຄົນຂອງທ່ານຈາກທັງອຸປະກອນ ແລະ ແອັບພລິເຄຊັ່ນທີ່ກ່ຽວຂ້ອງ. ການລຶບຂໍ້ມູນສ່ວນຕົວຂອງທ່ານຈະຊ່ວຍໃຫ້ແນ່ໃຈວ່າບໍ່ມີໃຜສາມາດເຂົ້າຂໍ້ມູນຂອງທ່ານໄດ້ຫຼັງຈາກທີ່ທ່ານໄດ້ກຳຈັດອຸປະກອນແລ້ວ. ລຶບບັນຊີອອນລາຍຂອງທ່ານ ຖ້າບໍ່ຈຳເປັນອີກຕໍ່ໄປ ຖ້າບໍ່ມີອຸປະກອນ IoT.

2. **ເຮັດການຣີເຊັດອຸປະກອນເປັນຄ່າເລີ່ມຕົ້ນຈາກໂຮງງານ.** ການຣີເຊັດເປັນຄ່າໂຮງງານແມ່ນອອກແບບມາເພື່ອລຶບຂໍ້ມູນທີ່ເກັບໄວ້ໃນພື້ນທີ່ທີ່ຈັດເກັບຂໍ້ມູນໃນເຄື່ອງ ແລະ ຣີເຊັດລະຫັດຜ່ານ, ຊື່ຜູ້ໃຊ້ ແລະ ການຕັ້ງຄ່າກັບຄືນສູ່ຄ່າເລີ່ມຕົ້ນ. ກວດສອບຄູ່ມືຜູ້ໃຊ້ຂອງອຸປະກອນ ຫຼື ເວັບໄຊທ໌ຂອງຜູ້ຜະລິດສຳລັບຂໍ້ມູນກ່ຽວກັບວິທີການຣີເຊັດຄ່າໂຮງງານ.

3. **ແຍກອຸປະກອນອອກຈາກໂທລະສັບມືຖື ແລະ ອຸປະກອນອື່ນໆ.** ການກຳຈັດອຸປະກອນທີ່ຍັງມີການເຂົ້າເຖິງອຸປະກອນອື່ນ, ເຄືອຂ່າຍ ຫຼື ບັນຊີອອນລາຍຂອງທ່ານອາດເຮັດໃຫ້ຜູ້ອື່ນເຂົ້າເຖິງໄດ້. ກວດສອບໃຫ້ແນ່ໃຈວ່າທ່ານກວດສອບອຸປະກອນອື່ນໆ ແລະ ລຶບການຈັບຄູ່ກັບອຸປະກອນທີ່ທ່ານກຳລັງກຳຈັດອອກ. ລຶບສິດໃດໆ ທີ່ໄດ້ຮັບຈາກແອັບພລິເຄຊັນມືຖືທີ່ບໍ່ຈຳເປັນອີກຕໍ່ໄປ.

4. **ຖອດສື່ທີ່ຖອດອອກໄດ້ທັງໝົດ (ເຊັ່ນ: ແຟລດໄດ USB, ກາດໜ່ວຍຄວາມຈຳ ແລະ ອື່ນໆ) ທີ່ຕິດຢູ່ກັບອຸປະກອນອື່ນໆ.** ສື່ທີ່ຖອດອອກໄດ້ອາດມີຂໍ້ມູນສ່ວນຕົວທີ່ບໍ່ໄດ້ຖືກລຶບອອກໃນການຣີເຊັດເປັນຄ່າໂຮງງານ ແລະ ຄວນຖອດອອກ, ທຳລາຍທາງຮ່າງກາຍ ແລະ ກຳຈັດແຍກຈາກອຸປະກອນ.

# ການຊ່ວຍເຫຼືອ

ຕິດຕໍ່ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕາລີໃນສັງກັດ Australian Signals Directorate ໂດຍສົ່ງອີເມວໄປທີ່ asd.assist@defence.gov.au ຫຼື ໂທຫາສາຍດ່ວນຕະຫຼອດ 24 ຊົ່ວໂມງ/7 ວັນ ເພື່ອຂໍຄວາມຊ່ວຍເຫຼືອດ່ວນທີ່ **1300 CYBER1 (1300 292 371)**.

ລາຍງານອາຊະຍາກຳທາງໄຊເບີໄປຍັງ ReportCyber ທີ່ www.cyber.gov.au/report

ຕິດຕໍ່ຫາ IDCARE ຜ່ານເວັບໄຊທ໌ www.idcare.org ຖ້າທ່ານປະສົບບັນຫາກັບການໂຈມລະກຳຂໍ້ມູນສ່ວນຕົວ.

ເຂົ້າເບິ່ງ www.cyber.gov.au ເພື່ອຮັບຄຳແນະນຳສຳລັບທ່ານ ແລະ ຄອບຄົວຂອງທ່ານ. ລົງທະບຽນເພື່ອຮັບບໍລິການແຈ້ງເຕືອນ ACSC ຟຣີກ່ຽວກັບໄພຂົ່ມຂູ່ອອນລາຍຫຼ້າສຸດ.

ມາເຮັດໃຫ້ອົດສະຕຣາລີເປັນສະຖານທີ່ທີ່ປອດໄພທີ່ສຸດໃນການເຊື່ອມຕໍ່ທາງອອນລາຍ.

ສຳລັບຄຳແນະນຳດ້ານຄວາມປອດໄພທາງໄຊເບີ, ກະລຸນາເຂົ້າໄປທີ່ www.cyber.gov.au

**ການປະຕິເສດຄວາມຮັບຜິດຊອບ**

ເນື້ອຫາໃນຄູ່ມືນີ້ແມ່ນມີລັກສະນະທົ່ວໄປ ແລະ ບໍ່ຄວນຖືເປັນຄຳແນະນຳທາງດ້ານກົດໝາຍ ຫຼື ໃຊ້ເປັນຂໍ້ມູນຊ່ວຍເຫຼືອໃນສະຖານະການສະເພາະໃດໜຶ່ງ ຫຼື ສະຖານະການສຸກເສີນ. ໃນເລື່ອງທີ່ສຳຄັນໃດໆ, ທ່ານຄວນຊອກຫາຄຳແນະນຳຈາກຜູ້ຊ່ຽວຊານອິດສະຫຼະທີ່ເໝາະສົມກັບສະຖານະການຂອງທ່ານເອງ.

ເຄື່ອງຈັກພາບຈະບໍ່ຮັບຜິດຊອບໃດໆ ຕໍ່ຄວາມເສຍຫາຍ, ການສູນເສຍ ຫຼື ຄ່າໃຊ້ຈ່າຍໃດໆທີ່ເກີດຂຶ້ນອັນເປັນຜົນມາຈາກເພິ່ງພາຂໍ້ມູນທີ່ມີຢູ່ໃນຄູ່ມືນີ້.

**ລິຂະສິດ**



**ການນຳໃຊ້ກາເຄື່ອງໝາຍ**

ເງື່ອນການໃຊ້ກາເຄື່ອງໝາຍນັ້ນມີລາຍລະອຽດຢູ່ໃນເວັບໄຊທ໌ຂອງກົມນາຍົກລັດຖະມົນຕີ ແລະ ຄະນະລັດຖະມົນຕີ ຂໍ້ມູນ ແລະ ແນວທາງກ່ຽວກັບກາເຄື່ອງໝາຍເຄື່ອງຈັກພາບ | pmc.gov.au.

**ຖ້າຕ້ອງການຂໍ້ມູນເພີ່ມເຕີມ ຫຼື ລາຍງານເຫດການຄວາມປອດໄພທາງໄຊເບີ, ໃຫ້ຕິດຕໍ່ພວກເຮົາ:**

**cyber.gov.au** | 1300 CYBER1 (1300 292 371)

ເບີໂທນີ້ສາມາດໃຊ້ໄດ້ພາຍໃນອອສເຕຣເລັຍເທົ່ານັ້ນ.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre