# ເຄັດລັບ ການນຳໃຊ້ໄວໄຟສາທາລະນະຢ່າງປອດໄພ

## ຄົນບໍ່ດີສາມາດໃຊ້ຜົນປະໂຫຍດຈາກການອອນລາຍຂອງທ່ານ. ອ່ານຂ້າງລຸ່ມ ສຳລັບເຄັດລັບ ເພື່ອພິຈາລະນາ ຖ້າທ່ານຕ້ອງໃຊ້ໄວໄຟສາທາລະນະ.

ເພື່ອຕອບກັບການແຜ່ລະບາດໂຄໂຣນາໄວຣັດ ແລະ ການປິດທຸລະກິດ ແລະ ຫໍສະມຸດ, ຫລາຍທ່ານຂອງພວກເຮົາ ອາດຈະກຳລັງໃຊ້ເວລາສ່ວນຫລາຍອອນລາຍທາງອິນເຕີເນັດ. ດັ່ງນັ້ນ, ພວກເຮົາຕ້ອງໃຊ້ໄວໄຟສາທາລະນະ ເພື່ອເຊື່ອມຕໍ່ອິນເຕີເນັດ. ຖ້າທ່ານພົບວ່າ ຕົວທ່ານເອງຕ້ອງການໃຊ້ໄວໄຟສາທາລະນະ, ກະລຸນາພິຈາລະນາຄຳແນະນຳຕ່າງໆດັ່ງຕໍ່ໄປນີ້ ຈາກຫ້ອງໜ້າຂໍ້ມູນຄວາມລັບແຫ່ງລັດ ເພື່ອຊ່ວຍປົກປ້ອງຂໍ້ມູນທ່ານ:

## 1. ຢືນຢັນວ່າ ທ່ານມີເຄືອຂ່າຍທີ່ຖືກຕ້ອງ.

ຮັບປະກັນວ່າ ທ່ານກຳລັງເຊື່ອມຕໍ່ເຄືອຂ່າຍທີ່ຖືກຕ້ອງ. ຄົນບໍ່ດີອາດຈະສ້າງເຄືອຂ່າຍ ທີ່ເບິ່ງຄືບໍ່ອັນຕະລາຍ ອີງຕາມຊື່ຂອງເຂົາເຈົ້າ ແຕ່ໃນຄວາມຈິງ ຈະນຳທ່ານໃຫ້ເຊື່ອມຕໍ່ກັບລະບົບເຄືອຂ່າຍ ທີ່ເບິ່ງລາຍລະອຽດ ເວລາທ່ານທ່ອງອິນເຕີເນັດ. ນີ້ໝາຍເຖິງ ຖ້າທ່ານໄດ້ເຂົ້າລະບົບໃຊ້ການອ້າງອີງຫລັກຖານ ຫລື ລະຫັດຜ່ານໃນເວັບໄຊ, ຄົນບໍ່ດີຈະສາມາດລັກຂໍ້ມູນຂອງທ່ານໄດ້. ເພື່ອປ້ອງກັນບັນຫານີ້, ອ່ານຊື່ເຄືອຂ່າຍຢ່າງລະອຽດ ແລະ ຖ້າເປັນໄປໄດ້, ຖາມພະນັກງານ ຫລື ກວດເບິ່ງທຸລະກິດ ເພື່ອຮັບປະກັນວ່າ ເຄືອຂ່າຍແມ່ນຖືກຕ້ອງຕາມກົດໝາຍ.

ເຄືອຂ່າຍທີ່ມີຊື່ສຽງ ຄືເຄືອຂ່າຍຂອງຕ່ອງໂສ້ການໂພທີ່ຄຸ້ນເຄີຍ ເບິ່ງຄືວ່າຈະໜ້າສົງໄສໜ້ອຍກວ່າ ເນື່ອງຈາກບໍລິສັດດຳເນີນເຄືອຂ່າຍ ຄືເປັນບໍລິການກັບທຸລະກິດເຂົ້າເຈົ້າ. ເຄືອຂ່າຍທີ່ມີຊື່ສຽງ ແມ່ນໂດຍປົກກະຕິຈະປອດໄພກວ່າ ເຄືອຂ່າຍໄວໄຟສຣິແບບສຸ່ມ ທີ່ງໂທລະສັບຂອງທ່ານ ໃນສະຖານທີ່ສາທາລະນະ.

## 2. ປິດການເຊື່ອມຕໍ່ອັດຕະໂນມັດ.

ຫລາຍອຸປະກອນ (ສະມາດໂຟນ, ແລັບທອບ ແລະ ເທັບເລັດ) ແມ່ນຈະມີການຕັ້ງຄ່າເຊື່ອມຕໍ່ອັດຕະໂນມັດ. ການຕັ້ງຄ່າເຫລົ່ານີ້ ຈະເຮັດໃຫ້ອຸປະກອນຂອງທ່ານ ເຊື່ອມຕໍ່ກັບເຄືອຂ່າຍໃກ້ໆໄດ້ຢ່າງສະດວກສະບາຍ. ນີ້ແມ່ນຈະບໍ່ມີບັນຫາ ກັບເຄືອຂ່າຍທີ່ໄວ້ໃຈໄດ້ ແຕ່ມັນຍັງສາມາດເຊື່ອມອຸປະກອນຂອງທ່ານເຂົ້າກັບເຄືອຂ່າຍທີ່ອາດຈະບໍ່ປອດໄພ. ທ່ານສາມາດປິດຟີດເຈີ້ນີ້ ຜ່ານການຟີດເຈີ້ການຕັ້ງຄ່າ ທ່ຽງໂທລະສັບຂອງທ່ານ. ປິດການຕັ້ງຄ່າເຫລົ່ານີ້, ໂດຍສະເພາະ ເມື່ອທ່ານກຳລັງເດີນທາງໄປສະຖານທີ່ ທີ່ບໍ່ຄຸ້ນເຄີຍ. ຄືເປັນການເຕືອນເພີ່ມເຕີມ, ທ່ານສາມາດກວດເບິ່ງ “forget network” ຫລັງຈາກນຳໃຊ້ໄວໄຟສາທາລະນະ.

ນອກນີ້ ທ່ານຄວນຈະຕິດຕາມ Bluetooth ຂອງທ່ານ ໃນຂະນະທີ່ຢູ່ໃນສະຖານທີ່ສາທາລະນະ. ການເຊື່ອມຕໍ່ Bluetooth ຈະເຮັດໃຫ້ອຸປະກອນຕ່າງໆ ເຊື່ອມເຂົ້າກັນ ແລະ ຄົນບໍ່ດີສາມາດຊອກຫາສັນຍານ Bluetooth ທີ່ເປີດໃຊ້ງານ ເພື່ອເອົາຜົນປະໂຫຍດຈາກໂທລະສັບຂອງທ່ານ. ປິດຟັງຊັ້ນນີ້ ທ່ຽງໂທລະສັບຂອງທ່ານ ແລະ ອຸປະກອນອື່ນໆ ເມື່ອທ່ານຢູ່ໃນສະຖານທີ່ບໍ່ຄຸ້ນເຄີຍ.

# 3. ປິດການແຊໄຟຣ.

ໝັ້ນໃຈວ່າ ຕ້ອງໄດ້ປິດອອບຊັນການແຊໄຟຣ ຂະນະທີ່ຫລິ້ນໄວໄຟສາທາລະນະ. ທ່ານສາມາດປິດການແຊໄຟຣ ຈາກຄວາມຕ້ອງການລະບົບ ຫລື ໜ້າແຜງບັດຄອບຄຸມ ອີງຕາມລະບົບປະຕິບັດການຂອງທ່ານ. AirDrop ແມ່ນຕົວຢ່າງໜຶ່ງຂອງຟີດເຈີ້ການແຊໄວໄຟ ທີ່ທ່ານຈະຕ້ອງໄດ້ມອດ. ບາງລະບົບປະຕິບັດການ ເຊັ່ນ Windows/PC ຈະປິດການແຊໄຟຣ ສຳລັບທ່ານ ໂດຍການເລືອກອອບຊັນ "ສາທາລະນະ" ເມື່ອເຊື່ອມຕໍ່ກັບເຄືອຂ່າຍສາທາລະນະໃໝ່ ເປັນຄັ້ງທຳອິດ.

ຂັ້ນຕອນການປິດແຊໄຟຣ

**ທີ່ໆ PC:**

1. ໄປຫາສູນແຊຂໍ້ມູນ ແລະ ເຄືອຂ່າຍ.
2. ຫລັງຈາກນັ້ນ ປ່ຽນການຕັ້ງຄ່າການແຊຂັ້ນສູງ.
3. ປິດການແຊໄຟຣ ແລະ ເຄື່ອງຖ່າຍເອກະສານ.

**ສຳລັບ Macs**:

1. ໄປຫາ System Preferences.
2. ເລືອກການແຊຂໍ້ມູນ.
3. ບໍ່ເລືອກທຸກຢ່າງ.
4. ຕໍ່ໄປໃນແອັບ Finder, ກົດປຸ່ມ AirDrop ແລະ ເລືອກ ອະນຸຍາດໃຫ້ຂ້ອຍຖືກພົບໂດຍ: ບໍ່ມີໃຜ.

ສຳລັບ iOS, ພຽງແຕ່ຊອກຫາແອັບ AirDrop ໃນສູນຄອບຄຸມ ແລະ ປິດແອັບ.

# 4. ໃຊ້ VPN.

ພິຈາລະນາການຕິດຕັ້ງ VPN (ເຄືອຂ່າຍສ່ວນຕົວສະເໝືອນຈິງ) ເທິ່ງອຸປະກອນຂອງທ່ານ. VPN ແມ່ນທາງເລືອກປອດໄພທີ່ສຸດ ສຳລັບຄວາມເປັນສ່ວນຕົວທາງດິຈິຕອນ ເທິ່ງໄວໄຟສາທາລະນະ. ມັນຈະເຂົ້າລະຫັດຂໍ້ມູນຂອງທ່ານ ຕາມທີ່ໄດ້ຜ່ານອຸປະກອນຂອງທ່ານ ແລະ ເຮັດຮດວຽກຄືເປັນ "ຊ່ອງທາງ" ປ້ອງກັນ ເພື່ອວ່າ ຈະບໍ່ສາມາດເບິ່ງເຫັນຂໍ້ມູນຂອງທ່ານ ໃນຂະນະທີ່ມັນຜ່ານລະບົບເຄືອຂ່າຍ.

# 5. FBI ແຈ້ງເຕືອນກ່ຽວກັບເວັບໄຊເຂົ້າລະຫັດ – HTTPS.

FBI ໄດ້ແຈ້ງເຕືອນ ກ່ຽວກັບເວັບໄຊ ຕາມທີ່ຢູ່ ທີ່ເລີ່ມດ້ວຍ "https." ຕົວອັກສອນ "https" ແລະ ໂອຄອນລ່ອກ ແມ່ນເບິ່ງຄືວ່າຈະແດງໃຫ້ເຫັນການເຄື່ອນໄຫວຂອງເວັບ ທີ່ຖືກເຂົ້າລະຫັດ ແລະ ຜູ້ຢ້ຽມຢາມ ສາມາດແບ່ງປັນຂໍ້ມູນໄດ້ຢ່າງປອດໄພ. ແນວໃດກໍ່ຕາມ, ອະສົຍະກຳທາງໄຊເບີ້ ຕອນນີ້ ກຳລັງລວບລວມຄວາມເຊື່ອໃຈຂອງສາທາລະນະ ໂດຍການລອກລ້ຽນເຂົ້າໄປໃນເວັບໄຊອັນຕະລາຍ ທີ່ຂຶ້ນຕົ້ນດ້ວຍ https ແລະ ປະກົດວ່າປອດໄພ ເມື່ອຕົວຈິງບໍ່ແມ່ນແນວນັ້ນ.

ຄຳແນະນຳຂອງ FBI:

- ບໍ່ຕ້ອງເຊື່ອຊື່ໃນອີເມວ: ຖາມຈຸດປະສົງຂອງເນື້ອໃນອີເມວ.
- ຖ້າທ່ານຮັບອີເມວທີ່ໜ້າສົງໄສ ດ້ວຍວິ້ງ ຈາກການຕິດຕໍ່, ຢັ້ງຢືນຂໍ້ຄວາມ ແມ່ນຖືກຕ້ອງໂດຍການໂທ ຫລື ອີເມວຫາການຕິດຕໍ່ນັ້ນ. ບໍ່ຕ້ອງຕອບອີເມວທີ່ໜ້າສົງໄສໂດຍກົງ.
- ກວດເບິ່ງຄຳຜິດ ຫລື ໂດເມັ້ນທີ່ຜິດ ພາຍໃນວິ້ງ (ເຊັ່ນ: ຖ້າທີ່ຢູ່ວົງທ້າຍດ້ວຍ ".gov" ວົງທ້າຍໃນ ".com" ແທນ).
- ຫ້າມເຊື່ອເວັບໄຊ ພຽງແຕ່ເນື່ອງຈາກມັນມີໄອຄອນລ໋ອກ ຫລື "https" ໃນແຖບທີ່ຢູ່ບາວເຊີ້.

# 6. ບໍ່ແນະນຳເຂົ້າຫາຂໍ້ມູນທີ່ລະອຽດອ່ອນ.

ແມ້ແຕ່ ຖ້າທ່ານມີ VPN ຍັງບໍ່ແນະນຳໃຫ້ ເຂົ້າຫາບັນຊີທະນາຄານສ່ວນຕົວ ຫລື ຂໍ້ມູນສ່ວນຕົວທີ່ລະອຽດອ່ອນຄ້າຍຄືກັນນີ້ ຄືເລກປະກັນໄພທາງສັງຄົມ ເທິ່ງເຄືອຂ່າຍສາທາລະນະທີ່ບໍ່ປອດໄພ. ແມ້ແຕ່ ເຄືອຂ່າຍທີ່ປອດໄພສາທາລະນະ ຍັງມີຄວາມສ່ຽງ. ໃຊ້ການຕັດສິນໃຈທີ່ດີສຸດຂອງທ່ານ ຖ້າທ່ານຕ້ອງໄດ້ເຂົ້າເຖິງບັນຊີເຫລົ່ານີ້ ເທິ່ງໄວໄຟສາທາລະນະ. ສຳລັບການເຄື່ອນໄຫວທາງການເງິນ, ມັນອາດຈະດີກວ່າ ທີ່ຈະໃຊ້ຟັງຊັນຮອດສະປອດຂອງສະມາດໂຟນຂອງທ່ານແທນ.

# 7. ປອດໄພ vs. ບໍ່ປອດໄພ.

ມີສອງປະເພດພື້ນຖານຂອງເຄືອຂ່າຍໄວໄຟສາທາລະນະ: ປອດໄພ ແລະ ບໍ່ປອດໄພ.

ເມື່ອໃດກໍ່ຕາມ ທີ່ເຊື່ອມຕໍ່ກັບເຄືອຂ່າຍສາທາລະນະທີ່ປອດໄພ. ເຄືອຂ່າຍທີ່ບໍ່ປອດໄພ ສາມາດເຊື່ອມເຂົ້າກັນ ໂດຍບໍ່ມີປະເພດຟີດເຈີ້ຄວາມປອດໄພ ຄືກັບລະຫັດຜ່ານ ຫລື ການເຂົ້າລະບົບ. ເຄືອຂ່າຍປອດໄພ ໂດຍທົ່ວໄປ ຕ້ອງການຜູ້ໃຊ້ຫັນດີກັບຂໍ້ກຳນົດ ແລະ ເງື່ອນໄຂ, ຂັ້ນທະບຽນບັນຊີ ຫລື ພິມລະຫັກຜ່ານ ກ່ອນເຊື່ອມຕໍ່ເຄືອຂ່າຍ.

# 8. ເປີດໃຊ້ລະບົບໄຟຂອນຂອງທ່ານ.

ຖ້າທ່ານກຳລັງໃຊ້ແລັບທອບ, ເປີດໃຊ້ໄຟຂອນ ຂະນທີ່ຢູ່ເທິ່ງໄວໄຟສາທາລະນະ. ໄຟຂອນ ຈະເຮັດວຽກຄືເປັນກຳແພງ ປ້ອງກັນອຸປະກອນທ່ານ ຈາກການຄຸມຂູ່ຂອງ malware. ຜູ້ໃຊ້ອາດຈະປິດໄຟຂອນ Windows ເນື່ອງຈາກການປອບອັບ ແລະ ການແຈ້ງເຕືອນ ແລະ ຫລັງຈາກນັ້ນ ລືມກ່ຽວກັບມັນ. ຖ້າທ່ານຕ້ອງການປິດເປີດໂປແກຼມໃໝ່ເທິ່ງ PC, ຈາກນັ້ນໄປຫາແຜງໂຄນໂທ, "ລະບົບ ແລະ ຄວາມປອດໄພ" ແລະ ເລືອກ "Windows Firewall". ຖ້າທ່ານແມ່ນຜູ້ໃຊ້ Mac, ໄປຫາ "ການຕັ້ງຄ່າລະບົບ", ຫລັງຈາກນັ້ນ "ຄວາມປອດໄພ & ຄວາມເປັນສ່ວນຕົວ", ຈາກນັ້ນແຖບ "ໄຟວໍ" ເພື່ອເປີດໃຊ້ຟີດເຈີ້ນີ້.

# 9. ໃຊ້ຊອບແວແອນຕີ້ໄວຣັສ.

ຮັບປະກັນ ການຕິດຕັ້ງໂປແກຼມແອນຕີ້ໄວຣັສເວີຊັນລ້າສຸດ ເທິ່ງແລັບທອບຂອງທ່ານ. ໂປແກຼມແອນຕີ້ໄວຣັສ ສາມາດຊ່ວຍປ້ອງກັນທ່ານ ຂະນະທີ່ນຳໃຊ້ໄວໄຟສາທາລະນະ ໂດຍການກວດເບິ່ງ malware ທີ່ອາດຈະເຂົ້າໄປໃນລະບົບຂອງທ່ານ ຂະນະນຳໃຊ້ເຄືອຂ່າຍແບ່ງປັນຂໍ້ມູນ. ຈະມີການແຈ້ງເຕືອນທ່ານ ຖ້າໄວຣັສໄດ້ຖືກຖ່າຍໂອນເຂົ້າໃນອຸປະກອນຂອງທ່ານ ຫລື ຖ້າມີການເຄື່ອນໄຫວທີ່ໜ້າສົງໄສ, ຈູໂຈມ ຫລື ຖ້າມີ malware ເຂົ້າໄປໃນລະບົບຂອງທ່ານ.

# 10. ໃຊ້ການກວດສອບສອງປັດໃຈ ຫລື ຫລາຍປັດໃຈ.

ໃຊ້ການກວດສອບຫລາຍປັດໃຈ (MFA) ເມື່ອເຂົ້າເວັບໄຊ ດ້ວຍຂໍ້ມູນສ່ວນຕົວຂອງທ່ານ. ນີ້ໝາຍເຖິງ ທ່ານມີລະຫັດ ຢັ້ງຢືນຄວາມຖືກຕ້ອງທີສອງ (ສິ່ງຂໍ້ຄວາມຫາໂທລະສັບຂອງທ່ານ ຫລື ມາຈາກແອັບ ຫລື ກຸນແຈ) ເຊິ່ງຈະຊ່ວຍປ້ອງ ກັນທ່ານເພີ່ມ. ສະນັ້ນ ແມ້ແຕ່ ຖ້າຄົນບໍ່ດີ ໄດ້ຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານຂອງທ່ານ, ເຂົາເຈົ້າບໍ່ສາມາດເຂົ້າເຖິງບັນຊີຂອງທ່ານ ໂດຍບໍ່ມີລະຫັດຢັ້ງຢືນຄວາມຖືກຕ້ອງ.

# 11. ຕິດຕາມອຸປະກອນສ່ວນຕົວຂອງທ່ານ.

ຫ້າມ ປ່ອຍແລັບທອບ, ເທັບເລັດ ຫລື ສະມາດໂຟນຂອງທ່ານ ໂດຍບໍ່ຕັ້ງໃຈ ໃນສະຖານທີ່ສາທາລະນະ ຫລື ຍານພາຫະນະ. ແມ້ແຕ່ຖ້າທ່ານມີຄວາມລະມັດລະວັງ ເທິ່ງເຄືອຂ່າຍໄວໄຟ ທີ່ຈະບໍ່ຢຸດໃຜຜູ້ໜຶ່ງ ຈາກການເອົາຊັບສິນຂອງທ່ານ ຫລື ລັກເບິ່ງຂໍ້ມູນຂອງທ່ານ. ເອົາໃຈໃສ່ສິ່ງແວດລ້ອມອ້ອມຂ້າງຂອງທ່ານ ແລະ ສົນໃຈສິ່ງເຫລົ່ານັ້ນ ຢູ່ອ້ອມຕົວທ່ານ.

# 12. ເຄັດລັບຄວາມປອດໄພອອນລາຍອື່ນໆ.

ທີ່ນີ້ແມ່ນສອງສາມເຄັກລັບ ໃນການຢູ່ເທິ່ງອອນລາຍແບບປອດໄພ ໂດຍສະເພາະ ຖ້າທ່ານກຳລັງໃຊ້ການເ ຊື່ອມຕໍ່ໄວໄຟສາທາລະນະ.

- ໃຊ້ລະຫັດຜ່ານທີ່ເຂັ້ມແຂງ.
- ເຂົ້າລະຫັດອຸປະກອນຂອງທ່ານ.
- ລະວັງອີເມວຫລອກລວງ.
- ລະມັດລະວັງກັບສິ່ງທີ່ທ່ານໄດ້ໂພສຢູ່ເທິ່ງສື່ສັງຄົມອອນລາຍ. ລາຍລະອຽດສ່ວນຕົວຫລາຍເກີນໄປ ສາມາດຊ່ວຍໃຫ້ຄົນບໍ່ດີເດົາລະຫັດຜ່ານໄດ້.
- ລຶບຂໍ້ມູນເກົ່າ ທີ່ທ່ານບໍ່ຕ້ອງການອີກຕໍ່ໄປ.
- ຖ້າເຄືອຂ່າຍຖາມທ່ານ ໃຫ້ຕິດຕັ້ງຊອບແວເພີ່ມເຕີມໃດໜຶ່ງ ຫລື ການຂະຫຍາຍບາວເຊີ ບໍ່ເຊື່ອມຕໍ່.
- ຮັບປະກັນ ລະບົບ ແລະ ການອັບເດດຊອບແວລ້າສຸດ ໃຫ້ຖືກຕິດຕັ້ງຢູ່ໃນອຸປະກອນຂອງທ່ານ ເພື່ອປ້ອງກັນບັນຫາຕ່າງໆ.