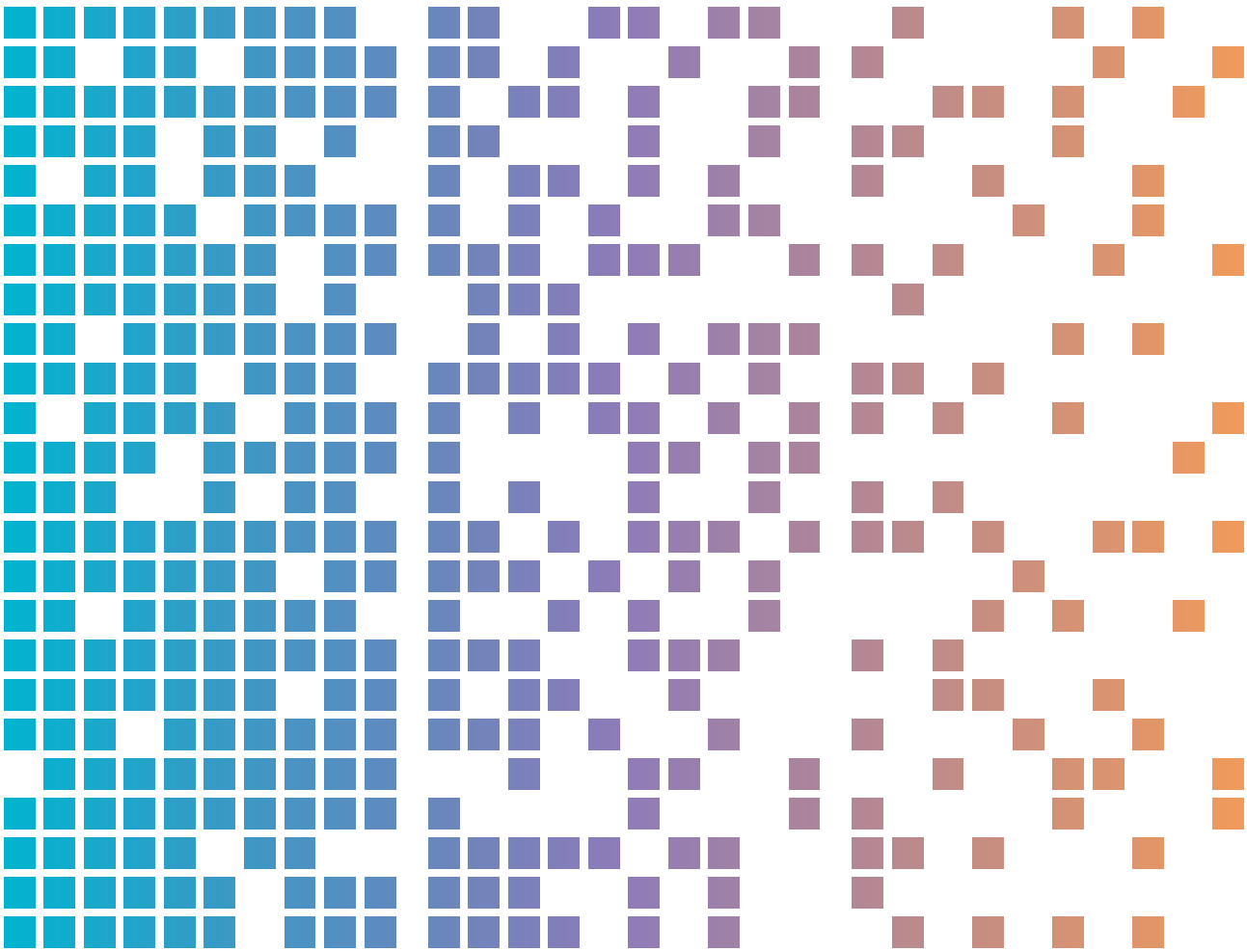
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ການໂຈມຕີທາງໄຊເບີໃຊ້ມັນເວລັກຂໍ້ມູນເພື່ອເຈາະເຄືອຂ່າຍອົງກອນ



ຄວາມຊັບຊ້ອນຂອງເນື້ອຫາ
ປານກາງ

cyber.gov.au

ສາລະບານ

ບໍລິບົດ

ມັນແວລັກຂໍ້ມູນຈະລັກຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ ແລະ ຂໍ້ມູນລະບົບທີ່ກໍ່ອາຊະຍາກຳທາງໄຊເບີໃຊ້ປະໂຫຍດ, ໂດຍສ່ວນໃຫຍ່ເພື່ອຜົນປະໂຫຍດທາງການເງິນ. ມີຜູ້ສັງເກດເຫັນຜູ້ລັກລອບຂໍ້ມູນໃນການໂຈມຕີທາງໄຊເບີຕໍ່ອົງກອນ ແລະ ພາກສ່ວນຕ່າງໆ ທົ່ວໂລກ, ລວມທັງໃນອອສເຕຣເລຍ. ສື່ສິ່ງພິມນີ້ໃຫ້ຄຳແນະນຳກ່ຽວກັບຄວາມປອດໄພທາງໄຊເບີໃຫ້ກັບຜູ້ອ່ານກ່ຽວກັບມັນແວທີ່ລັກຂໍ້ມູນ, ລວມທັງກິດຈະກຳຄຸກຄາມ ແລະ ຄຳແນະນຳໃນການບັນເທົາຜົນກະທົບສຳລັບອົງກອນ ແລະ ພະນັກງານຂອງພວກເຂົາ.

ປະເດັນສຳຄັນ

- ມັນແວລັກຂໍ້ມູນ, ທີ່ຮູ້ຈັກກັນໃນນາມຜູ້ລັກຂໍ້ມູນ, ເປັນມັນແວປະເພດໜຶ່ງທີ່ອອກແບບມາເພື່ອລວບລວມຂໍ້ມູນຈາກອຸປະກອນຂອງຜູ້ຖືກເຄາະຮ້າຍ. ເຊິ່ງອາດລວມເຖິງຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານ, ລາຍລະອຽດບັດເຄຣດິດ, ກະເປົ໋າເງິນສະກຸນເງິນດິຈິຕອນ, ໄຟລ໌ໃນເຄື່ອງ ແລະ ຂໍ້ມູນຂອງຕົວທ່ອງເວັບລວມທັງຄຸກກີ້, ປະຫວັດຜູ້ໃຊ້ ແລະ ລາຍລະອຽດແບບຟອມຕື່ມຂໍ້ມູນອັດຕະໂນມັດ.
- ອາຊະຍາກຳທາງໄຊເບີອາດຈະພະຍາຍາມຊື້ ແລະ ນຳໃຊ້ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ຖືກລັກທີ່ກ່ຽວຂ້ອງກັບບັນຊີຂອງອົງກອນ ເພື່ອເຂົ້າເຖິງອຸປະກອນຂອງນາຍຈ້າງຂອງເຫຍື່ອ ແລະ ລະບົບຂອງອົງກອນອື່ນໆ ເປັນຄັ້ງທຳອິດ. ຜົນກະທົບທີ່ເກີດຂຶ້ນຕໍ່ອົງກອນເຫຼົ່ານີ້ອາດລວມເຖິງ ຕໍ່ມາຕໍ່ກັບອົງການຈັດຕັ້ງເຫຼົ່ານີ້ສາມາດປະກອບມີແຣມຊັນແວ, ການຂົ່ມເຫັງ, ການບຸກລຸກອີເມວທຸລະກິດ ແລະ ການລັກຊັບສິນທາງປັນຍາ.
- ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອົດສະຕຣາລີ (ACSC ຂອງ ASD) ສັງກັດສຳນັກງານສັນຍານອົດສະຕາລີ ໄດ້ລະບຸເຖິງການລະເມີດເຄື່ອຂ່າຍຂອງອົງກອນທີ່ມີຕົ້ນຕໍມາຈາກສຳນັກງານທີ່ເຂົ້າເຖິງແຫຼ່ງຂໍ້ມູນການເຮັດວຽກຈາກອຸປະກອນສ່ວນຕົວທີ່ຖືກບຸກລຸກ. ໃນຫຼາຍໆກໍລະນີ, ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີສາມາດເຂົ້າເຖິງເຄືອຂ່າຍຂອງອົງກອນໃນເບື້ອງຕົ້ນໄດ້ໂດຍການໃຊ້ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ຖືກຕ້ອງທີ່ຖືກລັກ. ການສືບສວນຂອງພວກເຮົາໄດ້ສະແດງໃຫ້ເຫັນວ່າການປະນີປະນອມຢ່າງກວ້າງຂວາງມັກຈະເກີດຂຶ້ນຫຼັງຈາກທີ່ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີເຂົ້າເຖິງບັນຊີຜູ້ໃຊ້ທີ່ໄດ້ຮັບສິດທິພິເສດຢ່າງສຳເລັດຜົນ.
- ອົງກອນທີ່ອຳນວຍຄວາມສະດວກໃຫ້ແກ່ພະນັກງານ, ຜູ້ຮັບເໝົາ, ຜູ້ໃຫ້ບໍລິການ ຫຼື ໜ່ວຍງານອື່ນໆທີ່ມີການຄຸ້ມຄອງ ໃນການເຂົ້າເຖິງເຄືອຂ່າຍຈາກໄລຍະໄກ, ລວມທັງການນຳເອົາຮາດແວ Your Own Device (BYOD) ຈຳເປັນຕ້ອງຮູ້ເຖິງຄວາມສ່ຽງຂອງຜູ້ລັກຂໍ້ມູນ ແລະ ປົກປ້ອງຕົນເອງຈາກໄພຂົ່ມຂູ່ນີ້. ອາຊະຍາກຳທາງໄຊເບີໃຊ້ໂປຣແກຣມລັກຂໍ້ມູນກັບອຸປະກອນຂອງເຫຍື່ອ ໂດຍໃຊ້ເທດນິກຕ່າງໆ ຢ່າງຫຼວງຫຼາຍ ເຊັ່ນ: ອີເມວຟິດຊິງ, ການດາວໂຫຼດຊອບແວລະເມີດສິດທິ, ເທດນິກການເພີ່ມປະສິດທິພາບເຄື່ອງມືຄົ້ນຫາ (SEO) ໂຄສະນາທີ່ເປັນອັນຕະລາຍ ຫຼື ລິ້ງທີ່ເປັນອັນຕະລາຍທີ່ໂພສໃນເວທີສື່ມວນຊົນສັງຄົມ. ໂດຍທົ່ວໄປ, ອຸປະກອນທີ່ໃຊ້ສຳລັບທັງການເຮັດວຽກ ແລະ ຈຸດປະສົງສ່ວນບຸກຄົນ ມີຄວາມສ່ຽງສູງຕໍ່ການຕິດເຊື້ອໂດຍຜ່ານເຕັກນິກເຫຼົ່ານີ້ເນື່ອງຈາກພຶດຕິກຳຂອງຜູ້ໃຊ້ ແລະ ການຄວບຄຸມຄວາມປອດໄພຫຼຸດລົງ.
- ຜູ້ລັກຂໍ້ມູນສະເໜີຮູບແບບທີ່ໜ້າສົນໃຈສຳລັບອາຊະຍາກຳ ທາງໄຊເບີເພື່ອສ້າງລາຍໄດ້ຈາກກິດຈະກຳອາຊະຍາກຳທາງໄຊເບີ, ໂດຍສະເພາະສຳລັບອາຊະຍາກຳທາງໄຊເບີລະດັບເລີ່ມຕົ້ນ ແລະ ຜູ້ທີ່ມີຄວາມຮູ້ດ້ານເຕັກນິກທີ່ຈຳກັດ. ອາຊະຍາກຳທາງໄຊເບີບາງຄົນຈະເຮັດການຕະຫຼາດຜະລິດຕະພັນຂອງຜູ້ລັກຂໍ້ມູນໂດຍໃຊ້ໂປຣແກຣມປະເພດ Malware-as-a-Service (MaaS), ໂດຍຄິດຄ່າບໍລິການການສະໝັກເປັນລາຍເດືອນ.

ຄວາມເປັນມາ

ການໃຊ້ເຄື່ອງມືລັກຂໍ້ມູນໂດຍອາດຊະຍາກຳທາງໄຊເບີ ກໍ່ໃຫ້ເກີດເປັນໄພຂົ່ມຂູ່ຕໍ່ຄວາມປອດໄພ ແລະ ຄວາມເປັນຢູ່ທີ່ດີຂອງອົງກອນຕ່າງໆ ໃນອົດສະຕຣາລີ. ການຕິດເຊື້ອຂອງຜູ້ລັກຂໍ້ມູນມີຢູ່ທົ່ວໄປເປັນກິດຈະກຳເບື້ອງຕົ້ນຂອງເຫດການຄວາມປອດໄພທາງໄຊເບີຄັ້ງໃຫ່ຍ, ເນື່ອງຈາກຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີໃຊ້ການຕິດໄວຣັດເພື່ອເກັບກຳຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້. ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ເຫຼົ່ານີ້, ໂດຍສະເພາະຜູ້ທີ່ສະໜອງການເຂົ້າເຖິງການບໍລິການທາງໄກທີ່ປະເຊີນກັບອິນເຕີເນັດ ຫຼື ບັນຊີສິດທິພິເສດ, ຈະຖືກນຳໄປໃຊ້ປະໂຫຍດເພື່ອໃຫ້ສາມາດເຂົ້າຫາລະບົບ ແລະ ຂໍ້ມູນຂອງອົງກອນໄດ້ໃນເບື້ອງຕົ້ນ.

ໝາຍເຫດ: ນາຍໜ້າການເຂົ້າເຖິງເບື້ອງຕົ້ນມີບົດບາດພິເສດພາຍໃນລະບົບນິເວດອາຊະຍາກຳທາງໄຊເບີໂດຍການຊື້ ແລະ ການກວດສອບຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ທີ່ຖືກລັກ. ຫຼັງຈາກນັ້ນ, ພວກເຂົານຳຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ມີຄຸນນະພາບສູງໄປປະມູນ, ເພື່ອນຳໄປໃຊ້ໃນສະພາບແວດລ້ອມຂອງອົງກອນທີ່ເປັນທີ່ຕ້ອງການ, ໃຫ້ກັບອາຊະຍາກຳທາງໄຊເບີທີ່ຈະນຳໃຊ້ຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ເພື່ອສະແຫ່ວງຫາຜົນປະໂຫຍດຈາກເຄື່ອຂ່າຍອົງກອນ.

ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຖືກລັກແມ່ນມີຄຸນຄ່າສູງສຳລັບອາຊະຍາກຳທາງໄຊເບີ, ເນື່ອງຈາກຈະເຮັດໃຫ້ການເຂົ້າເຖິງເຄືອຂ່າຍຂອງອົງກອນ ແລະ ລະບົບອົງກອນໃນເບື້ອງຕົ້ນວ່ອງໄວຍິ່ງຂຶ້ນ. ດ້ວຍການລັກຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ທີ່ຖືກຕ້ອງ, ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີສາມາດຫຼີກລ້ຽງວິທີ ແລະ ເທັກນິກທົ່ວໆໄປຫຼາຍປະການໄດ້ເຊັ່ນ:

- ການລະບຸ ແລະ ການວິໄຈເປົ້າໝາຍ
- ການລະບຸຈຸດອ່ອນໃນເຄື່ອຂ່າຍເປົ້າໝາຍ
- ການພັດທະນາວິທເຕີສຳລັບການເຂົ້າເຖິງເບື້ອງຕົ້ນ, ເຊັ່ນ:
  - ວັດສະດຸຟິດຊິ່ງ
  - ການໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫ່ວຂອງຊອບແວ
  - ການກຳໜົດເປົ້າໝາຍການບໍລິການທາງໄກ, ລວມທັງບໍລິການນະໂຍບາຍເດັສທ໊ອບທາງໄກ(RDP) ຫຼື ເຄືອຂ່າຍສ່ວນຕົວສະເໝືອນ(VPN)
  - ການໂຈມຕີແບບຮ້າຍຕໍ່ຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ (ການເດົາລະຫັດຜ່ານ).

ຂັ້ນຕອນເຫຼົ່ານີ້ຮຽກຮ້ອງໃຫ້ມີການລົງທຶນ ແລະ ລະດັບຄວາມຊຳນິຊຳນານດ້ານເທດນິກທີ່ນຳສະເໜີອຸປະສັກຕໍ່ອາຊະຍາກຳທາງໄຊເບີຈຳນວນໜຶ່ງ. ໂດຍສະເພາະ, ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີທີ່ບໍ່ສາມາດເຈາະລະບົບປ້ອງກັນເຄືອຂ່າຍຂອງອົງກອນນັ້ນໄດ້ຮັບຜົນປະໂຫຍດໂດຍກົງຈາກການຕິດເຊື້ອຂອງຜູ້ລັກຂໍ້ມູນ, ເນື່ອງຈາກການຕິດເຊື້ອເຫຼົ່ານີ້ສາມາດໃຫ້ການເຂົ້າເຖິງຂໍ້ມູນປະຈຳຕົວຂອງເຄື່ອຂ່າຍຜູ້ອົງກອນທີ່ຕ້ອງການໄດ້ໄວ ແລະ ງ່າຍດາຍ.

ໃນສະພາບແວດລ້ອມການເຮັດວຽກໄລຍະໄກ, ພະນັກງານບາງຄົນໃຊ້ອຸປະກອນສ່ວນຕົວສຳລັບທັງບ່ອນເຮັດວຽກ ແລະ ການຊອກຫາອິນເຕີເນັດສ່ວນຕົວ. ໃນການດຳເນີນການດັ່ງກ່າວ, ພະນັກງານອາດຈະເລືອກທີ່ຈະເກັບຮັກສາຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ຂອງຕົນຢູ່ໃນຄັງເກັບລະຫັດຜ່ານ ແລະ ສ່ວນຂະຫຍາຍຂອງຕົວທ່ອງເວັບ ຫຼື ພວກເຂົາອາດຈະໃຊ້ຄຸນສົມບັດການຕື່ມຂໍ້ມູນອັດຕະໂນມັດຂອງຕົວທ່ອງເວັບ. ຜູ້ລັກຂໍ້ມູນຈະກຳນົດເປົ້າໝາຍທີ່ຈັດເກັບລະຫັດຜ່ານເຫຼົ່ານີ້, ພ້ອມກັບຄຸກກີ້ການພິສູດຢືນຢັນ ແລະ ຂໍ້ມູນສ່ວນຕົວອື່ນໆພາຍໃນເວັບບຣາວເຊີ.

ບໍ່ເໝືອນກັບອຸປະກອນຂອງອົງກອນ, ອຸປະກອນສ່ວນບຸກຄົນບໍ່ໄດ້ບັງຄັບໃຊ້ນະໂຍບາຍຄວາມປອດໄພຂອງອົງກອນສະເໝີໄປ, ເຊິ່ງມີຄວາມສ່ຽງສູງຕໍ່ອົງກອນ. ຕົວຢ່າງ, ພະນັກງານອາດຈະມີສ່ວນຮ່ວມໃນກິດຈະກຳຕ່າງໆ ເຊັ່ນ: ການດາວໂຫຼດຊອບແວທີ່ລະເມີດລິຂະສິດ ແລະ ການທ່ອງເວັບອອນລາຍທີ່ມີຄວາມສ່ຽງສູງ, ເຊິ່ງເພີ່ມຄວາມສ່ຽງຕໍ່ກັບໄພຂົ່ມຂູ່ທາງໄຊເບີ ແລະ ການຕິດມັນແວຫຼາຍຂຶ້ນ.

ຜູ້ລັກຂໍ້ມູນ, ຜູ້ຈັດຈຳໜ່າຍ, ນາຍໜ້າເຂົ້າເຖິງເບື້ອງຕົ້ນ ແລະ ບໍລິສັດໃນເຄືອທີ່ຮັບແຮມຊັມແວກາຍມາເປັນສ່ວນສຳຄັນຂອງລະບົບນິເວດອາຊະຍາກຳທາງໄຊເບີທີ່ຂັບເຄື່ອນໂດຍຜົນກຳໄລທາງດ້ານການເງິນໃນປັດຈຸບັນ. ລະບົບນິເວດຈະເລີນເຕີບໂຕມີປະສິດທິພາບຫຼາຍຂຶ້ນເມື່ອອາດຊະຍາກຳທາງໄຊເບີຊ່ຽວຊານ ແລະ ພັດທະນາຂີດຄວາມສາມາດທີ່ກຳນົດເປົ້າໝາຍສະເພາະຂັ້ນຕອນຂອງການໂຈມຕີ ຈາກນັ້ນຈຶ່ງຂາຍຄວາມສາມາດດັ່ງກ່າວເປັນບໍລິການໃຫ້ກັບກຸ່ມອາຍາກຳອື່ນໆ.

ກິດຈະກຳໄພຂົ່ມຂູ່

ACSC ຂອງ ASD ກຳລັງຕິດຕາມ ແລະ ກວດສອບການເພີ່ມຂຶ້ນຂອງກິດຈະກຳລັກລອບຂໍ້ມູນທົ່ວໂລກ, ເຊິ່ງກໍ່ໃຫ້ເກີດໄພຂົ່ມຂູ່ທີ່ເພີ່ມຫຼາຍຂຶ້ນຕໍ່ເຄືອຂ່າຍອົດສະຕາລີ. ບົດລາຍງານຂອງອຸດສາຫະກຳຊີ້ໃຫ້ເຫັນວ່າຜູ້ລັກຂໍ້ມູນເປັນຮູບແບບມັນແວທີ່ໄດ້ຮັບຄວາມນິຍົມຫຼາຍທີ່ສຸດໃນກິດຈະກຳອາຊະຍາກຳທາງໄຊເບີຕະຫຼອດປີ 2023. ປະລິມານຂໍ້ມູນທີ່ລັກມາເພື່ອຂາຍໃນຕະຫລາດເວັບມືດທີ່ເພີ່ມຂຶ້ນ ແລະ ເພີ່ມຂຶ້ນຂອງກິດຈະກຳນາຍໜ້າການເຂົ້າເຖິງເບື້ອງຕົ້ນທີ່ນຳໃຊ້ຂໍ້ມູນນີ້ແມ່ນສະທ້ອນໃຫ້ເຫັນເຖິງແນວໂນ້ມທີ່ເພີ່ມຂຶ້ນນີ້, ເຊິ່ງໄດ້ເລັ່ງໄປສູ່ປີ 2024.

ລະບົບນິເວດຜູ້ລັກຂໍ້ມູນ

ໄລຍະທີ 1: ຮັບມັນແວ

ໂດຍປົກກະຕິແລ້ວຜູ້ລັກຂໍ້ມູນຖືກສະເໜີໃຫ້ຢູ່ໃນຕະຫຼາດອາດຊະຍາກຳທາງໄຊເບີ, ໃນຮູບແບບ MaaS ຫຼື Stealer-as-a-Service ຫຼື ຂາຍໃນຮູບແບບລະຫັດຕົ້ນສະບັບ. MaaS ໝາຍເຖິງຮູບແບບທຸລະກິດທີ່ຜູ້ພັດທະນາມັນແວທີ່ເປັນອັນຕະລາຍຈະຂາຍການສະໝັກໃຊ້ງານຂອງຊອບແວທີ່ເປັນອັນຕະລາຍໃຫ້ກັບບຸກຄົນຕ່າງໆ ຜ່ານເວທີເວັບໄຊທ໌, ຄ້າຍຄືກັນກັບການສະເໜີຊອບແວທີ່ຖືກຕ້ອງຕາມກົດໝາຍ. ຮູບແບບ MaaS ຊ່ວຍຫຼຸດລົງອຸປະສັກຕໍ່ການເຂົ້າເຖິງສຳລັບຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີ, ເນື່ອງຈາກຮູບແບບນີ້ເປີດໂອກາດໃຫ້ບຸກຄົນທີ່ບໍ່ມີທັກສະດ້ານເທດນິກຢ່າງກວ້າງຂວາງໃນການເຜີຍແຜ່ມັນແວ ແລະ ເກັບກຳຂໍ້ມູນທີ່ຖືກລັກເພື່ອໃຊ້ໃນການໂຈມຕີທາງໄຊເບີໄດ້.

ຜູ້ລັກຂໍ້ມູນທີ່ສະໜອງໃຫ້ເປັນ MaaS ໂດຍທົ່ວໄປແລ້ວ ແມ່ນໂຄສະນາສຳລັບຄ່າທຳນຽມລາຍເດືອນທີ່ຂ້ອນຂ້າງບໍ່ແພງ ແລະ ໃຫ້ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີສາມາດເຂົ້າເຖິງແຜງໜ້າປັດຜູ້ລັກຂໍ້ມູນໄດ້. ແຜງໜ້າປັດຊ່ວຍອຳນວຍຄວາມສະດວກໃນການສ້າງມັນແວໂດຍຂໍ້ມູນ, ຈັດລະບຽບຂໍ້ມູນທີ່ຖືກລັກ ແລະ ຕິດຕາມຈຳນວນຂອງລະບົບທີ່ຖືກບຸກລຸກ. ຜູ້ໃຫ້ບໍລິການ MaaS ນຳສະເໜີການອັບເດດຄຸນສົມບັດ, ເຄື່ອງມື ແລະ ການສະໜັບສະໜູນທາງເທດນິກ ເພື່ອຫຼີກລ່ຽງການຊອກຄົ້ນຫາໂດຍຊອບແວຕ້ານໄວຣັສ ແລະ ເພື່ອດຶງດູດ ແລະ ຮັກສາສະມາຊິກໄວ້. ຜູ້ລັກຂໍ້ມູນຈຳນວນຫຼາຍມີຄວາມສາມາດທີ່ຈະລຶບຕົນເອງອອກຈາກອຸປະກອນຂອງຜູ້ເຄາະຮ້າຍຫຼັງຈາກດຳເນີນການລັກຂໍ້ມູນ.

ໄລຍະທີ 2: ການແຜ່ກະຈາຍ

ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີທີ່ເຜີຍແຜ່ຜູ້ລັກຂໍ້ມູນ ແລະ ເກັບກຳຂໍ້ມູນຈາກອຸປະກອນທີ່ຖືກບຸກລຸກເອີ້ນວ່າ ‘ຜູ້ເຜີຍແຜ່ຂໍ້ມູນ’ (ຜູ້ເຜີຍແຜ່ຂໍ້ມູນ). ຜູ້ລັກລອບສົ່ງເຫຍື່ອໄປຍັງລິ້ງທີ່ເປັນອັນຕະລາຍ, ເຊິ່ງຊ່ວຍໃຫ້ຜູ້ລັກຂໍ້ມູນແຜ່ກະຈາຍໄດ້ ເຊິ່ງເປັນສ່ວນໜຶ່ງຂອງການໂຄສະນາຢ່າງກວ້າງຂວາງ. ການໂຄສະນາສ່ວນໃຫຍ່ແມ່ນບໍ່ເລືອກປະຕິບັດ, ໂດຍອາໄສການສວຍໂອກາດຕິດເຊື້ອ. ແນວໃດກໍ່ຕາມ, ແຄມເປນບາງສ່ວນໄດ້ຮັບການປັບແຕ່ງໃຫ້ເໝາະສົມກັບອຸດສາຫະກຳສະເພາະ ແລະ ກ່ຽວຂ້ອງກັບການຟິດຊິງແບບເຈາະຈົງກັບຜູ້ເຄາະຮ້າຍສະເພາະ. ຜູ້ຊື້ຂາຍດຳເນີນການແຄມເປນທີ່ກົງກັບເປົ້າໝາຍຫຼາຍຂຶ້ນເພື່ອຕອບສະໜອງຄວາມຕ້ອງການຂອງລູກຄ້າ; ຕົວຢ່າງ, ໃນກໍລະນີຜູ້ຊື້ຕ້ອງການເຂົ້າເຖິງອົງກອນ ຫຼື ພາກສ່ວນທີ່ມີມູນຄ່າສູງໂດຍສະເພາະ.

ຜູ້ລັກລອບນຳຂໍ້ມູນໄປໃຊ້ລັກຂໍ້ມູນໃນອຸປະກອນຜູ້ຖືກເຄາະຮ້າຍໂດຍໃຊ້ເຕັກນິກທີ່ຫຼາກຫຼາຍ, ລວມທັງ:

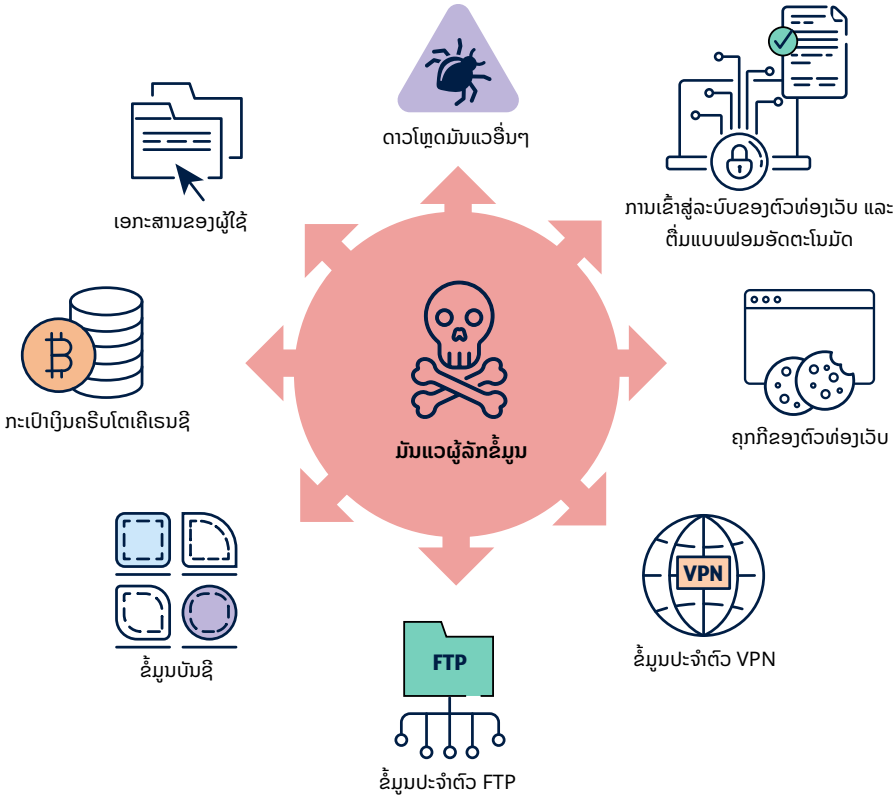
- **ບ້ອດເນັດ**: ເຄືອຂ່າຍຂອງລະບົບຄອມພິວເຕີທີ່ຖືກທຳລາຍທີ່ ຄວບຄຸມໂດຍອາຊະຍາກຳທາງໄຊເບີເພື່ອດຳເນີນການທີ່ເປັນອັນຕະລາຍ, ເຊັ່ນການສົ່ງຂໍ້ຄວາມຟິດຊິງ ຫຼື ມັນແວ

- **ຟິດຊິງ**: ຄວາມພະຍາຍາມທີ່ຈະໄດ້ຮັບຂໍ້ມູນທີ່ລະອຽດອ່ອນໂດຍການຫຼອກລວງ, ລວມທັງຜ່ານທາງອີເມວ ຫຼື ຂໍ້ຄວາມໂດຍກົງໃນສື່ສັງຄົມ, ກະດານສົນທະນາ ແລະ ແອັບສົ່ງຂໍ້ຄວາມ, ເຊິ່ງເປັນວິທີການເຜີຍແຜ່ທົ່ວໄປທີ່ຫຼຸດອຸປະສັກໃນການເຂົ້າເຖິງຂອງອາຊະຍາກຳທາງໄຊເບີ:
  - ໂດຍທົ່ວໄປຂໍ້ຄວາມເຫຼົ່ານີ້ຈະມີລິ້ງທີ່ເປັນອັນຕະລາຍ, ແທນທີ່ຈະແນບໄຟລ໌ທີ່ເປັນອັນຕະລາຍກັບອີເມວນັ້ນເອງ.
- **ຜົນການຄົ້ນຫາທີ່ເປັນອັນຕະລາຍ**: ສົ່ງຜ່ານເຕັກນິກການເພີ່ມປະສິດທິພາບຂອງເຄື່ອງຈັກຊອກຫາ (SEO) ທີ່ມີເປົ້າໝາຍໂດຍກົງໄປຫາເວັບໄຊທ໌ທີ່ໃຫ້ບໍລິການມັນແວທີ່ປອມຕົວເປັນຊອບແວທີ່ຖືກຕ້ອງຕາມກົດໝາຍ ຫຼື ເນື້ອຫາອື່ນໆ
- **ການໂຄສະນາແບບມັນແວ**: ການໃຊ້ລະຫັດທີ່ເປັນອັນຕະລາຍ, ທີ່ແຮກເຂົ້າໄປໃນໂຄສະນາອອນລາຍທີ່ຖືກຕ້ອງຕາມກົດໝາຍ, ເພື່ອເຜີຍແຜ່ມັນແວ
- **ຊອບແວທີ່ຖອນລະຫັດ ຫຼື ລະເມີດລິຂະສິດ**: ການດາວໂຫຼດ, ລວມທັງເກມວິດີໂອ, ແບ່ງປັນຜ່ານວິດີໂອ YouTube, ໂດຍມີລິ້ງທີ່ເປັນອັນຕະລາຍໃນຄຳອະທິບາຍວິດີໂອ ຫຼື ຄຳຄິດເຫັນ ຫຼື ຈາກເວັບໄຊດາວໂຫຼດທີ່ບໍ່ໜ້າເຊື່ອຖື
- **ການໂຄສະນາ ແລະ ໂພສໃນສື່ສັງຄົມອອນລາຍ**: ກຳນົດເປົ້າໝາຍໄປຫາໄຟລ໌ມັນແວທີ່ປອມຕົວ
- **ການອັບເດດຊອບແວທີ່ເປັນອັນຕະລາຍ**: ໂດຍທົ່ວໄປແລ້ວມັດປອມຕົວເປັນການອັບເດດຕົວທ່ອງເວັບ

ໄລຍະທີ 3: ການຂຸດຄົ້ນຂໍ້ມູນ

ເມື່ອຜູ້ລັກຂໍ້ມູນດຳເນີນການໃນອຸປະກອນຂອງຜູ້ເຄາະຮ້າຍ, ມັນຈະເລີ່ມເກັບກຳຂໍ້ມູນທີ່ລະອຽດອ່ອນຈາກເຄື່ອງຈັກທີ່ຖືກບຸກລຸກ. ນອກເໜືອຈາກການລັກເອົາຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້, ໃນກໍລະນີທີ່ຜູ້ລັກຂໍ້ມູນເປັນສ່ວນໜຶ່ງຂອງບັອດເນັດ, ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີສາມາດຄວບຄຸມອຸປະກອນທີ່ຖືກທຳລາຍຈາກໄລຍະໄກໄດ້ໂດຍການສົ່ງຄຳສັ່ງການຕັ້ງຄ່າເພື່ອເປີດໃຊ້ຄວາມສາມາດເພີ່ມເຕີມ ຫຼື ສົ່ງມັນແວອື່ນໆ. ໂດຍທົ່ວໄປ, ຜູ້ລັກຂໍ້ມູນມີສາມາດໃນການລັກໄດ້:

- ຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານ, ໂດຍສະເພາະທີ່ເກັບໄວ້ໃນເຊສຊັນຜູ້ໃຊ້/ໂທເຄັນການກວດສອບສິດທິຫຼາຍປັດໃຈ (MFA) ຂອງຕົວທ່ອງເວັບ
- ຄຸກກີ້ການກວດສອບສິດທິ
- ແບບຟອມການຕື່ມຂໍ້ມູນອັດຕະໂນມັດຕົວທ່ອງເວັບ
- ຂໍ້ມູນອີເມວ, ເນື້ອຫາ ແລະ ລາຍຊື່ຕິດຕໍ່
- ປະຫວັດການທ່ອງເວັບ
- ເອກະສານຜູ້ໃຊ້
- ລາຍລະອຽດບັດເຄຣດິດ
- ບັນທຶກການສົນທະນາຈາກແອັບສົ່ງຂໍ້ຄວາມໃນເດັສທ໊ອບ
- ຂໍ້ມູນລະບົບ
- ກະເປົ໋າເງິນລະຫັດລັບ
- ຂໍ້ມູນປະຈຳຕົວ VPN ຫຼື ອະນຸສັນຍາການໂອນໄຟລ໌ (FTP).



ຮູບທີ 1. ຄວາມສາມາດໃນການລັກຂໍ້ມູນ

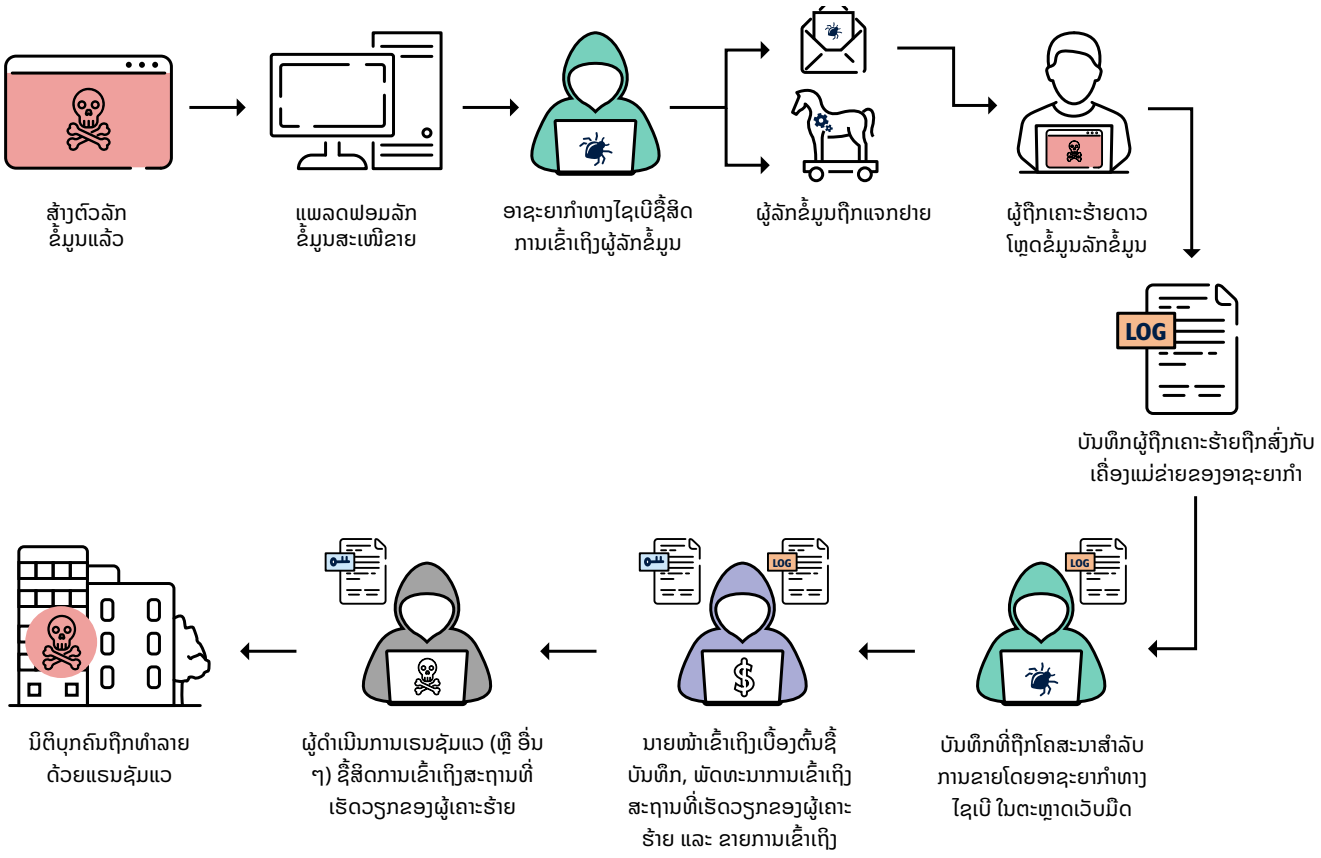
ຄຸກກີການກວດສອບຄວາມຖືກຕ້ອງຂອງຕົວທ່ອງເວັບ ບາງຕົວຊ່ວຍເຮັດໃຫ້ຜູ້ໃຊ້ເຂົ້າສູ່ລະບົບບັນຊີ ຫຼື ການ ບໍລິການເປັນເວລາຫຼາຍວັນໃນແຕ່ລະຄັ້ງ, ດັ່ງນັ້ນຜູ້ໃຊ້ບໍ່ ຈຳເປັນຕ້ອງເຮັດການພິສູດຢືນຢັນຄືນໃໝ່. ຖ້າຖືກລັກ, ຄຸກກີການກວດສອບຄວາມຖືກຕ້ອງເຫຼົ່ານີ້ອາດຫຼີກລ້ຽງ ຂໍ້ກຳນົດຂອງ MFA ໄດ້ຢ່າງມີປະສິດທິພາບ ແລະ ເຮັດໃຫ້ ຜູ້ກໍ່ອາຊະຍາກຳທາງໄຊເບີສາມາດເຂົ້າເຖິງບັນຊີຜູ້ຖືກເຄາະ ຮ້າຍ, ເຄືອຂ່າຍຂອງອົງກອນ ແລະ ລະບົບວິອົງກອນໄດ້.

ຂັ້ນຕອນທີ 4: ການລອບລອມ ຂໍ້ມູນ ແລະ ການສ້າງລາຍໄດ້

ຜູ້ລັກຂໍ້ມູນໄດ້ຮັບການກຳນົດຄ່າໃຫ້ລັກຂໍ້ມູນຂອງຜູ້ເຄາະ ຮ້າຍ, ເອີ້ນວ່າ 'ບັນທຶກ', ໄປຫາເຊີບເວີຄວບຄຸມ ແລະ ສັ່ງການ ທີ່ເປັນອັນຕະລາຍ. ໂດຍທົ່ວໄປແລ້ວ, ຜູ້ລັກຂໍ້ມູນຈະໃຊ້ແອັບ ສົ່ງຂໍ້ຄວາມຍອດນິຍົມ ເຊັ່ນ: Telegram ແລະ Discord, ເພື່ອແບ່ງປັນຂໍ້ມູນບັນທຶກກັບພວກອາດຊະຍາກຳທາງໄຊເບີ.

ຕະຫຼາດພິເສດມີຢູ່ໃນ Telegram ແລະ ທົ່ວເວັບມືດສຳ ລັບການຂາຍ ແລະ ແລກປ່ຽນ. ອາຊະຍາກຳທາງໄຊເບີສ້າງ ລາຍໄດ້ຈາກບັນທຶກຂໍ້ມູນດ້ວຍຫຼາຍວິທີ, ລວມທັງ:

- ການຂາຍບັນທຶກໃນຕະຫຼາດອາຊະຍາກຳ, ລວມທັງໃຫ້ນາຍໜ້າເຂົ້າເຖິງເບື້ອງຕົ້ນ
- ຂູດຮີດຜູ້ຖືກເຄາະຮ້າຍໂດຍກົງ, ຜ່ານການໂຈມ ລະກຳຂໍ້ມູນປະຈຳຕົວ ແລະ ການຂົ່ມເຫັງ
- ນຳໃຊ້ປະໂຫຍດຈາກຂໍ້ມູນສຳລັບການເຂົ້າເຖິງ ເບື້ອງຕົ້ນເຂົ້າໄປໃນເຄືອຂ່າຍຂອງອົງກອນ ເພື່ອດຳເນີນກິດຈະກຳແຮນຊັມແວ.



ຮູບທີ 2. ລະບົບນິເວດຜູ້ລັກຂໍ້ມູນ ແລະ ຜົນກະທົບທີ່ເປັນໄປໄດ້ຕໍ່ອົງກອນ

ຜົນກະທົບ

ຜູ້ລັກຂໍ້ມູນອາດສົ່ງຜົນກະທົບຮ້າຍແຮງຕໍ່ບຸກຄົນ ແລະ ອົງກອນ. ໃນກໍລະນີທີ່ຜູ້ລັກຂໍ້ມູນເກັບກຳຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້, ຜູ້ກໍ່ອາຊະຍາກຳອາດຈະໃຊ້ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ເຫຼົ່ານີ້ ເພື່ອເຂົ້າເຖິງເຄືອຂ່າຍຂອງອົງກອນ ຫຼື ລະບົບອົງກອນທີ່ມີບັນຊີຜູ້ໃຊ້ທີ່ຖືກຕ້ອງ, ເຊິ່ງມັກເຮັດໃຫ້ເຈົ້າຂອງລະບົບກວດພົບຊັກຊ້າ.

ສຳລັບ**ອົງກອນ** ທີ່ໄດ້ຮັບຜົນກະທົບຈາກຜູ້ລັກຂໍ້ມູນ, ຜົນສະທ້ອນອາດຈະປະກອບມີ:

- ແຮນຊັມແວ
- ການລະເມີດຂໍ້ມູນ
- ການບຸກລຸກອີເມວທຸລະກິດ
- ການລັກຊັບສິນທາງປັນຍາ
- ການລັກຂໍ້ມູນທີ່ລະອຽດອ່ອນ.

ສຳລັບ **ບຸກຄົນ** ທີ່ໄດ້ຮັບຜົນກະທົບຈາກຜູ້ລັກຂໍ້ມູນ, ຜົນສະທ້ອນອາດຈະປະກອບມີ:

- ການເຂົ້າເຖິງອີເມວສ່ວນຕົວ ຫຼື ບັນຊີສື່ສັງຄົມທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ
- ຄວາມສ່ຽງທີ່ເພີ່ມຂຶ້ນຂອງການໂຈມລະກຳຂໍ້ມູນສ່ວນບຸກຄົນ
- ຄວາມສ່ຽງຂອງການໂຈມຕີແບບຟິດຊິງທີ່ເພີ່ມຂຶ້ນຟິດຊິງ
- ການສູນເສຍທາງດ້ານການເງິນ ຫຼື ການເຂົ້າເຖິງບັນຊີທາງດ້ານການເງິນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ
- ການສູນເສຍຄວາມເປັນສ່ວນຕົວ.

ກໍລະນີສຶກສາ

ກໍລະນີສຶກສານີ້ໄດ້ຖືກເປີດເຜີຍຊື່ ເພື່ອໃຫ້ສາມາດເຜີຍແຜ່ສູ່ສາທາລະນະໄດ້. ໂດຍອ້າງອີງຈາກເຫດການຄວາມປອດໄພທາງໄຊເບີ ຫຼາຍກໍລະນີທີ່ສົ່ງຜົນກະທົບຕໍ່ໜ່ວຍງານຂອງອອສເຕຣເລຍທີ່ໄດ້ລາຍງານຕໍ່ ACSC ຂອງ ASD. ຕໍ່ໄປນີ້ໜ່ວຍງານທີ່ໄດ້ຮັບຜົນກະທົບແມ່ນເອີ້ນວ່າ 'ອົງກອນ'. ຊື່ຂອງບຸກຄົນໃນກໍລະນີສຶກສານີ້ແມ່ນສົມມຸດຕິຖານ ແລະ ມີການລຶບລາຍລະອຽດອອກໄປເພື່ອປົກປ້ອງຕົວຕົນຂອງຜູ້ຖືກເຄາະຮ້າຍ.

ອົງກອນນີ້ເປັນທຸລະກິດໃນອົດສະຕາລີທີ່ອະນຸຍາດໃຫ້ພະນັກງານສາມາດເຂົ້າເຖິງລະບົບຂອງກອນຈາກອຸປະກອນສ່ວນຕົວ. ອາລິສເປັນພະນັກງານຂອງອົງກອນທີ່ເຮັດວຽກຈາກໄລຍະໄກ.

ເມື່ອເຮັດວຽກຢູ່ບ້ານ, ອາລິສຈະເຂົ້າເຖິງເຄືອຂ່າຍຂອງອົງກອນຂອງນາງຈາກໄລຍະໄກໂດຍໃຊ້ແລັບທັອບສ່ວນຕົວຂອງນາງ. Alice **ດາວໂຫຼດ**, ລົງໃນ **ແລັບທັອບສ່ວນຕົວ**ຂອງນາງ, ເຊິ່ງເປັນເວີຊັນຂອງ Notepad++ (ເຊິ່ງເປັນຊອບແວຈົດບັນທຶກປະເພດໜຶ່ງ) ຈາກເວັບໄຊທ໌ທີ່ນາງເຊື່ອວ່າຖືກຕ້ອງ. **ຜູ້ລັກຂໍ້ມູນ** ປອມຕົວເປັນຜູ້ຕິດຕັ້ງຊອບແວ Notepad++.

ເມື່ອ Alice ພະຍາຍາມຕິດຕັ້ງຊອບແວ, ຕົວລັກຂໍ້ມູນຈະເປີດໃຊ້ງານ ແລະ ເລີ່ມ **ເກັບກ່ຽວຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້** ຈາກແລັບທັອບຂອງນາງ. ນີ້ລວມມີຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານສະຖານທີ່ເຮັດວຽກຂອງນາງ, ເຊິ່ງນາງໄດ້ບັນທຶກໄວ້ໃນຄຸນນະສົມບັດການເຂົ້າສູ່ລະບົບທີ່ບັນທຶກໄວ້ຂອງຕົວທ່ອງເວັບຂອງນາງ. ຫຼັງຈາກນັ້ນ, ຜູ້ລັກຂໍ້ມູນຈະສົ່ງຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ເຫຼົ່ານັ້ນໄປຫາເຄື່ອງແມ່ຂ່າຍຄຳສັ່ງ ແລະ ການຄວບຄຸມໄລຍະໄກທີ່ຄວບຄຸມໂດຍກຸ່ມອາຊະຍາກຳທາງໄຊເບີ.

ບັນທຶກທີ່ຖືກລັກຈະຖືກນຳໄປລວມໄວ້ກັບບັນທຶກອື່ນໆ ແລະ ຈາກນັ້ນ **ຂາຍໃຫ້ພວກອາດຊະຍາກຳທາງໄຊເບີ** ຜ່ານຕະຫຼາດຊື້ຂາຍໃນເວັດມືດ.

ອາຊະຍາກຳທາງໄຊເບີຊື່ບັອບໄດ້ຊື້ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ຂອງ Alice, ທີ່ໃຊ້ລະບຸຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້ສຳລັບການບໍລິການໃນເຄືອຂ່າຍຂອງອົງກອນຂອງນາງ. ອົງກອນຂອງ Alice **ບໍ່ໄດ້ກຳນົດຄ່າ MFA** ສຳລັບການບໍລິການເຫຼົ່ານີ້, ຊຶ່ງໝາຍຄວາມວ່າບັອບ ສາມາດໃຊ້ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ຖືກລັກພຽງຢ່າງດຽວເພື່ອ**ການກວດສອບ ແລະ ເຂົ້າເຖິງ** ເຄືອຂ່າຍຂອງອົງກອນໄດ້ສຳເລັດ.

ບັອບເຂົ້າເຖິງເຄືອຂ່າຍອົງກອນຂອງ Alice ໂດຍບໍ່ໄດ້ກວດພົບໂດຍໃຊ້ **ຂໍ້ມູນປະຈຳຕົວຜູ້ໃຊ້ທີ່ຖືກຕ້ອງ** ທີ່ຖືກລັກໄປ. ບັອບສາມາດປັບປ່ຽນທິດທາງໃນເຄືອຂ່າຍຂອງອົງກອນໄດ້, ໂດຍກຳນົດຂໍ້ມູນທີ່ລະອຽດອ່ອນຂອງອົງກອນ ແລະ ດຶງຂໍ້ມູນນັ້ນອອກມາເພື່ອຮີບໄຖ່ບໍລິສັດ.

ຫຼັງຈາກລັກຂໍ້ມູນທີ່ລະອຽດອ່ອນ, ບັອບ **ກໍ່ໄດ້ເຂົ້າລະຫັດ ຖານຂໍ້ມູນ ແລະ ລະບົບໄຟລ໌** ຂອງອົງກອນເພື່ອເຮັດໃຫ້ພວກເຂົາເຂົ້າບໍ່ໄດ້.

ການຂັ້ນເທິ

ອົງກອນອາດຈະບໍ່ສາມາດບັງຄັບໃຊ້ການຄວບຄຸມອຸປະກອນທີ່ເຊື່ອມຕໍ່ກັບເຄືອຂ່າຍຂອງອົງກອນຂອງເຂົາເຈົ້າ, ໂດຍສະເພາະໃນອຸປະກອນສ່ວນບຸກຄົນທີ່ໃຊ້ໂດຍພະນັກງານທີ່ເຮັດວຽກໄລຍະໄກ. ACSC ຂອງ ASD ແນະນຳໃຫ້ອົງກອນສຸມໃສ່ການປະຕິບັດການຄວບຄຸມເພື່ອປົກປ້ອງຕົນເອງຈາກຄວາມສ່ຽງຂອງຜູ້ລັກຂໍ້ມູນຈະກຳນົດເປົ້າໝາຍລັກຂໍ້ມູນປະຈຳຕົວຂອງຜູ້ໃຊ້. ການຫຼຸດຜ່ອນຜົນກະທົບເຫຼົ່ານີ້ລວມມີ:

ຈັດໃຫ້ມີການຝຶກອົບຮົມຄວາມຮັບຮູ້ດ້ານຄວາມປອດໄພທາງໄຊເບີໃຫ້ແກ່ພະນັກງານ

- ການປ້ອງກັນການໂຈມຕີທາງສັງຄົມແບບກຳນົດເປົ້າໝາຍ ແລະ ການດາວໂຫຼດໄຟລ໌ທີ່ເປັນອັນຕະລາຍໂດຍການຈັດໃຫ້ມີການຝຶກອົບຮົມທີ່ມີປະສິດທິພາບແກ່ພະນັກງານ.
- ສ້າງຄວາມຮັບຮູ້ກ່ຽວກັບຜູ້ລັກຂໍ້ມູນ, ວິທີການຈັດສົ່ງ ແລະ ໄພຂົ່ມຂູ່ຟິດຊິງຕໍ່ກັບອົງກອນຂອງທ່ານ.

ບັນຊີອົງກອນທີ່ປອດໄພ

- ນຳ MFA ໄປໃຊ້:
- ນຳ MFA ໄປໃຊ້ກັບບໍລິການພາຍນອກ ແລະ ພາຍໃນ, ລະບົບ ແລະ ບ່ອນເກັບຂໍ້ມູນທີ່ລະອຽດອ່ອນ, ໂດຍສະເພາະສຳລັບເວັບເມລ, VPNs ແລະ ບັນຊີຜູ້ໃຊ້ສິດທິພິເສດທີ່ເຂົ້າເຖິງລະບົບທີ່ສຳຄັນ. ການປະຕິບັດທີ່ດີທີ່ສຸດແມ່ນຕ້ອງໃຊ້ MFA ທີ່ປ້ອງກັນຟິດຊິງກັບບັນຊີທັງໝົດ.
- ປິດການໃຊ້ງານບັນຊີຜູ້ໃຊ້ເມື່ອພວກເຂົາບໍ່ຈຳເປັນອີກຕໍ່ໄປ.
- ຈຳກັດສິດທິຂອງຜູ້ດູແລລະບົບ:
- ປະຕິບັດການຄຸ້ມຄອງເຄືອຂ່າຍ ແລະ ວຽກງານສິດທິພິເສດອື່ນໆໂດຍໃຊ້ສະຖານີເຮັດວຽກທີ່ຖືກລັອກສະເພາະເທົ່ານັ້ນ (ເຊັ່ນ: ສະຖານີເຮັດວຽກທີ່ປອດໄພ).
- ປະຕິບັດຕາມແນວທາງທີ່ດີທີ່ສຸດສຳລັບສິດທິພິເສດຂັ້ນຕ່ຳໂດຍກຳນົດໃຫ້ຜູ້ດູແລລະບົບໃຊ້ບັນຊີຜູ້ໃຊ້ທີ່ມີສິດທິພິເສດສຳລັບການຄຸ້ມຄອງລະບົບ ແລະ ບັນຊີຜູ້ໃຊ້ມາດຕະຖານສຳລັບວຽກງານທີ່ບໍ່ແມ່ນການດູແລ.
- ການປ້ອງກັນບັນຊີຜູ້ໃຊ້ທີ່ມີສິດທິພິເສດ (ບໍ່ລວມຜູ້ທີ່ໄດ້ຮັບອານຸຍາດຢ່າງຊັດເຈນໃນການເຂົ້າເຖິງບໍລິການອອນລາຍ) ຈາກການເຂົ້າເຖິງອິນເຕີເນັດ, ມີເມວ ແລະ ບໍລິການເວັບ.
- ພິຈາລະນາການນຳການບໍລິການຈັດການແບບທັນເວລາໄປໃຊ້ກັບລະບົບ ແລະ ແອັບພລິເຄຊັ່ນ.
- ບັງຄັບໃຊ້ການຄຸ້ມຄອງ ແລະ ການກວດສອບບັນຊີຜູ້ໃຊ້ທີ່ມີສິດທິພິເສດ.
- ອັບເດດລະຫັດຜ່ານເປັນໄລຍະ, ໂດຍສະເພາະບັນຊີການເຂົ້າເຖິງໄລຍະໄກທີ່ເຜີຍແຜ່ພາຍນອກ.
- ບັງຄັບໃຊ້ການໝົດອາຍຸການໃຊ້ງານ ແລະ ນະໂຍບາຍການຢຸດໃຊ້ງານໃນໂທເຄັນເຊສຊັນ ແລະ ຄຸກກີ້.

ເສີມສ້າງຄວາມຄ່ອງຕົວຂອງອົງກອນ

- ດຳເນີນການປະເມີນຄວາມສ່ຽງຕໍ່ການເຄື່ອນທີ່ຂອງອົງກອນ ແລະ ປະຕິບັດ ຂໍ້ແນະນຳການເສີມຄວາມເຂັ້ມແຂງດ້ານການເຄື່ອນໄຫວຂອງອົງກອນມາໃຊ້.
- ປະຕິບັດນະໂຍບາຍນຳເອົາອຸປະກອນຂອງທ່ານເອງ (BYOD) ຖ້າທ່ານອະນຸຍາດໃຫ້ພະນັກງານໃຊ້ອຸປະກອນສ່ວນຕົວສຳລັບການເຮັດວຽກ, ເນື່ອງຈາກເຄື່ອງມືບໍລິຫານຈັດການໂດຍອົງກອນມີຄວາມປອດໄພຫຼາຍກວ່າເຄື່ອງມືສ່ວນຕົວທີ່ບໍ່ໄດ້ຮັບການຈັດການ.

ກວດສອບ ແລະ ປະເມີນຄວາມສ່ຽງຂອງລະບົບຕ່ອງໂສ້ການສະໜອງຈາກຜູ້ຂາຍທີ່ເຂົ້າເຖິງເຄືອຂ່າຍຂອງທ່ານ, ລວມທັງຜູ້ຈຳໜ່າຍຊອບແວແບບບໍລິການ (Saas) ແລະ ຜູ້ໃຫ້ບໍລິການທີ່ມີການຄຸ້ມຄອງ. ວິທີຈັດການຄວາມປອດໄພຂອງທ່ານເມື່ອມີສ່ວນຮ່ວມກັບຜູ້ໃຫ້ບໍລິການທີ່ມີການຈັດການ.

ປົກປ້ອງເຄືອຂ່າຍອົງກອນຂອງທ່ານ

- ຮັກສາແອັບພລິເຄຊັ່ນ ແລະ ລະບົບປະຕິບັດການໃຫ້ທັນສະໄໝ.
- ນຳໃຊ້ນະໂຍບາຍຄວາມປອດໄພໃນທ້ອງຖິ່ນ ເພື່ອບັງຄັບໃຊ້ການຄວບຄຸມແອັບພລິເຄຊັ່ນດ້ວຍລາຍການອະນຸຍາດທີ່ເຂັ້ມງວດ.
- ດຳເນີນການແບ່ງສ່ວນເຄືອຂ່າຍເພື່ອແຍກພາກສ່ວນເຄືອຂ່າຍໂດຍອີງໃສ່ບົດບາດ ແລະ ໜ້າທີ່.
- ກວດສອບ ແລະ ຕິດຕາມກິດຈະກຳຂອງຜູ້ໃຊ້, ໂດຍສະເພາະສຳລັບພະນັກງານໄລຍະໄກ.
- ການກວດສອບບັນຊີທີ່ມີສິດທິພິເສດສາມາດເປີດເຜີຍການເຂົ້າເຖິງຂໍ້ມູນທີ່ລະອຽດອ່ອນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຫຼື ກິດຈະກຳການໂອນຂໍ້ມູນທີ່ຜິດປົກກະຕິ, ເຊັ່ນ: ຂໍ້ມູນຈຳນວນຫຼາຍທີ່ອັບໂຫຼດໄປຍັງເຄືອຂ່າຍພາຍນອກ.
- ປະຕິບັດຕາມນະໂຍບາຍການປ້ອງກັນການສູນເສຍຂໍ້ມູນ ແລະ ເຄື່ອງມືເພື່ອປ້ອງກັນການໂອນຂໍ້ມູນທີ່ບໍ່ໄດ້ຮັບອະນຸຍາດ.

ກາຍເປັນຄູ່ຮ່ວມມືເຄືອຂ່າຍຄວາມປອດໄພທາງໄຊເບີ ASD ແລະ ເຂົ້າຮ່ວມແບ່ງປັນຂ່າວກອງໄພຄຸກຄາມທາງໄຊເບີ (CTIS) ຂອງ ASD

- CTIS ເປັນແພລະຕະຟອມການແບ່ງປັນສອງທາງທີ່ຊ່ວຍໃຫ້ລັດຖະບານແລະ ຄູ່ຮ່ວມມືອຸດສາຫະກຳໄດ້ຮັບ ແລະ ແບ່ງປັນຂໍ້ມູນກ່ຽວກັບກິດຈະກຳທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ.
- ACSC ຂອງ ASD ກຳລັງຕິດຕາມກິດຈະກຳການລັກຂໍ້ມູນ ແລະ ແບ່ງປັນລາຍລະອຽດຂອງຄຳສັ່ງ ແລະ ໂຄງສ້າງພື້ນຖານການຄວບຄຸມທີ່ມີການເຄື່ອນໄຫວຜ່ານແພລະຕະຟອມ CTIS.
- ລົງທະບຽນເພື່ອກາຍເປັນຄູ່ຮ່ວມມື ແລະ ປົກປ້ອງອົງກອນ ແລະ ຂໍ້ມູນລູກຄ້າຂອງທ່ານຈາກໄພຂົ່ມຂູ່ທາງໄຊເບີ.

ກະກຽມສຳລັບການປະນີປະນອມ

- ພັດທະນາແຜນການຕອບໂຕ້ກັບເຫດການຄວາມປອດໄພທາງໄຊເບີ ເພື່ອໃຊ້ໃນກໍລະນີທີ່ມີການປະນີປະນອມຂອງຜູ້ລັກຂໍ້ມູນ. ໃຫ້ແນ່ໃຈວ່າພະນັກງານຮູ້ສິ່ງທີ່ຕ້ອງເຮັດ ແລະ ຕິດຕໍ່ໃຜຖ້າພວກເຂົາສົງໃສວ່າພວກເຂົາໄດ້ດາວໂຫຼດໄຟລ໌ທີ່ໜ້າສົງໄສ.

ນຳ ACSC's Essential Eight ຂອງ ASD ມາໃຊ້

- ນອກເໜືອຈາກການບັນເທົາທີ່ໄດ້ກ່າວມາຂ້າງເທິງ, ACSC ຂອງ ASD ແນະນຳຢ່າງຍິ່ງໃຫ້ນຳ Essential Eight ສ່ວນທີ່ເຫຼືອຂອງ ACSC ຂອງ ASD ມາໃຊ້.

ຄຳແນະນຳສຳລັບພະນັກງານຂອງທ່ານເມື່ອເຮັດວຽກຈາກໄລຍະໄກ

- ປົກປ້ອງຂໍ້ມູນຂອງທ່ານໃນອຸປະກອນສ່ວນຕົວຂອງທ່ານ
  - ພັດທະນາສຸຂະອະນາໄມທາງໄຊເບີທີ່ດີ ແລະ ຢ່າຄລິກໃສ່ລິ້ງ ຫຼື ປ໊ອບອັບທີ່ໜ້າສົງໄສ ຫຼື ດາວໂຫຼດໄຟລ໌ ຫຼື ຊອບແວຈາກແຫຼ່ງທີ່ບໍ່ຮູ້ຈັກ ຫຼື ທີ່ບໍ່ເຊື່ອຖືໄດ້.
  - ໃຊ້ລະຫັດຜ່ານທີ່ແຕກຕ່າງສຳລັບບັນຊີທີ່ເຮັດວຽກ ແລະ ສ່ວນຕົວ. ໃຊ້ MFA ສຳລັບບັນຊີສ່ວນບຸກຄົນຖ້າເປັນໄປໄດ້.
  - ຢ່າເກັບຂໍ້ມູນປະຈຳຕົວການເຮັດວຽກຂອງທ່ານໄວ້ໃນຕົວຈັດການລະຫັດຜ່ານສ່ວນຕົວ ເວັ້ນເສຍແຕ່ໄດ້ຮັບການອະນຸມັດຈາກນາຍຈ້າງຂອງທ່ານຢ່າງຈະແຈ້ງ. ນີ້ປະກອບມີຕົວຈັດການລະຫັດຜ່ານຂອງຕົວທ່ອງເວັບຂອງທ່ານ. **ຖ້າມີຂໍ້ສົງໄສ, ຂໍໃຫ້ນາຍຈ້າງຂອງທ່ານສະໜອງຕົວຈັດການລະຫັດຜ່ານທີ່ໄດ້ຮັບການສະໜັບສະໜູນຈາກອົງກອນ.**
  - ຢ່າເຂົ້າສູ່ລະບົບບັນຊີບ່ອນເຮັດວຽກຂອງທ່ານຈາກສະຖານີເຮັດວຽກຮ່ວມກັນ ຫຼື ຊຸມຊົນ.
  - ລະວັງສິ່ງທີ່ຖືກເກັບໄວ້ໃນຄຸນສົມບັດການຕື່ມຂໍ້ມູນອັດຕະໂນມັດຂອງຕົວທ່ອງເວັບຂອງທ່ານ. ຜູ້ລັກຂໍ້ມູນມຸ່ງເປົ້າໝາຍໄປທີ່ຂໍ້ມູນທີ່ຕົວທ່ອງເວັບບັນທຶກເພື່ອຕື່ມແບບຟອມອັດຕະໂນມັດ. ເມື່ອຕື່ມແບບຟອມໃນເວັບ, ຄວນພິຈາລະນາການປ້ອນຂໍ້ມູນທີ່ລະອຽດອ່ອນດ້ວຍຕົນເອງ, ເຊັ່ນ: ເລກບັດເຄຣດິດ, ແທນທີ່ຈະບັນທຶກລົງໃນຄຸນສົມບັດການຕື່ມຂໍ້ມູນອັດຕະໂນມັດຂອງຕົວທ່ອງເວັບ.
  - ອອກຈາກລະບົບການບໍລິການອອນລາຍທັງໝົດ ແລະ ລຶບລ້າງຄຸກກີ້ຂອງບຣາວເຊີເວັບ ຫຼັງຈາກສຳເລັດການທ່ອງເວັບເພື່ອຫຼຸດຂໍ້ມູນທີ່ມີໃຫ້ກັບຜູ້ລັກຂໍ້ມູນ.
  - ກວດສອບໃຫ້ແນ່ໃຈວ່າໄດ້ເປີດໃຊ້ງານລະບົບປະຕິບັດການທີ່ສ້າງຂຶ້ນໃນການແກ້ໄຂຕ້ານໄວຣັສໄດ້ຖືກເປີດໃຊ້. ຖ້າທ່ານໃຊ້ການແກ້ໄຂປ້ອງກັນໄວຣັດຂອງບໍລິສັດອື່ນ, ໃຫ້ແນ່ໃຈວ່າມີການອັບເດດຢູ່ສະເໝີ ແລະ ມາຈາກຜູ້ຈຳໜ່າຍທີ່ມີຊື່ສຽງ.

ການຊ່ວຍເຫຼືອ

ອົງກອນຂອງອົດສະຕຣາລີທີ່ໄດ້ຮັບຜົນກະທົບ ຫຼື ຕ້ອງການຄວາມຊ່ວຍເຫຼືອກ່ຽວກັບການໂຈມຕີ ກຳ ຂໍ້ມູນສາມາດຕິດຕໍ່ ACSC ຂອງ ASD ໄດ້ທີ່ **1300 CYBER1** (**1300 292 371**) ຫຼື ໂດຍການສົ່ງບົດລາຍງານຢູ່ທີ່ cyber.gov.au/report.

ACSC ຂອງ ASD ສະໜັບສະໜູນໃຫ້ໜ່ວຍງານຕ່າງໆລາຍງານການເຄື່ອນໄຫວເຄືອຂ່າຍທີ່ໜ້າສົງໄສ ແລະ ຕົວຊີ້ວັດການບຸກລຸກທີ່ກ່ຽວຂ້ອງກັບຜູ້ລັກຂໍ້ມູນ, ເຖິງແມ່ນວ່າເຫດການນັ້ນໄດ້ຮັບການຄວບຄຸມແລ້ວກໍຕາມ. ພວກເຮົາໃຊ້ຂໍ້ມູນທີ່ທ່ານໃຫ້ມາເພື່ອປັບປຸງຄວາມເຂົ້າໃຈຂອງພວກເຮົາກ່ຽວກັບຍຸດທະວິທີ, ເຕັກນິກ ແລະ ຂັ້ນຕອນການຂົ່ມຂູ່ທາງໄຊເບີ, ເຊິ່ງຊ່ວຍໃຫ້ພວກເຮົາສາມາດການເຕືອນໄພແກ່ອົງກອນອື່ນໆ ໃນອົດສະຕຣາລີທີ່ຕົກເປັນເປົ້າໝາຍໃນລັກສະນະດຽວກັນໄດ້.

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

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

ເຄື່ອງຈັກພາບຈະບໍ່ຮັບຜິດຊອບໃດໆ ຕໍ່ຄວາມເສຍຫາຍ, ການສູນເສຍ ຫຼື ຄ່າໃຊ້ຈ່າຍໃດໆທີ່ເກີດຂຶ້ນອັນເປັນຜົນມາຈາກເພິ່ງພາຂໍ້ມູນທີ່ມີຢູ່ໃນຄູ່ມືນີ້.

ຖ້າຕ້ອງການຂໍ້ມູນເພີ່ມເຕີມຫຼືລາຍງານເຫດການຄວາມປອດໄພທາງໄຊເບີ,ໃຫ້ຕິດຕໍ່ພວກເຮົາ:

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

ເບີໂທນີ້ສາມາດໃຊ້ໄດ້ພາຍໃນອອສເຕຣເລັຍເທົ່ານັ້ນ.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre