Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ທຸລະກິດຂະໜາດນ້ອຍ ຄູ່ມືຄວາມປອດໄພ ດ້ານໄຊເບີ

ຄວາມຊັບຊ້ອນຂອງເນື້ອຫາ
ງ່າຍດາຍ ● ○ ○

cyber.gov.au

ແນະນຳ

ສຳລັບທຸລະກິດຂະໜາດນ້ອຍ, ແມ່ນແຕ່ເຫດການເລັກໆນ້ອຍໆດ້ານຄວາມປອດໄພທາງໄຊເບີກໍ່ສາມາດມີຜົນກະທົບທີ່ຮ້າຍແຮງໄດ້.
ຄູ່ມືນີ້ກວມເອົາມາດຕະການຮັກສາຄວາມປອດໄພຂັ້ນພື້ນຖານເພື່ອຊ່ວຍປົກປ້ອງ
ທຸລະກິດຂອງທ່ານຈາກໄພຂົ່ມຂູ່ດ້ານຄວາມປອດໄພທາງໄຊເບີທົ່ວໄປ. ໃນເບື້ອງຕົ້ນ,
ພວກເຮົາຂໍແນະນຳສາມມາດຕະການດັ່ງຕໍ່ໄປນີ້:

- ເປີດໃຊ້ການຢັ້ງຢືນຕົວຕົນແບບຫຼາຍປັດໃຈ
- ອັບເດດຊອັບແວຂອງທ່ານ
- ສຳຮອງຂໍ້ມູນຂອງທ່ານ

ຄຳແນະນຳນີ້ອາດຈະລວມມີມາດຕະການທີ່ບໍ່ກ່ຽວຂ້ອງກັບທຸລະກິດຂອງທ່ານ ຫຼື ທຸລະກິດຂອງທ່ານ
ອາດຈະມີຄວາມຕ້ອງການທີ່ຊັບຊ້ອນຫຼາຍຂຶ້ນ. ຫຼັງຈາກທີ່ໄດ້ເຮັດຕາມຄຳແນະນຳນີ້ແລ້ວ,
ພວກເຮົາຂໍແນະນຳໃຫ້ທຸລະກິດຂະໜາດນ້ອຍນຳປະຕິບັດການເຕີບໂຕເຕັມທີ່
ລະດັບໜຶ່ງ ຂອງ (ຄວາມຈຳເປັນແປດຢ່າງ) Essential Eight.
ຖ້າທ່ານມີຄຳຖາມກ່ຽວກັບຄຳແນະນຳນີ້ຫຼືການຮັກສາຄວາມປອດໄພທາງໄຊເບີໃນວົງກວ້າງ,
ພວກເຮົາຂໍແນະນຳໃຫ້ທ່ານເວົ້າລົມກັບຜູ້ຊ່ຽວຊານດ້ານໄອທີຫຼືທີ່ປຶກສາທີ່ເຊື່ອຖືໄດ້.

ເຂົ້າຢ້ຽມເບິ່ງ cyber.gov.au ເພື່ອອ່ານຄູ່ມືສະບັບເຕັມຂອງພວກເຮົາ,
ລວມທັງຄຳແນະນຳວິທີການສຳລັບແຕ່ລະມາດຕະການ.

ສາລະບານ

ໄພຂົ່ມຂູ່ຕໍ່ທຸລະກິດ ຂະໜາດນ້ອຍ

ຂໍ້ຄວາມຫຼອກລວງ

ການຫຼອກລວງແມ່ນວິທີການທົ່ວໄປທີ່ອາດຊະຍາກອນທາງໄຊເບີມຸ່ງເປົ້າໄປທີ່ທຸລະກິດ ຂະໜາດນ້ອຍ. ເປົ້າໝາຍຂອງພວກເຂົາແມ່ນເພື່ອຫຼອກລວງທ່ານ ຫຼື ພະນັກງານຂອງທ່ານເຂົ້າໄປໃນ:

- ການສົ່ງເງິນ ຫຼື ບັດຂອງຂວັນ
- ການຄລິກໃສ່ລິງກ໌ເຊື່ອມຕໍ່ ຫຼື ໄຟລ໌ແນບທີ່ເປັນອັນຕະລາຍ
- ໃຫ້ຂໍ້ມູນທີ່ລະອຽດອ່ອນ, ເຊັ່ນ ລະຫັດຜ່ານ.

ອາດຊະຍາກອນທາງໄຊເບີອາດຈະພະຍາຍາມຫຼອກລວງທຸລະກິດຂອງທ່ານຜ່ານທາງອີເມວ, ຂໍ້ຄວາມ, ໂທລະສັບ ແລະ ສື່ສັງຄົມ. ພວກເຂົາຈະທຳທ່າວ່າເປັນບຸກຄົນ ຫຼື ອົງການທີ່ທ່ານໄວ້ໃຈ.

ການໂຈມຕີ ແບບຫຼອກລວງ ຟິຊຊິ່ງ (phishing)

ຄວາມກັງວົນສະເພາະສຳລັບທຸລະກິດຂະໜາດນ້ອຍແມ່ນ ການ**ໂຈມຕີແບບ phishing**. ການຫຼອກລວງເຫຼົ່ານີ້ມັກຈະມີລິງກ໌ເຊື່ອມຕໍ່ໄປຫາເວັບໄຊທ໌ປອມທີ່ທ່ານຖືກຊຸກຍູ້ໃຫ້ເຂົ້າສູ່ ລະບົບບັນຊີຫຼືໃສ່ລາຍລະອຽດທີ່ເປັນຄວາມລັບ.

ໂດຍທົ່ວໄປແລ້ວການໂຈມຕີແບບ phishing ຈະທຳລາຍລະຫັດຜ່ານບັນຊີຂອງທ່ານ. ອາດຊະຍາກອນທາງໄຊເບີມັກຈະໃຊ້ວິທີນີ້ເພື່ອ “ຄອບຄອງ” ບັນຊີສື່ສັງຄົມ ຂອງທຸລະກິດ ຂະໜາດນ້ອຍ ແລະ ເອີ້ນເອົາຄ່າໄຖ່.

ວິທີການຫຼຸດຜ່ອນ

ຖ້າຂໍ້ຄວາມແມ່ນມາຈາກບຸກຄົນທີ່ຮູ້ຈັກ ແລະ ເບິ່ງຄືວ່າໜ້າສົງໄສ, ໃຫ້ໃຊ້ຄວາມລະມັດລະວັງ. ຕິດຕໍ່ບຸກຄົນ ຫຼື ທຸລະກິດແຍກກັນເພື່ອກວດສອບເບິ່ງວ່າຂໍ້ຄວາມນັ້ນຖືກຕ້ອງຫຼືບໍ່.

ໃຊ້ລາຍລະອຽດການຕິດຕໍ່ທີ່ທ່ານພົບຜ່ານແຫຼ່ງທີ່ມາທີ່ຖືກຕ້ອງ, ຕົວຢ່າງເຊັ່ນໂດຍການເຂົ້າເບິ່ງເວັບໄຊທ໌ທາງການຂອງທຸລະກິດ, ແລະບໍ່ແມ່ນຂໍ້ມູນທີ່ມີຢູ່ໃນຂໍ້ຄວາມທີ່ໜ້າສົງໄສ.

ຮຽນຮູ້ເພີ່ມເຕີມກ່ຽວກັບການລະບຸການຫຼອກລວງ ແລະ ການໂຈມຕີ ແບບ ຟິຊຊິ່ງ ດ້ວຍແຫຼ່ງຂໍ້ມູນຕໍ່ໄປນີ້:

- ຮັບຮູ້ແລະລາຍງານການຫຼອກລວງ
- ຮຽນຮູ້ວິທີການສັງເກດການຫຼອກລວງ ແບບ ຟິຊຊິ່ງ
- ກວດຫາຂໍ້ຄວາມທີ່ຖືກອອກແບບທາງສັງຄົມ.

ກໍລະນີສຶກສາ:

ພະນັກງານຢູ່ບໍລິສັດສົ່ງເຄື່ອງໄດ້ຮັບອີເມ ຈາກເຈ້າໜ້າທີ ລະດັບບໍລິຫານຄົນໜຶ່ງວ່າ ໃຫ້ພວກເຂົາຊື້ບັດເຄຣດິດມາສເຕີກາ໌ດແບ ຈ່າຍລ່ວງໜ້າມູນຄ່າ 500 ໂດລາ x 6ບັດ. ຜູ້ບໍລິຫານໄດ້ບອກໃຫ້ນາງຮັກສາໄວ້ເປັນຄວາມລັບເພາະວ່າບັດນັ້ນຈະເປັນບັດຂອງຂວັນສຳລັບພະນັກງານ. ເມື່ອຊື້ແລ້ວ, ພະນັກງານໄດ້ຖືກຮ້ອງຂໍໃຫ້ຖ່າຍຮູບ ທັງສອງດ້ານ ຂອງບັດ ແລະສົ່ງໄປໃຫ້ຜູ້ບໍລິຫານເປັນຫຼັກຖານການຊື້.

ຕາມຄຳແນະນຳ, ພະນັກງານໄດ້ໄປຫາຫ້ອງການໄປສະນີ ແລະໃຊ້ ບັດເຄຣດິດສ່ວນຕົວຂອງນາງເພື່ອຊື້ບັດ ຂອງຂວັນ. ນາງໄດ້ຕອບອີເມວ ຂອງຜູ້ບໍລິຫານແລະ ສົ່ງຜ່ານຮູບພາບຂອງບັດຂອງຂວັນເປັນຫຼັກຖານ.

ຫຼັງຈາກກັບຄືນມາຈາກຫ້ອງການໄປສະນີ, ພະນັກງານໄດ້ມອບບັດແທ້ຈິງໃຫ້ຜູ້ບໍລິຫານ ຊຶ່ງບໍ່ຮູ້ເລື່ອງບັດເຫຼົ່ານັ້ນ. ຈາກການກວດສອບ, **ອີເມວທັງໝົດກ່ຽວກັບບັດຂອງຂວັນແມ່ນມາຈາກທີ່ຢູ່ອີເມວແບບສຸ່ມ ແລະບໍ່ໄດ້ມາຈາກບັນຊີອີເມວທີ່ຖືກຕ້ອງຂອງຜູ້ບໍລິຫານ. ມັນເປັນການຫຼອກລວງ**

ການໂຈມຕີທາງອີເມວ

ນອກເໜືອຈາກການຫຼອກລວງແບບ ຟິຊຊິ່ງ ແລ້ວ, ການໂຈມຕີທາງອີເມວທົ່ວໄປຕໍ່ທຸລະກິດຂະໜາດນ້ອຍແມ່ນ **ການຫຼອກລວງທາງອີເມວ ທຸລະກິດ (BEC)**. ອາດຊະຍາກອນສາມາດປອມຕົວເປັນຕົວແທນທາງທຸລະກິດໄດ້ໂດຍການໃຊ້ບັນຊີອີເມວທີ່ຖືກບຸກລຸກ ຫຼື ໂດຍຜ່ານວິທີອື່ນ - ເຊັ່ນການໃຊ້ຊື່ໂດເມນທີ່ຄ້າຍຄືກັບທຸລະກິດທີ່ແທ້ຈິງ. ນອກເໜືອຈາກການລັກຂໍ້ມູນແລ້ວ, ເປົ້າໝາຍຂອງການໂຈມຕີເຫຼົ່ານີ້ຕາມປົກກະຕິແລ້ວມັກເປັນການຫຼອກລວງຜູ້ເຄາະຮ້າຍ ໃຫ້ສົ່ງເງິນໄປຫາບັນຊີທະນາຄານທີ່ດຳເນີນການໂດຍຜູ້ຫຼອກລວງ.

ວິທີການຫຼຸດຜ່ອນ

ການປ້ອງກັນ ການໂຈມຕີທາງອີເມວທີ່ດີທີ່ສຸດແມ່ນ ການຝຶກອົບຮົມແລະເສີມສ້າງ ຄວາມຮັບຮູ້ສຳລັບ ພະນັກງານຂອງທ່ານ. ກວດສອບໃຫ້ແນ່ໃຈວ່າພະນັກງານ ຂອງທ່ານຮູ້ວ່າຈະຕ້ອງລະມັດລະວັງ ອີເມວດັ່ງຕໍ່ໄປນີ້:

- ການຮ້ອງຂໍການຈ່າຍເງິນ, ໂດຍສະເພາະ ຖ້າຮີບດ່ວນຫຼືເກີນກຳນົດ
- ການປ່ຽນແປງລາຍລະອຽດຂອງທະນາຄານ
- ທີ່ຢູ່ອີເມວທີ່ເບິ່ງຄືວ່າບໍ່ຖືກຕ້ອງ, ເຊັ່ນວ່າຊື່ໂດເມນບໍ່ກົງກັບຊື່ບໍລິສັດ ຂອງຜູ້ສະໜອງ.

ເຖິງແມ່ນວ່າການໂຈມຕີເຫຼົ່ານີ້ສາມາດສ້າງຄວາມເສຍຫາຍກະທົບນັ້ນແມ່ນງ່າຍແລະເກືອບບໍ່ມີຄ່າໃຊ້ຈ່າຍໃດໆເລີຍ. **ເມື່ອພະນັກງານໄດ້ຮັບອີເມວລັກສະນະນີ້, ການຫຼຸດຜ່ອນ ທີ່ມີປະສິດທິພາບທີ່ສຸດແມ່ນການໂທຫາຜູ້ສົ່ງເພື່ອຢືນຢັນວ່າພວກເຂົາແມ່ນມາຈາກແຫຼ່ງທີ່ຖືກຕ້ອງ.** ຢ່າໃຊ້ລາຍລະອຽດ ການຕິດຕໍ່ທີ່ເຂົາສົ່ງມາໃຫ້ທ່ານ ເພາະສິ່ງເຫຼົ່ານີ້ອາດເປັນການສໍ້ໂກງ. ແນະນຳຂະບວນການທີ່ເປັນທາງການສຳລັບພະນັກງານເພື່ອປະຕິບັດຕາມເມື່ອໄດ້ຮັບຄຳຮ້ອງຂໍໃຫ້ຈ່າຍເງິນ ຫຼື ລາຍລະອຽດ ຂອງທະນາຄານໄດ້ມີການປ່ຽນແປງ.

ຮຽນຮູ້ເພື່ອປົກປ້ອງທຸລະກິດຂອງທ່ານຈາກການຫຼອກລວງ ຂອງ BEC ແລະການປອມແປງທາງ ອີເມວດ້ວຍແຫຼ່ງຂໍ້ມູນດັ່ງຕໍ່ໄປນີ້:

- ການປອມແປງອີເມວທຸລະກິດ
- ປົກປ້ອງທຸລະກິດຂອງທ່ານຈາກການສໍ້ໂກງ ແລະການປອມແປງທາງອີເມວ
- ຈະເຮັດແນວໃດຖ້າທຸລະກິດຂອງທ່ານຖືກຕົກເປັນເປົ້າໝາຍຂອງອີເມວຫຼອກລວງຫຼື ປອມແປງ.

ກໍລະນີສຶກສາ:

ທຸລະກິດຮັບເໝົາກໍ່ສ້າງຂະໜາດນ້ອຍແຫ່ງໜຶ່ງໄດ້ຮັບອີເມວຈາກຜູ້ສະໜອງຂອງພວກ ເຂົາວ່າພວກເຂົາໄດ້ປ່ຽນທະນາຄານແລ້ວ. ຜູ້ສະໜອງໃຫ້ລາຍລະອຽດບັນຊີໃໝ່ສຳລັບການຈ່າຍເງິນຕາມໃບເກັບເງິນ. ເນື່ອງຈາກວ່າ ອີເມວເບິ່ງຄືວ່າຖືກຕ້ອງ, **ທຸລະກິດຮັບເໝົາກໍ່ສ້າງບໍ່ໄດ້ໂທຫາຜູ້ສະໜອງເພື່ອຢືນຢັນການປ່ຽນແປງໃນລາຍລະອຽດ ບັນຊີທະນາຄານ.**

ທຸລະກິດໄດ້ຈ່າຍເງິນຕາມໃບເກັບເງິນຈາກຜູ້ສະໜອງ ຫຼາຍກວ່າ 70,000 ໂດລາ. ໃນມື້ຕໍ່ມາ, ພະນັກງານ ອີກຄົນນຶ່ງໄດ້ຈ່າຍໃບເກັບເງິນແບບຜິດໆອີກຄັ້ງເປັນ ຈຳນວນເງິນເພີ່ມເຕີມຫຼາຍກວ່າ 70,000 ໂດລາ. ລວມ ແລ້ວມີການຈ່າຍທັງໝົດ ຫຼາຍກວ່າ 150,000ໂດລາ ທີ່ຖືກຈ່າຍໃຫ້ກັບ ບັນຊີທະນາຄານໃໝ່.

ເມື່ອທຸລະກິດໂທຫາຜູ້ສະໜອງຂອງພວກເຂົາເພື່ອ ຖາມວ່າພວກເຂົາສາມາດຄືນເງິນທີ່ຈ່າຍຊ້ຳກັນໄດ້ ຫຼື ບໍ່, ຜູ້ສະໜອງແຈ້ງວ່າລາຍລະອຽດຂອງທະນາຄານເຫຼົ່ານັ້ນ ບໍ່ຖືກຕ້ອງ. ການສືບສວນໄດ້ເລີ້ມຂຶ້ນໃນທັນທີ ແລະ ຜູ້ສະໜອງໄດ້ຄົ້ນພົບວ່າໜຶ່ງໃນບັນຊີອີເມວຂອງພວກເຂົາ ຖືກແຮັກແລະສົ່ງລາຍລະອຽດ ບັນຊີທະນາຄານທີ່ ຫຼອກລວງອອກໄປ. **ເງິນທີ່ເສຍໄປບໍ່ສາມາດກູ້ຄືນມາໄດ້.**

ຊອັບແວທີ່ເປັນອັນຕະລາຍ

ມາລແວ (Malware) ເປັນຄຳຫຍໍ້ຂອງຊອັບແວທີ່ເປັນອັນຕະລາຍທີ່ອອກແບບມາເພື່ອເຮັດໃຫ້ເກີດ ອັນຕະລາຍ ເຊັ່ນ ແຣນຊຳແວ (ransomeware), ໄວຣັສ, ສະປາຍແວ (spyware) ແລະ ໂທຣຈັນ (trojans). ມາລແວ ສາມາດ:

- ລັກ ຫຼື ລ໊ອກໄຟລ໌ຢູ່ໃນອຸປະກອນຂອງທ່ານ
- ລັກເລກທະນາຄານ ຫຼື ບັດເຄຣດິດຂອງທ່ານ
- ລັກຊື່ຜູ້ໃຊ້ແລະລະຫັດຜ່ານຂອງທ່ານ
- ຄວບຄຸມ ຫຼື ສອດແນມຄອມພິວເຕີຂອງທ່ານ.

ມາລແວ ສາມາດຢຸດບໍ່ໃຫ້ ອຸປະກອນຂອງທ່ານເຮັດວຽກ ຢ່າງຖືກຕ້ອງ, ລຶບ ຫຼື ເຮັດໃຫ້ໄຟລ໌ຂອງທ່ານ ເສຍຫາຍ ຫຼື ອະນຸຍາດໃຫ້ຜູ້ອື່ນເຂົ້າເຖິງຂໍ້ມູນສ່ວນຕົວ ຫຼື ຂໍ້ມູນທາງທຸລະກິດ ຂອງທ່ານໄດ້. ຖ້າອຸປະກອນຂອງທ່ານຕິດມາລແວ ທ່ານ ອາດຈະມີຄວາມສ່ຽງຕໍ່ການຖືກໂຈມຕີອື່ນໆ. ມາລແວ ສາມາດ ແຜ່ລາມໄປຍັງອຸປະກອນອື່ນໆໃນເຄືອຂ່າຍຂອງທ່ານໄດ້.

ອຸປະກອນຂອງທ່ານ ສາມາດຕິດໄວຣັສມາລ ແວ ໄດ້ໃນຫຼາຍວິທີ, ລວມທັງ:

- ຢ້ຽມຢາມເວັບໄຊທ໌ທີ່ຖືກຕິດໄວຣັສ ມາລແວ
- ດາວໂຫຼດໄຟລ໌ ຫຼື ຊອັບແວທີ່ຕິດໄວຣັສຈາກອິນເຕີເນັດ
- ເປີດໄຟລ໌ແນບອີເມວທີ່ຕິດໄວຣັສ.

ແຣນຊຳແວ

ແຣນຊຳແວ ເປັນ ມາລແວ ປະເພດທີ່ພົບເຫັນເລື້ອຍ ແລະ ເປັນອັນຕະລາຍ. ມັນເຮັດວຽກໂດຍການລ໊ອກ ຫຼື ເຂົ້າ ລະຫັດໄຟລ໌ຂອງທ່ານເພື່ອບໍ່ໃຫ້ທ່ານເຂົ້າເຖິງໄຟລ໌ເຫຼົ່ານັ້ນໄດ້ ອີກຕໍ່ໄປ. ຄ່າໄຖ່, ປົກກະຕິແລ້ວ ຈະເປັນໃນຮູບແບບຂອງ ສະ ກຸນເງິນດິຈິຕອລ, ແມ່ນຖືກເອີ້ນເອົາເພື່ອຟື້ນຟູການເຂົ້າເຖິງ ໄຟລ໌. ອາດຊະຍາກອນໄຊເບີອາດຈະຂົ່ມຂູ່ວ່າຈະເຜີຍແຜ່ ຫຼື ຂາຍຂໍ້ມູນທາງອອນລາຍ, ເວັ້ນເສຍແຕ່ຈະຈ່າຍເງິນຄ່າໄຖ່.

ວິທີການຫຼຸດຜ່ອນ

ເຖິງແມ່ນວ່າຊອັບແວຕ້ານໄວຣັສ ຫຼື ຊອັບແວຮັກສາ ຄວາມປອດໄພສາມາດຊ່ວຍປົກປ້ອງທ່ານຈາກ ມາລ ແວ ໄດ້ ແຕ່ບໍ່ມີຊອັບແວໃດມີປະສິດທິພາບ 100%. ພະນັກງານຕ້ອງລະມັດລະວັງກັບອີເມວ, ເວັບໄຊທ໌ ແລະ ການດາວໂຫຼດໄຟລ໌, ແລະ ອັບເດດອຸປະກອນຂອງ ພວກເຂົາ ເປັນປະຈຳເພື່ອຮັກສາ ຄວາມປອດໄພ.

ເບິ່ງແຫຼ່ງຂໍ້ມູນຕໍ່ໄປນີ້ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບການ ປົກປ້ອງ ທຸລະກິດຂອງທ່ານຈາກ ແຣນຊຳແວ:

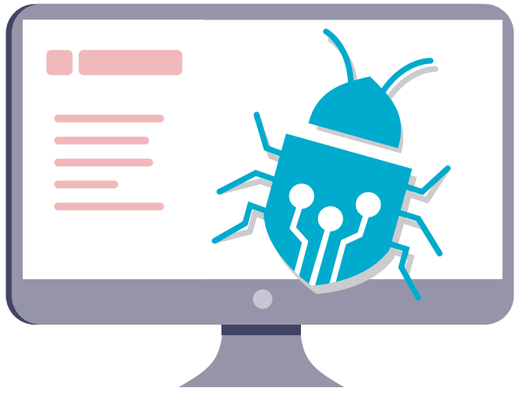
- ແຣນຊຳແວ
- ປົກປ້ອງຕົວທ່ານເອງຈາກການໂຈມຕີຂອງ ແຣນຊຳແວ
- ຈະເຮັດແນວໃດ ຖ້າທ່ານຖືກເອີ້ນເອົາຄ່າໄຖ່.

ກໍລະນີສຶກສາ:

ພະນັກງານຂອງຮ້ານອາໄຫລ່ລົດຍົນເຂົ້າມາເຮັດວຽກໃນ ຕອນເຊົ້າມື້ໜຶ່ງ ແລະບໍ່ສາມາດເປີດເຄື່ອງຄອມພິວເຕີ ເຊີຟເວີຂອງພວກເຂົາໄດ້. ໃນເວລາທີ່ຜູ້ໃຫ້ບໍລິການ ໄອ ທີ ຂອງພວກເຂົາ ເຂົ້າໄປໄດ້, ພວກເຂົາໄດ້ພົບວ່າໂປຣ ແກຣມວິນໂດເປີດຢູ່ຊຶ່ງລະບຸວ່າລະຫັດຂໍ້ມູນຄອມພິວເຕີ ທັງໝົດໄດ້ຖືກລັກເຂົ້າ. ຂໍ້ຄວາມນັ້ນຮຽກຮ້ອງໃຫ້ ພວກເຂົາຈ່າຍຄ່າໄຖ່ເປັນ bitcoin ເພື່ອປົດລ໊ອກໄຟລ໌.

ມີໄດຣຟ໌ສຳຮອງສຽບຢູ່ໃນຄອມພິວເຕີເຊິ່ງໄດ້ຖືກ ເຂົ້າລະຫັດໄວ້ເຊັ່ນກັນ. ພວກເຂົາພະຍາຍາມເຊື່ອມ ຕໍ່ ໄດຣຟ໌ສຳຮອງເພີ່ມເຕີມ, ແຕ່ໄຟລ໌ຖືກເຂົ້າລະຫັດ ໂດຍອັດຕະໂນມັດພາຍໃນບໍ່ເທົ່າໃດວິນາທີ. **ພວກເຂົາ ບໍ່ສາມາດທີ່ຈະລຶບແຣນຊຳແວຮ໋ອກກ່ອນທີ່ຈະ ພະຍາຍາມກູ້ຄືນຂໍ້ມູນແລະເຮັດໃຫ້ໄຟລ໌ສຳຮອງ ຂໍ້ມູນ ທັງໝົດທີ່ພວກເຂົາມີໄວ້ນັ້ນສູນເສຍໄປ.**

ທາງເລືອກດຽວທີ່ເຫຼືອແມ່ນການຕັ້ງຄ່າເຊີຟເວີ ຄືນໃໝ່ເປັນຄ່າເລີ້ມຕົ້ນ ແລະ ເລີ່ມຕົ້ນໃໝ່ດ້ວຍ ລະບົບໃໝ່. ທຸລະກິດຂອງພວກເຂົາສູນເສຍຂໍ້ມູນ ທີ່ສະສົມມາຫຼາຍປີແລະຕ້ອງເລີ່ມຕົ້ນໃຫມ່.



ຮັກສາບັນຊີຂອງທ່ານໃຫ້ປອດໄພ

ເປີດໃຊ້ການຢັ້ງຢືນຕົວຕົນ ດ້ວຍຫຼາຍປັດໄຈ

ການຢັ້ງຢືນຕົວຕົນດ້ວຍຫຼາຍປັດໄຈ (MFA) ເຮັດອາຊະ ຍາກອນໄຊເບີເຂົ້າເຖິງບັນຊີຂອງທ່ານ ໄດ້ຍາກຂຶ້ນ.

MFA ເພີ່ມຄວາມປອດໄພອີກຊັ້ນໜຶ່ງໃຫ້ກັບບັນຊີຂອງທ່ານ. ມັນເປັນວິທີໜຶ່ງທີ່ມີປະສິດທິພາບທີ່ສຸດໃນການປົກປ້ອງບັນຊີ ຂອງທ່ານບໍ່ໃຫ້ຄົນ ເຂົ້າເຖິງໄດ້, ດັ່ງນັ້ນທ່ານຄວນໃຊ້ມັນໃນທຸກ ຄັ້ງທີ່ເປັນໄປໄດ້. ໃຜກໍຕາມທີ່ລົງຊື່ເຂົ້າສູ່ລະບົບບັນຊີຂອງທ່ານ ຈະຕ້ອງລະບຸສິ່ງອື່ນນອກຈາກຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານ ຂອງ ທ່ານ. ນີ້ອາດຈະເປັນລະຫັດສະເພາະຈາກຂໍ້ຄວາມ ຫຼື ແອັບ ຢືນຢັນຕົວຕົນ ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ, ຈົ່ງອ່ານຄຳແນະນຳຂອງ ພວກເຮົາກ່ຽວກັບ MFA, ທີ່ມີຢູ່ໃນ **cyber.gov.au/mfa.**

✓ **ເປີດ MFA ໃນທຸກທີ່ທີ່ເປັນໄປໄດ້, ເລີ່ມຕົ້ນ ດ້ວຍບັນຊີທີ່ສຳຄັນ ທີ່ສຸດຂອງທ່ານ.**

ນຳໃຊ້ປະຕິບັດການຄວບຄຸມການເຂົ້າເຖິງ

ການຈຳກັດການເຂົ້າເຖິງຂອງຜູ້ໃຊ້ສາມາດຈຳກັດຄວາມເສຍຫາຍ ທີ່ເກີດຈາກເຫດການ ຄວາມປອດໄພທາງໄຊເບີໄດ້.

ການຄວບຄຸມການເຂົ້າເຖິງແມ່ນວິທີການຈຳກັດການເຂົ້າເຖິງໄຟລ໌ ແລະລະບົບບາງຢ່າງ. ໂດຍປົກກະຕິແລ້ວ ພະນັກງານບໍ່ຈຳເປັນ ຕ້ອງເຂົ້າເຖິງຂໍ້ມູນ, ບັນຊີ ແລະ ລະບົບທັງໝົດໃນທຸລະກິດ. ພວກເຂົາຄວນຈະໄດ້ຮັບອະນຸຍາດໃຫ້ເຂົ້າເຖິງສະເພາະສິ່ງທີ່ ພວກເຂົາຕ້ອງການເພື່ອປະຕິ ບັດໜ້າທີ່ ຂອງເຂົາເຈົ້າເທົ່ານັ້ນ.

ການຈຳກັດການເຂົ້າເຖິງຈະຊ່ວຍຈຳກັດຄວາມເສຍຫາຍທີ່ເກີດຈາກ ເຫດການຄວາມ ປອດໄພ ທາງໄຊເບີ. ຕົວຢ່າງ, ຖ້າຄອມພິວເຕີ ຂອງພະນັກງານຕິດໄວຣັສ ແຣນຊຳແວຮ໋, ດ້ວຍການຄວບຄຸມ ການເຂົ້າເຖິງທີ່ເໝາະສົມ ມັນອາດຈະສົ່ງຜົນກະທົບຕໍ່ໄຟລ໌ພຽງ ຈຳນວນນ້ອຍເທົ່ານັ້ນແທນທີ່ ຈະເປັນທຸລະກິດທັງໝົດ.

✓ **ໃຫ້ແນ່ໃຈວ່າຜູ້ໃຊ້ແຕ່ລະຄົນສາມາດ ເຂົ້າເຖິງສະເພາະແຕ່ສິ່ງທີ່ພວກເຂົາຕ້ອງ ການສຳລັບ ໜ້າທີ່ຂອງພວກເຂົາ.**

ໃຊ້ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ ຫຼື ຂໍ້ຄວາມລະຫັດຜ່ານ

ປົກປ້ອງບັນຊີຂອງທ່ານຈາກອາດຊະຍາກອນໄຊເບີດ້ວຍ ລະຫັດຜ່ານ ຫຼື ຂໍ້ຄວາມລະຫັດຜ່ານທີ່ປອດໄພ.

ທຸລະກິດຂະຫນາດນ້ອຍຈຳນວນຫຼາຍປະເຊີນກັບການໂຈມຕີ ທາງອິນເຕີເນັດເນື່ອງຈາກພຶດຕິກຳ ລະຫັດຜ່ານທີ່ບໍ່ດີ. ຕົວຢ່າງ, ການໃຊ້ລະຫັດຜ່ານດຽວກັນຊ້ຳໃນຫຼາຍບັນຊີ. ທ່ານສາມາດໃຊ້ **ຕົວຈັດການລະຫັດຜ່ານ** ແລະຂໍ້ຄວາມລະຫັດຜ່ານເພື່ອສ້າງ ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ. ຕົວຈັດການລະຫັດຜ່ານເຮັດໜ້າທີ່ ຄືກັບຕູ້ເຊຟສຳລັບລະຫັດຜ່ານຂອງທ່ານ. ທ່ານສາມາດ ນຳ ໃຊ້ມັນເພື່ອສ້າງແລະເກັບຮັກສາລະຫັດຜ່ານທີ່ເຂັ້ມແຂງແລະ **ເປັນເອກະລັກ**ສຳລັບແຕ່ ລະບັນຊີ ຂອງທ່ານ. ຖ້າທ່ານມີຫຼາຍ ບັນຊີ ສິ່ງນີ້ຈະຊ່ວຍເອົາພາລະຂອງການຈື່ຈຳລະຫັດຜ່ານທີ່ ເປັນເອກະລັກ. ທ່ານບໍ່ຈຳເປັນຕ້ອງຈື່ລະຫັດຜ່ານຫຼືບັນຊີທີ່ ເປັນຂອງລະຫັດຜ່ານນັ້ນ ເພາະວ່າລະຫັດຜ່ານທັງໝົດ ໄດ້ ຖືກບັນທຶກໄວ້ໃນຕົວຈັດການລະຫັດຜ່ານຂອງທ່ານ.

ສຳລັບບັນຊີທີ່ທ່ານລົງຊື່ເຂົ້າສູ່ລະບົບເປັນປະຈຳ ຫຼືບັນຊີທີ່ ທ່ານບໍ່ຕ້ອງການທີ່ຈະເກັບຮັກສາໄວ້ໃນ ຕົວຈັດການລະຫັດ ຜ່ານ, ໃຫ້ພິຈາລະນາໃຊ້ຂໍ້ຄວາມລະຫັດຜ່ານເປັນລະຫັດຜ່ານ ຂອງທ່ານ. ຂໍ້ຄວາມລະຫັດຜ່ານແມ່ນການປະສົມປະສານຂອງ ຄຳສັບແບບສຸ່ມ, ຕົວຢ່າງ ‘ຄຣິສຕັນ ໂອນຽນ ເຄລ ເປຣສໂຊ (‘crystal onion clay pretzel’). ພວກມັນມີປະໂຫຍດໃນ ເວລາທີ່ທ່ານຕ້ອງການລະຫັດຜ່ານທີ່ປອດໄພແລະຈື່ງ່າຍ. ການ ໃຊ້ຄຳປະສົມ ແບບສຸ່ມຂອງສີ່ຄຳ ຫຼື ຫຼາຍກວ່ານັ້ນແລະເຮັດໃຫ້ ມັນເປັນເອກະລັກ - **ຢ່າໃຊ້ຂໍ້ຄວາມລະຫັດຜ່ານຊ້ຳກັນ** ກັບຫຼາຍ ບັນຊີ. ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ, ອ່ານຄຳແນະນຳຂອງພວກເຮົາ ກ່ຽວກັບຂໍ້ຄວາມລະຫັດຜ່ານ ແລະ ຕົວຈັດການລະຫັດຜ່ານ ຂອງພວກເຮົາ, ມີຢູ່ທີ່: **cyber.gov.au/passphrases.**

✓ **ໃຊ້ຕົວຈັດການລະຫັດຜ່ານເພື່ອສ້າງ ແລະ ເກັບຮັກສາລະຫັດຜ່ານເປັນເອກະລັກສຳ ລັບ ແຕ່ລະບັນຊີທີ່ສຳຄັນຂອງທ່ານ.**

ຄຸ້ມຄອງບັນຊີທີ່ໃຊ້ຮ່ວມກັນ

ການແບ່ງປັນບັນຊີສາມາດເຮັດໃຫ້ຄວາມປອດໄພ ຫຼຸ ດລົງ ແລະ ເຮັດໃຫ້ຍາກທີ່ຈະ ຕິດຕາມກິດຈະກຳທີ່ເປັນອັນຕະລາຍ.

ໃນທຸລະກິດຂະໜາດນ້ອຍ, ອາດຈະມີເຫດຜົນທີ່ຖືກຕ້ອງວ່າເປັນ ຫຍັງພະນັກງານຈຳເປັນຕ້ອງໃຊ້ ບັນຊີຮ່ວມກັນ, ແຕ່ກໍຄວນຈະ ຫຼີກລ່ຽງໃຫ້ຫຼາຍເທົ່າທີ່ເປັນໄປໄດ້. ເມື່ອພະນັກງານຫຼາຍຄົນໃຊ້ ບັນຊີດຽວກັນ ອາດຈະເປັນການຍາກທີ່ຈະຕິດຕາມກິດຈະກຳກັບ ຄືນໄປຫາພະນັກງານຄົນໃດຄົນນຶ່ງ ສະເພາະ ແລະ ຍັງຍາກທີ່ຈະ ຕິດຕາມອາຊະຍາກອນທາງໄຊເບີທີ່ລັກເຂົ້າມາ. ເວັ້ນເສຍແຕ່ວ່າ ທ່ານປ່ຽນລະຫັດຜ່ານ, ພະນັກງານຍັງສາມາດສືບຕໍ່ເຂົ້າເຖິງບັນຊີ ໄດ້ເຖິງແມ່ນວ່າພວກເຂົາອອກ ຈາກທຸລະກິດແລ້ວກໍຕາມ.

✓ **ຈຳກັດການໃຊ້ບັນຊີທີ່ໃຊ້ຮ່ວມກັນ ແລະ ຮັບປະກັນ ອັນໃດນຶ່ງທີ່ ໃຊ້ໃນທຸລະກິດຂອງທ່ານ.**

ປົກປ້ອງອຸປະກອນ ແລະ ຂໍ້ມູນ ຂອງທ່ານ

ອັບເດດຊອັບແວຂອງທ່ານ

ການຮັກສາຊອັບແວຂອງທ່ານໃຫ້ທັນສະໄໝເປັນ ໜຶ່ງໃນວິທີທີ່ດີທີ່ສຸດໃນການປົກປ້ອງ ທຸລະກິດ ຂອງທ່ານຈາກການໂຈມຕີທາງໄຊເບີ.

ການອັບເດດສາມາດແກ້ໄຂຂໍ້ບົກພ່ອງດ້ານຄວາມປອດໄພໃນ ລະບົບປະຕິບັດການ ແລະ ຊອັບແວອື່ນໆ ຂອ ທ່ານ, ດັ່ງນັ້ນ ມັນເປັນເລື່ອງຍາກສຳລັບອາຊະຍາກອນໄຊເບີທີ່ຈະລັກເຂົ້າ ໄດ້. ຂໍ້ບົກພ່ອງໃໝ່ໆ ຖືກຄົ້ນພົບຕະຫຼອດເວລາ, ດັ່ງນັ້ນ ຢ່າຖືເບົາກັບການແຈ້ງເຕືອນໃຫ້ອັບເດດ. ການອັບເດດຊອັບ ແວ ຂອງທ່ານເປັນປົກກະຕິຈະຫຼຸດຜ່ອນໂອກາດຂອງອາຊະຍາ ກອນໄຊເບີຈະໃຊ້ຈຸດອ່ອນທີ່ຮູ້ຈັກ ເພື່ອໃຊ້ ມາລແວຣ໌ ຫຼື ແຮັກ ອຸປະກອນຂອງທ່ານ. ຖ້າທ່ານຕ້ອງການຄວາມຊ່ວຍເຫຼືອ, ACSC ໄດ້ເຜີຍແຜ່ ຄຳແນະນຳກ່ຽວກັບການອັບເດດ.

ຖ້າອຸປະກອນ ຫຼື ຊອັບແວຂອງທ່ານເກົ່າເກີນໄປ, ການອັບ ເດດອາດຈະບໍ່ມີໃຫ້. ຖ້າຜູ້ຜະລິດຢຸດການສະໜັບສະໜູນ ຜະລິດຕະພັນດ້ວຍການອັບເດດ, ທ່ານຄວນພິຈາລະນາ ຍົກລະດັບເປັນຜະລິດຕະພັນທີ່ໃໝ່ເພື່ອໃຫ້ປອດໄພ. ຕົວຢ່າງຂອງລະບົບທີ່ບໍ່ໄດ້ຮັບ ການອັບເດດທີ່ສຳຄັນ ແມ່ນ **iPhone 7** ແລະ **Microsoft Windows 7.**

ສຳລັບຂໍ້ມູນເພີ່ມເຕີມອ່ານຄຳແນະນຳຂອ ພວກເຮົາກ່ຽວກັບ ການອັບເດດ ມີຢູ່ທີ່ **cyber.gov.au/updates.**

✓ **ເປີດການອັບເດດອັດຕະໂນມັດສຳລັບ ອຸປະກອນ ແລະ ຊອັບແວຂອງທ່ານ.**

ໃຊ້ຊອັບແວຄວາມປອດໄພ

ຊອັບແວຮັກສາຄວາມປອດໄພເຊັ່ນ ແອນຕິໄວຣັສ ແລະ ແຮມຊຳ ແວ ສາມາດ ຊ່ວຍປົກປ້ອງ ອຸປະກອນຂອງທ່ານ.

ໃຊ້ຊອັບແວຄວາມປອດໄພເພື່ອກວດຫາ ແລະ ລຶບ ມາລ ແວ ອອກຈາກອຸປະກອນຂອງທ່ານ. ຊອັບແວແອນຕິໄວຣັສ ສາມາດຖືກຕັ້ງຄ່າເພື່ອສະແກນຫາໄຟລ໌ ແລະ ໂປຣແກຣມທີ່ ໜ້າສົງໄສ ເປັນປະຈຳ. ເມື່ອພົບໄພຂົ່ມຂູ່, ທ່ານຈະໄດ້ຮັບການ ແຈ້ງເຕືອນແລະໄຟລ໌ທີ່ໜ້າສົງໄສຈະຖືກ ກັກກັນຫຼືເອົາອອກ.

ທຸລະກິດຂະໜາດນ້ອຍຈຳນວນຫຼາຍສາມາດນຳໃຊ້ **Windows Security** ເພື່ອປົກປ້ອງຕົນເອງ ຈາກໄວຣັສແລະ ມາລແວ. Windows Security ແມ່ນມີຢູ່ໃນອຸປະກອນ ວິນໂດສ໌ 10 ແລະ ວິນໂດສ໌ 11 ແລະ ປະກອບມີການປ້ອງກັນໄວຣັສ ແລະ ໄພ ຂົ່ມຂູ່ຟຣີ. ທ່ານຍັງສາມາດໃຊ້ມັນ ເພື່ອເປີດໃຊ້ຄຸນສົມບັດ ການປ້ອງກັນ ແຮມຊຳແວ໌ ໃນອຸປະກອນຂອງທ່ານ.

ສຳລັບຜະລິດຕະພັນແລະທາງເລືອກອື່ນໆ ຈົ່ງອ່ານ ຄຳແນະ ນຳຂອງພວກເຮົາກ່ຽວກັບຊອັບແວ ແອນຕິໄວຣັສ, ໂດຍ ການຊອກຫາ ແອນຕິໄວຣັສ ໃນ **cyber.gov.au.**

✓ **ຕັ້ງຄ່າຊອັບແວຮັກສາຄວາມປອດໄພເພື່ອທຳການ ສະແກນອຸປະກອນຂອງທ່ານເປັນປະຈຳ.**

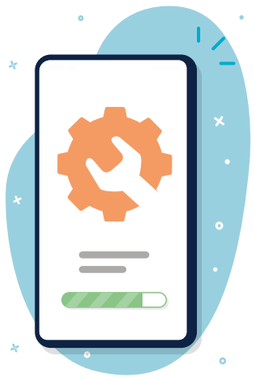
ສຳຮອງຂໍ້ມູນ ຂອງທ່ານ

ການສຳຮອງຂໍ້ມູນເປັນປະຈຳສາມາດຊ່ວຍໃຫ້ທ່ານກູ້ຄືນ ຂໍ້ມູນຂອງທ່ານຖ້າຫາກວ່າມັນສູນ ເສຍຫຼືຖືກບຸກລຸກ.

ການສຳຮອງຂໍ້ມູນສຳຄັນຄວນຈະເປັນການປະຕິບັດປົກກະຕິ ຫຼື ເປັນໂດຍອັດຕະໂນມັດ ໃນທຸລະກິດຂອງທ່ານ. ຖ້າຫາກບໍ່ມີ ການສຳຮອງຂໍ້ມູນເປັນປະຈຳ, ມັນອາດເປັນໄປບໍ່ໄດ້ສຳລັບທ່ານ ທີ່ຈະກູ້ຄືນຂໍ້ມູນຂອງທ່ານຫຼັງຈາກການໂຈມຕີທາງໄຊເບີ.

ມີຫຼາຍວິທີ ແລະ ຜະລິດຕະພັນທີ່ທ່ານສາມາດໃຊ້ເພື່ອສຳຮອງຂໍ້ມູນ ຂອງທ່ານ. ສຳລັບຄຳແນະນຳ ຢ່າງລະອຽດກ່ຽວກັບການສຳຮອງ ຂໍ້ມູນທຸລະກິດຂອງທ່ານ, ຈົ່ງອ່ານຄຳແນະນຳສຳລັບການສຳຮອງ ຂໍ້ມູນຂອງພວກເຮົາ ຊຶ່ງມີໃຫ້ຢູ່ທີ່ **cyber.gov.au/backups.** ທາງເລືອກທີ່ດີທີ່ສຸດຈະແຕກຕ່າງ ກັນໄປສຳລັບແຕ່ລະທຸລະກິດ ດັ່ງນັ້ນຈົ່ງເວົ້າລົມກັບຜູ້ຊ່ຽວຊານດ້ານ IT ຖ້າຫາກວ່າທ່ານບໍ່ແນ່ໃຈ.

✓ **ສ້າງແລະນຳປະຕິບັດແຜນການເພື່ອ ສຳຮອງຂໍ້ມູນຂອງທ່ານຢ່າງສະໝ່ຳສະເໝີ.**



ຮັກສາຄວາມປອດໄພເຄືອຂ່າຍຂອງ ທ່ານ ແລະການບໍລິການພາຍນອກ

ປົກປ້ອງທຸລະກິດຂອງທ່ານຈາກການໂຈມຕີທາງໄຊເບີ ໂດຍການແກ້ໄຂ ຄວາມສ່ຽງທີ່ອາດເກີດຂຶ້ນໄດ້ໃນ ເຄືອຂ່າຍຂອງທ່ານ

ອຸປະກອນ ແລະ ການບໍລິການຕ່າງໆໃນເຄືອຂ່າຍຂອງທ່ານ ສາມາດເປັນເປົ້າໝາຍຫຼັກຂອງ ອາຊະຍາກອນໄຊເບີ.

ຫຼາຍໆລະບົບຈາກລະບົບເຫຼົ່ານີ້ອາດມີຄວາມຊັບຊ້ອນໃນ ການຮັກສາຄວາມປອດໄພ, ສະນັ້ນ ໃຫ້ປຶກສາຫາລືກ່ຽວ ກັບຄຳແນະນຳຕໍ່ໄປນີ້ກັບຜູ້ຊ່ຽວຊານດ້ານໄອທີ.

- **ຮັກສາຄວາມປອດໄພເຊີຟເວີຣ໌ຂອງທ່ານ:** ຖ້າທ່ານໃຊ້ NAS ຫຼື ເຊີຟເວີຣ໌ອື່ນໆຢູ່ໃນເຮືອນ ຫຼື ທຸລະກິດຂອງທ່ານ, ໃຫ້ໃຊ້ ຄວາມລະມັດລະວັງເປັນພິເສດເພື່ອຮັກສາຄວາມປອດໄພ. ອຸປະກອນເຫຼົ່ານີ້ ແມ່ນເປົ້າໝາຍທົ່ວໄປສຳລັບອາຊະຍາກອນໄຊເບີ ເພາະວ່າພວກເຂົາມັກຈະເກັບຮັກສາໄຟລ໌ທີ່ສຳຄັນ ຫຼື ປະຕິບັດໜ້າ ທີ່ສຳຄັນ. ມີຫຼາຍຍຸດທະສາດ ການຫຼຸດຜ່ອນທີ່ຈຳເປັນຈຳນວນຫຼາຍ ເພື່ອປົກປ້ອງອຸປະກອນເຫຼົ່ານີ້. ຕົວຢ່າງ, ມັນເປັນສິ່ງສຳຄັນທີ່ ຈະໃຫ້ແນ່ໃຈວ່າເຄື່ອງເຊີຟເວີຣ໌ ຫຼື ອຸປະກອນ NAS ໄດ້ຮັບການອັບ ເດດ ເປັນປະຈຳ. ບັນຊີບໍລິຫານລະບົບຄວນໄດ້ຮັບການຮັບປະກັນ ດ້ວຍລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ ຫຼື ການຢືນຢັນດ້ວຍຫຼາຍປັດໄຈ.
- **ຫຼຸດຮອຍສຳຜັດກັບພາຍນອກໃຫ້ເຫຼືອໜ້ອຍທີ່ສຸດ:** ກວດສອບ ແລະຮັບປະກັນການບໍລິການໃດໆທີ່ເປີດເຜີຍທາງອິນເຕີເນັດຢູ່ໃນ ເຄືອຂ່າຍຂອງທ່ານ. ອັນນີ້ອາດຈະລວມເຖິງ Remote Desktop, File Shares, Webmail ແລະບໍລິການບໍລິຫານທາງໄກ.
- **ຍ້າຍໄປບໍລິການຄລາວ:** ພິຈາລະນາໃຊ້ບໍລິການອອນໄລນ໌ ຫຼື ບໍລິການຄລາວ ທີ່ໃຫ້ຄວາມປອດໄພໃນຕົວ ແທນທີ່ຈະ ຈັດການດ້ວຍຕົນເອງ. ຕົວຢ່າງ, ໃຊ້ບໍລິການອອນໄລນ໌ສຳລັບ ສິ່ງຕ່າງໆເຊັ່ນອີເມວ ຫຼື ໂຮສຕ໌ເວັບໄຊທ໌ແທນທີ່ຈະດຳເນີນການ ແລະຮັບປະກັນການບໍລິການເຫຼົ່ານີ້ ດ້ວຍຕົວທ່ານເອງ.
- **ປັບປຸງຄວາມປອດໄພຂອງ ເຣົາເຕີຣ໌ ຂອງທ່ານ:** ປະຕິບັດຕາມ ຄຳແນະນຳຂອງພວກເຮົາກ່ຽວກັບ ວິທີປົກປ້ອງ ເຣົາເຕີຣ໌ ຂອງທ່ານ, ລວມທັງການອັບເດດລະຫັດຜ່ານເລີ່ມຕົ້ນ, ເປີດ Wi-Fi “ແຂກ” ສຳລັບລູກຄ້າ ຫຼື ຜູ້ເຂົ້າຢ້ຽມຊົມ ແລະ ການ ໃຊ້ພິທີການການເຂົ້າລະຫັດທີ່ແຂງແຮງທີ່ສຸດ. ຊອກຫາເຣົາ ເຕີຣ໌ ໃນ **cyber.gov.au** ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ.
- **ໃຫ້ເຂົ້າໃຈລະບົບການສະໜອງແບບຕ່ອງໂສ້ທາງໄຊເບີ ຂອງທ່ານ:** ທຸລະກິດທີ່ທັນສະໄໝມັກຈະໃຊ້ ບໍລິການຈາກ ພາຍນອກໃນການບໍລິການຫຼາຍຢ່າງ. ຕົວຢ່າງ, ການນຳໃຊ້ຜູ້ ໃຫ້ບໍລິການທີ່ມີການຄຸ້ມຄອງເພື່ອຮັກສາ ລະບົບໄອທີຂອງ ພວກເຂົາ. ບັນຫາດ້ານຄວາມປອດໄພຂອງການບໍລິການ ຫຼື ຜູ້ ໃຫ້ບໍລິການເຫຼົ່ານີ້ອາດມີຜົນ ກະທົບອັນໃຫຍ່ຫຼວງຕໍ່ທຸລະກິດ ຂອງທ່ານ. ສຳລັບຄຳແນະນຳຢ່າງລະອຽດກ່ຽວກັບການຄຸ້ມຄອງ ຄວາມສ່ຽງລະບົບຕ່ອງໂສ້ການ ສະໜອງທາງໄຊເບີ ໃຫ້ອ່ານ ຄຳແນະນຳ ການສະໜອງແບບຕ່ອງໂສ້ທາງໄຊເບີ (Cyber Supply Chain) ຂອງພວກເຮົາທີ່ **cyber.gov.au.**

✓ **ເວົ້າລົມກັບຜູ້ຊ່ຽວຊານດ້ານໄອທີກ່ຽວກັບ ວິທີຮັກສາຄວາມປອດໄພເຄືອຂ່າຍຂອງທ່ານ.**

ເຮັດໃຫ້ເວັບໄຊທ໌ຂອງທ່ານເຂັ້ມແຂງຂຶ້ນ

ເວັບໄຊທ໌ແມ່ນເປົ້າໝາຍຫຼັກສຳລັບການໂຈມຕີທາງໄຊເບີ.

ປົກປ້ອງເວັບໄຊທ໌ຂອງທ່ານຈາກການຖືກແຮັກໂດຍປະຕິບັດຕາມ ມາດຕະການການຮັກສາຄວາມປອດໄພ ຂັ້ນພື້ນຖານບາງຢ່າງ:

- ຮັບປະກັນການເຂົ້າສູ່ລະບົບເວັບໄຊທ໌ຂອງທ່ານດ້ວຍການ ຢືນຢັນດ້ວຍຫຼາຍປັດໄຈ ຫຼື ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ
- ອັບເດດລະບົບການຈັດການເນື້ອຫາ ແລະ ປລັກ ອິນຂອງເວັບໄຊທ໌ຂອງທ່ານເປັນປະຈຳ
- ສຳຮອງເວັບໄຊທ໌ຂອງທ່ານເປັນປະຈຳເພື່ອໃຫ້ທ່ານ ສາມາດກູ້ຄືນໄດ້ຫຼັງຈາກການໂຈມຕີທາງໄຊເບີ.

ACSC ມີຊັບພະຍາກອນເພີ່ມເຕີມສຳລັບເຈົ້າຂອງເວັບໄຊທ໌. ຄົ້ນຫາຊັບພະຍາກອນເຫຼົ່ານີ້ຢູ່ໃນ **cyber.gov.au:**

- Quick Wins ສຳລັບເວັບໄຊທ໌ຂອງທ່ານ
- ການນຳໃຊ້ປະຕິບັດໃບຢັ້ງຢືນ, TLS, HTTPS ແລະ TLS ທີ່ສ້າງໂອກາດ
- ຄວາມປອດໄພຂອງລະບົບຊື່ໂດເມນສຳລັບເຈົ້າຂອງໂດເມນ
- ການກະກຽມແລະຕອບສະໜອງຕໍ່ການໂຈມຕີ ແບບປະຕິເສດການໃຫ້ບໍລິການ

✓ **ອ່ານຊັບພະຍາກອນ ຂອງ ACSC ກ່ຽວກັບຄວາມປອດໄພຂອງເວັບໄຊທ໌.**

ຣີເຊັດອຸປະກອນຂອງທ່ານກ່ອນ ການຂາຍ ຫຼື ກຳຈັດພວກມັນ

ຂໍ້ມູນໃນອຸປະກອນເຄື່ອງເກົ່າຂອງທ່ານສາມາດ ຖືກເຂົ້າເຖິງໄດ້ໂດຍຄົນແປກໜ້າ.

ຖ້າທ່ານບໍ່ຖິ້ມອຸປະກອນຂອງທ່ານຢ່າງປອດໄພ, ອາດຊະຍາກອນໄຊເບີ ສາມາດເຂົ້າເຖິງ ຂໍ້ມູນໃນອຸປະກອນນັ້ນໄດ້. ອັນນີ້ອາດຮວມມີອີເມວ, ໄຟລ໌ ແລະ ຂໍ້ມູນທຸລະກິດອື່ນໆ. ເອົາຂໍ້ມູນທັງໝົດອອກຈາກອຸປະກອນ ທຸລະກິດຂອງທ່ານກ່ອນທີ່ຈະຂາຍ, ແລກປ່ຽນ ຫຼື ໂຍນຖິ້ມໄປ. ຕົວຢ່າງ ເຊັ່ນ ດ້ວຍການເຣັດ ແຟັກຕໍຣີ ຣີເຊັດ. ສິ່ງນີ້ຈະຊ່ວຍໃຫ້ລຶບຂໍ້ມູນ ໃດໆແລະຟື້ນຟູອຸປະກອນ ໃຫ້ກັບໄປສູ່ການຕັ້ງຄ່າດັ້ງເດີມຂອງມັນ.

ສຳລັບຄຳແນະນຳກ່ຽວກັບການຣີເຊັດອຸປະກອນຂອງທ່ານ, ໃຫ້ອ່ານ ຄຳແນະນຳຂອງພວກເຮົາກ່ຽວກັບ ວິທີການກຳຈັດອຸປະກອນຂອງ ທ່ານຢ່າງປອດໄພ. ຊອກຫາການກຳຈັດ ທີ່ **cyber.gov.au.**

✓ **ເຣັດ ແຟັກຕໍຣີ ຣີເຊັດ ກ່ອນການຂາຍ ຫຼື ການຖິ້ມອຸປະກອນທາງທຸລະກິດ.**

ລັອກອຸປະກອນຂອງທ່ານ ໄວ້ ແລະ ເກັບຮັກສາໜ່ວ ອຸປະກອນໃຫ້ປອດໄພ

ການຈຳກັດການເຂົ້າເຖິງອຸປະກອນທຸລະກິດຂອງທ່ານຈະ ຫຼຸດຜ່ອນໂອກາດສຳລັບກິດຈະກຳທີ່ເປັນອັນຕະລາຍ.

ການຈຳກັດການເຂົ້າເຖິງອຸປະກອນທຸລະກິດຂອງທ່ານເປັນ ວິທີງ່າຍໆເພື່ອປ້ອງກັນບໍ່ໃຫ້ຂໍ້ ມູນຖືກລັກ ຫຼື ກິດຈະກຳ ທີ່ເປັນອັນຕະລາຍອື່ນໆ. ອຸປະກອນທຸລະກິດບໍ່ຄວນ ຖືກເກັບຮັກສາໄວ້ໃນບ່ອນທີ່ພະນັກງານຫຼືສະມາຊິກ ສາທາລະນະທີ່ບໍ່ ໄດ້ຮັບອະນຸຍາດສາມາດເຂົ້າເຖິງໄດ້.

ໃຊ້ການຄວບຄຸມຄວາມປອດໄພເພື່ອປົກປ້ອງອຸປະກອນທາງ ທຸລະກິດຂອງທ່ານຕື່ມອີກ. ຢ່າງຫນ້ອຍ, ອຸປະກອນນັ້ນຄວນ ຈະຖືກລັອກດ້ວຍຂໍ້ຄວາມລະຫັດຜ່ານ, PIN ຫຼື ໄບໂອເມຕຣິກ ກວດສອບໃຫ້ ແນ່ໃຈວ່າອຸປະກອນເຫຼົ່ານີ້ໄດ້ຮັບການຕັ້ງຄ່າໃຫ້ລັອກ ໂດຍອັດຕະໂນມັດຫຼັງຈາກທີ່ບໍ່ມີການໃຊ້ງານ ເປັນ ໄລຍະເວລາສັ້ນໆ.

✓ **ຕັ້ງຄ່າອຸປະກອນໃຫ້ອັດຕະໂນມັດ ລັອກໄວ້ຫຼັງຈາກບໍ່ມີການໃຊ້ງານເປັນເວລາສັ້ນໆ.**

ປົກປ້ອງຂໍ້ມູນທຸລະກິດຂອງທ່ານ

ຂໍ້ມູນທີ່ເກັບກຳໄວ້ໂດຍທຸລະກິດຂອງທ່ານເປັນ ເປົ້າໝາຍທີ່ໜ້າດຶງດູດສຳລັບອາຊະຍາກອນໄຊເບີ.

ການລະເມີດຂໍ້ມູນເພີ່ມຂຶ້ນເລື້ອຍໆ - ຢ່າປ່ອຍໃຫ້ທຸລະກິດຂອງ ທ່ານຕົກເປັນເຫຍື່ອ. ມັນເປັນສິ່ງສຳຄັນ ທີ່ຈະເຂົ້າໃຈວ່າທຸລະກິດ ຂອງທ່ານມີຂໍ້ມູນໃດແດ່ ແລະ ຢູ່ໃນສະຖານທີ່ໃດ. ເມື່ອທ່ານຮູ້ແລ້ວ, ໃຫ້ໃຊ້ຄຳແນະນຳໃນຄູ່ມືນີ້ເພື່ອຊ່ວຍປົກປ້ອ ຂໍ້ມູນຂອງທ່ານ ຈາກການຖືກເຂົ້າເຖິງໂດຍ ອາຊະຍາກອນໄຊເບີ. ບາງທຸລະກິດ ຂະໜາດນ້ອຍອາດມີພັນທະເພີ່ມເຕີມພາຍໃຕ້ກົດໝາຍ.

- **ລວມສູນຂໍ້ມູນທຸລະກິດຂອງທ່ານ.** ທ່ານອາດຈະມີຂໍ້ມູນ ເກັບຮັກສາໄວ້ໃນອຸປະກອນ ຫຼື ການບໍລິການຕ່າງໆຈຳນວນ ຫຼາຍ. ເມື່ອຂໍ້ມູນຖືກແບ່ງຂັ້ນຄຸ້ມຄອງ, ມັນຈະເພີ່ມຈຳນວນ ຂອງລະບົບທີ່ທ່ານຕ້ອງຮັກສາຄວາມປອດໄພແລະສຳຮອງ ຂໍ້ມູນ. ລະບົບຈຳນວນຫຼາຍຍັງສາມາດສ້າງໂອກາດໃຫ້ອາຊະ ຍາກອນໄຊເບີທີ່ຈະໂຈມຕີໄດ້ຫຼາຍຂຶ້ນ. ຖ້າເປັນໄປໄດ້, ໃຫ້ ເກັບຮັກສາຂໍ້ມູນທຸລະກິດຂອງທ່ານໄວ້ຢູ່ໃນຕຳແໜ່ງສູນກາງ ທີ່ປອດໄພ ແລະ ສຳຮອງຂໍ້ມູນເປັນປະຈຳ. ການລວມສູນ ຂໍ້ມູນຂອງທ່ານສາມາດສ້າງການລະເມີດທີ່ໃຫຍ່ກວ່າຖ້າ ລະບົບ ຂອງທ່ານຖືກທຳລາຍ, ດັ່ງນັ້ນໃຫ້ແນ່ໃຈວ່າຕຳແໜ່ງ ສູນກາງນີ້ຖືກປົກປ້ອງຢ່າງພຽງພໍດ້ວຍການຕັ້ງຄ່າ ທີ່ປອດໄພ ແລະການເຂົ້າເຖິງທີ່ຖືກຈຳກັດ. ເວົ້າລົມກັບຜູ້ຊ່ຽວຊານດ້ານ ໄອທີ ຫຼື ຄວາມປອດໄພທາງໄຊເບີ ເພື່ອຂໍຄຳແນະນຳ.
- **ຮູ້ຈັກພາລະໜ້າທີ່ຂອງທ່ານໃນການປົກປ້ອງຂໍ້ມູນ.** ບາງ ທຸລະກິດຂະໜາດນ້ອຍອາດມີພັນທະທາງດ້ານກົດໝາຍ ໃນການຈັດການຂໍ້ມູນສ່ວນຕົວທີ່ພວກເຂົາເກັບກຳ. ອ່ານ ຂ່າວສານຂອງ ຄະນະກຳມາທິການຂໍ້ມູນ ຂອງອອສເຕຣ ເລັຍ ກ່ຽວກັບ ຄຳແນະນຳສຳລັບທຸລະກິດຂະໜາດນ້ອຍ ເພື່ອຮຽນຮູ້ເພີ່ມເຕີມ, ມີໃຫ້ຢູ່ທີ່ **oaic.gov.au** ປຶກສາ ກັບຜູ້ຊ່ຽວຊານດ້ານກົດໝາຍຖ້າທ່ານບໍ່ແນ່ໃຈ.

✓ **ໃຫ້ເຂົ້າໃຈຂໍ້ມູນທີ່ທຸລະກິດຂອງທ່ານເກັບໄວ້ ແລະ ຄວາມຮັບຜິດຊອບຂອງທ່ານໃນການປົກປ້ອງມັນ.**

ກະກຽມພະນັກງານຂອງທ່ານ

ໃຫ້ຄວາມຮູ້ແກ່ພະນັກງານ

ພະນັກງານທີ່ມີແນວປະຕິບັດດ້ານຄວາມປອດໄພທາງໄຊເບີທີ່ ດີແມ່ນການປ້ອງກັນການໂຈມຕີ ທາງໄຊເບີທຳອິດຂອງທ່ານ.

ພະນັກງານຂອງທ່ານຄວນມີຄວາມຮັບຮູ້ກ່ຽວກັບ ຄວາມປອດໄພທາງໄຊເບີ, ລວມທັງຫົວຂໍ້ຕໍ່ໄປນີ້:

- ໄພຂົ່ມຂູ່ຕໍ່ຄວາມປອດໄພທາງໄຊເບີທົ່ວໄປເຊັ່ນ: ການປອມແປງ ອີເມວທຸລະກິດ ແລະ ແຣນຊໍາແວ໌
- ມາດຕະການປ້ອງກັນລວມທັງລະຫັດຜ່ານ ຫຼື ຂໍ້ຄວາມ ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ, MFA ແລະ ການອັບເດດຊອັບແວ
- ວິທີການສັງເກດການຫຼອກລວງ ແລະ ການໂຈມຕີ ແບບ ຟິຊຊິ່ງ
- ນະໂຍບາຍສະເພາະທາງທຸລະກິດ (ຕົວຢ່າງ ຂະບວນການ ລາຍງານອີເມວທີ່ໜ້າສົງໄສ ຫຼື ການກວດສອບ ໃບເກັບເງິນວ່າເປັນຂອງແທ້ກ່ອນຈ່າຍເງິນ)
- ຈະເຮັດແນວໃດໃນກໍລະນີສຸກເສີນ.

ເວັບໄຊທ໌ ACSC ມີຊັບພະຍາກອນສຳລັບຫົວຂໍ້ເຫຼົ່ານີ້ສ່ວນໃຫຍ່ ຢູ່ທີ່ cyber.gov.au/learn ທ່ານອາດຈະພິຈາລະນາວິທີອື່ນ ໆຂອງການໃຫ້ຄວາມຮູ້ແກ່ພະນັກງານຂອງທ່ານ, ຍົກຕົວຢ່າງ ວ່າ, ມີຫຼັກສູດຢ່າງເປັນທາງການຫຼືການຝຶກອົບຮົມພາຍໃນ. ຢ່າງໃດກໍຕາມ, ບໍ່ວ່າທ່ານຕັດສິນໃຈແນວໃດ, ຈື່ໄວ້ວ່າການ ຝຶກອົບຮົມຄວາມປອດໄພທາງໄຊເບີບໍ່ແມ່ນຄວາມຕ້ອງການ ຄັ້ງດຽວແລະ ຄວນຈະໄດ້ຮັບ ການທວນຄືນເປັນໄລຍະ.

✓ **ກຳນົດວ່າ ການຮັບຮູ້ຄວາມປອດໄພທາງໄຊເບີ ຈະຖືກສອນໂດຍວິທີໃດໃນທຸລະກິດຂອງທ່ານ.**

ສ້າງແຜນການສຸກເສີນ

ແຜນສຸກເສີນສາມາດຫຼຸດຜ່ອນຜົນກະທົບ ຈາກການໂຈມຕີທາງໄຊເບີກ່ຽວກັບທຸລະກິດຂອງທ່ານໄດ້.

ເມື່ອຕອບສະໜອງຕໍ່ເຫດການຄວາມປອດໄພທາງໄຊເບີ, ຕ້ອງ ຄິດລະວັງທຸກໆນາທີ. ການມີແຜນສຸກເສີນໝາຍຄວາມວ່າ ພະນັກງານຂອງທ່ານສາມາດໃຊ້ເວລາໜ້ອຍລົງໃນການຄິດວ່າ ຕ້ອງເຮັດຫຍັງ ແລະ ໃຊ້ເວລາຫຼາຍຂຶ້ນໃນການດຳເນີນການ.

ພິຈາລະນາຄຳຖາມຕໍ່ໄປນີ້ໃນເວລາສ້າງແຜນສຸກເສີນຂອງທ່ານ:

- ພະນັກງານຂອງທ່ານມີຂະບວນການຢ່າງໃດສຳລັບລາຍງານ ເຫດການຄວາມປອດໄພທາງໄຊເບີທີ່ ອາດຈະເກີດຂຶ້ນ?
- ທ່ານຈະຕິດຕໍ່ຫາໃຜເພື່ອຂໍຄວາມຊ່ວຍເຫຼືອ? ຕົວຢ່າງ, ຜູ້ຊ່ຽວຊານດ້ານໄອທີແລະທະນາຄານຂອງທ່ານ.
- ເຫດການດັ່ງກ່າວຈະຖືກສື່ສານໄປຫາພະນັກງານ, ຜູ້ມີສ່ວນຮ່ວມ ຫຼື ລູກຄ້າຂອງທ່ານແນວໃດ?
- ທ່ານຈະຈັດການທຸລະກິດຕາມປົກກະຕິໄດ້ແນວ ໃດ ຖ້າລະບົບສຳຄັນໃດນຶ່ງຍັງອອຟໄລນ໌ຢູ່?

ໃຫ້ແນ່ໃຈວ່າພະນັກງານຂອງທ່ານມີຄວາມຄຸ້ນເຄີຍກັບແຜນການ ສຸກເສີນ ລວມທັງພາລະບົດບາດຫຼືຄວາມຮັບຜິດຊອບທີ່ ພວກເຂົາອາດຈະມີ. ຮັກສາສຳເນົາຂອງແຜນໃນກໍລະນີທີ່ ລະບົບຂອງທ່ານບໍ່ມີອິນເຕີເນັດໃນເວລາທີ່ທ່ານຕ້ອງການ.

✓ **ສ້າງແຜນສຸກເສີນສຳລັບ ເຫດການຄວາມປອດໄພທາງໄຊເບີ.**

ໃຫ້ທັນກັບສະພາບໃນການຮັບຊາບຂໍ້ມູນ

ກາຍເປັນຄູ່ຮ່ວມງານຂອງ ACSC ທີ່ຈະໄດ້ຮັບ ຂໍ້ມູນຫຼ້າສຸດຈາກ ACSC.

ຮັບຮູ້ຂໍ້ມູນໄພຂົ່ມຂູ່ທາງອິນເຕີເນັດຫຼ້າສຸດ ແລະຈຸດອ່ອນ ໂດຍການເປັນຄູ່ຮ່ວມງານຂອງ ACSC. ການບໍລິການ ນີ້ຈະສົ່ງຈົດໝາຍຂ່າວ ແລະການແຈ້ງເຕືອນລາຍເດືອນ ໃຫ້ທ່ານເມື່ອມີການລະບຸໄພຂົ່ມຂູ່ທາງໄຊເບີໃໝ່.

ຄວາມປອດໄພທາງໄຊເບີແມ່ນຂົງເຂດທີ່ພັດທະນາຢ່າງໄວວາ. ອາດຊະຍາກອນໄຊເບີ ໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫວ່ຢ່າງແຂງຂັນ ພາຍໃນບໍ່ເທົ່າໃດນາທີຫຼັງຈາກການຄົ້ນພົບ. ການທັນກັບສະ ພາບໃນການຮັບຊາບຂໍ້ມູນກ່ຽວກັບພູມສັນຖານຄວາມປອດໄພ ທາງໄຊເບີຈະຊ່ວຍໃຫ້ທຸລະກິດຂອງທ່ານເຂົ້າໃຈເຖິງໄພຂົ່ມຂູ່ ທີ່ມັນອາດຈະປະເຊີນ ແລະ ວິທີການປ້ອງກັນພວກມັນ.

✓ **ລົງທະບຽນທຸລະກິດຂອງທ່ານກັບ ໂຄງການເປັນຄູ່ຮ່ວມກັບ ACSC.**

ຂໍ້ຈຳກັດຄວາມຮັບຜິດຊອບ
ເນື້ອຫາໃນຄູ່ມືນີ້ແມ່ນມີລັກສະນະທົ່ວໄປ ແລະ ບໍ່ຄວນຖືວ່າເປັນຄຳແນະນຳທາງດ້ານກົດໝາຍ ຫຼື ອີງໃສ່ເປັນການຊ່ວຍເຫຼືອໃນສະຖານະການສະເພາະຫຼືສະຖານະການສຸກເສີນໃດໜຶ່ງ. ໃນເລື່ອງທີ່ສຳຄັນໃດໆ, ທ່ານຄວນຊອກຫາຄຳແນະນຳຈາກມືອາຊີບອິດສະລະທີ່ເໝາະສົມກັບສະຖານະການຂອງທ່ານເອງ.

ລັດຖະບານກາງຈະບໍ່ຮັບຜິດຊອບ ຫຼື ຮັບຜິດຊອບຕໍ່ຄວາມເສຍຫາຍ, ການສູນເສຍຫຼືຄ່າໃຊ້ຈ່າຍໃດໆທີ່ເກີດຂຶ້ນ ອັນເປັນຜົນມາຈາກການອີງໃສ່ຂໍ້ມູນທີ່ມີຢູ່ໃນຄູ່ມືນີ້.

ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ ຫຼື ລາຍງານເຫດການຄວາມປອດໄພທາງໄຊເບີ ຕິດຕໍ່ພວກເຮົາ:
cyber.gov.au | 1300 CYBER1 (1300 292 371)
ເບີໂທນີ້ສາມາດໃຊ້ໄດ້ພາຍໃນອອສເຕຣເລັຍເທົ່ານັ້ນ.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre