ໃຫ້ທຶນໂດຍ
ສະຫະພາບ ເອີຣົບ

Lao Journalists Association

ການນຳໃຊ້ສື່ອອນລາຍ ແບບປອດໄພ

ນຳສະເໜີໂດຍ: ແສງທອງ ໄຊຍະວົງ

ວາລະການຮຽນຮູ້ (Agenda)

ພາກທີ 1: ຄວາມສຳຄັນຂອງຄວາມປອດໄພໄຊເບີ

ພາກທີ 2 ໄພອັນຕະລາຍໃນໂລກອອນລາຍ

ພາກທີ 3: ກົດເຫຼັກ ແລະ ການປ້ອງກັນຕົນເອງ

ພາກທີ 4: ການສັງເກດເວັບໄຊປອດໄພ (HTTPS)

ພາກທີ 5: ຄວາມເປັນສ່ວນຕົວໃນ Social Media

ພາກທີ 6: ການແກ້ໄຂບັນຫາເມື່ອຖືກແຮັກ

Q&A: ແລກປ່ຽນ-ສົນທະນາ

ພາກທີ 1: ຄວາມສຳຄັນຂອງຄວາມປອດໄພໄຊເບີ

ຄວາມປອດໄພໄຊເບີ (Cybersecurity) ແມ່ນຫຍັງ?

ແມ່ນການປົກປ້ອງລະບົບ, ເຄືອຂ່າຍ, ຄອມພິວເຕີ, ອຸປະກອນມືຖື, ໂປຣແກຣມ ແລະ ຂໍ້ມູນຕ່າງໆ ໃຫ້ປອດໄພຈາກການໂຈມຕີ, ການເຂົ້າເຖິງໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ, ການທຳລາຍ ຫຼື ການປ່ຽນແປງທາງດິຈິຕອນ.

ສະຖິຕິໄພຄຸກຄາມທາງໄຊເບີທົ່ວໂລກ

95%

ຂອງບັນຫາເກີດຈາກ Human Error

ຄວາມອ່ອນແອທີ່ສຸດຄືມະນຸດ

95% ຂອງການໂຈມຕີທາງໄຊເບີທີ່ປະສົບ ຜົນສຳເລັດແມ່ນມີສາເຫດມາຈາກຄວາມຜິດພາດ ຂອງບຸກຄົນ ເຊັ່ນ: ການກົດລິ້ງຫຼອກລວງ ຫຼື ຕັ້ງ ລະຫັດຜ່ານທີ່ເດົາງ່າຍ.

ການສ້າງຈິດສຳນຶກ ແລະ ຄວາມຮູ້ທີ່ຖືກຕ້ອງຈຶ່ງເປັນ ເກາະປ້ອງກັນທີ່ດີທີ່ສຸດ.

ເປັນຫຍັງພວກເຮົາຕ້ອງປ້ອງກັນຕົນເອງ?

ປົກປ້ອງຂໍ້ມູນສ່ວນຕົວ: ຂໍ້ມູນບັດປະຊາຊົນ, ເບີໂທລະສັບ, ແລະ ທີ່ຢູ່, ຫາກຮົ່ວໄຫຼອາດຖືກນຳໄປໃຊ້ໃນທາງທີ່ຜິດກົດໝາຍ.

ປ້ອງກັນການສູນເສຍຊັບສິນ: ບັນຊີທະນາຄານ ແລະ ແອັບການເງິນແມ່ນເປົ້າໝາຍຫຼັກຂອງແຮັກເກີ.

ຮັກສາຊື່ສຽງ ແລະ ຄວາມໜ້າເຊື່ອຖື: ການຖືກແຮັກບັນຊີ Facebook ຫຼື ອີເມວ ອາດເຮັດໃຫ້ເສຍຊື່ສຽງ ແລະ ສົ່ງຜົນກະທົບຕໍ່ຄົນອ້ອມຂ້າງ.

ຜົນກະທົບຕໍ່ຊີວິດປະຈຳວັນ

ຜົນກະທົບທາງກົງ

ການສູນເສຍເງິນໃນບັນຊີ, ຂໍ້ມູນສຳຄັນໃນ
ຄອມພິວເຕີຖືກລຶບ ຫຼື ຖືກລັອກເພື່ອຮຽກ
ຄ່າໄຖ່ (Ransomware) ເຮັດໃຫ້ວຽກງານ
ຢຸດສະງັກ.

ຜົນກະທົບທາງອ້ອມ

ຄວາມຕຶງຄຽດທາງຈິດໃຈ, ການສູນເສຍ
ຄວາມເຊື່ອໝັ້ນຈາກໝູ່ເພື່ອນ ແລະ ຄູ່ຄ້າ,
ລວມເຖິງປະຫວັດອາຊະຍາກຳທາງເທັກໂນໂລ
ຊີທີ່ແກ້ໄຂໄດ້ຍາກ.

ພາກທີ 2: ໄພອັນຕະລາຍໃນໂລກອອນລາຍ

ໝວດໝູ່ໄພອັນຕະລາຍໃນໂລກອອນລາຍ

1. ໄພທາງດ້ານການຕົ້ມຕຸ່ນ ແລະ ການເງິນ (Scams & Financial Fraud)

- **ແກ້ງຄໍເຊັນເຕີ (Call Center Scams):** ການໂທມາແອບອ້າງເປັນເຈົ້າໜ້າທີ່ລັດ, ຕຳຫຼວດ ຫຼື ບໍລິສັດຂົນສົ່ງ ເພື່ອສ້າງຄວາມຕົກໃຈ, ຂົ່ມຂູ່ ຫຼື ຫຼອກໃຫ້ໂອນເງິນ.
- **Phishing:** ການສົ່ງອີເມວ ຫຼື ຂໍ້ຄວາມ SMS ປອມ ທີ່ມີລິງແນບມາ ນຳພາໄປສູ່ເວັບໄຊປອມທີ່ຮຽນແບບທະນາຄານ ຫຼື ໂຊຊຽວມີເດຍ ເພື່ອດັກ ຂະໂມຍລະຫັດຜ່ານ.
- **ການຫຼອກລົງທຶນ (Investment Scams):** ການຊັກຊວນໃຫ້ຮ່ວມ ທຶນໃນແອັບພລິເຄຊັນ ຫຼື ເວັບໄຊຕ່າງໆ ໂດຍອ້າງວ່າຈະໄດ້ຜົນຕອບແທນສູງ ເກີນຈິງໃນໄລຍະເວລາສັ້ນໆ.

ໝວດໝູ່ໄພອັນຕະລາຍໃນໂລກອອນລາຍ(ຕໍ່)

2. ໄພທາງດ້ານເຕັກນິກ ແລະ ຄວາມເປັນສ່ວນຕົວ (Technical & Privacy Threats)

- **Ransomware (ເມົາແວຮຽກຄ່າໄຖ່)):** ໄວຣັສຊະນິດໜຶ່ງທີ່ເຂົ້າມາລັອກໄຟລ์ຂໍ້ມູນທັງໝົດໃນລະບົບຄອມພິວເຕີ ເຮັດໃຫ້ບໍ່ສາມາດໃຊ้ງານໄດ้ ຈົນກວ่າຈะยอมจ่ายเงินค่าไถ่ให้กับแฮักเกิ.
- **Identity Theft (ການປອມແປງຕົວຕົນ):** ການທີ่ຜู้บ่ำหวังดีมาเอ้าฮูบพาบ, ชื่ ແລะ ข้ ມูนส่วนตัวที่ร่ั่วไห฼ ไปส้างบันชีปอม ເพื่ອไปห฼อกลวงถ์นอื่น ฼ื ใช้ไมทางที่ผิดกัด ฆาย.
- **SQL Injection / Web Attacks:** ການທີ่แฮักเกิเจาะเข้าละบับถามข้มูนของเวับไซ ผ่านช่องโหว่ของโถด เพื่อลักเอ้าข้มูนผู้ใช้งาน.

ໝວດໝູ່ໄພອັນຕະລາຍໃນໂລກອອນລາຍ(ຕໍ່)

3. ໄພທາງສັງຄົມ ແລະ ຜົນກະທົບຕໍ່ຈິດໃຈ (Social & Psychological Threats)

- **Cyberbullying (ການກັ່ນແກ້ງທາງອອນລາຍ):** ການໃຊ້ສື່ສັງຄົມອອນລາຍໃນການໂຈມຕີ, ໃສ່ຮ້າຍ, ປະຈານ ຫຼື ບິດເບືອນຄວາມຈິງ ເຮັດໃຫ້ຜູ້ອື່ນເສຍຊື່ສຽງ ແລະ ເກີດຄວາມກົດດັນທາງຈິດໃຈ.
- **Fake News (ຂ່າວປອມ):** ການສ້າງ ແລະ ເຜີຍແຜ່ຂໍ້ມູນທີ່ບໍ່ມີຄວາມຈິງ ເພື່ອສ້າງຄວາມປັ່ນປ່ວນ ຫຼື ຫວັງຜົນປະໂຫຍດທາງການເມືອງ/ທຸລະກິດ.

ພາກທີ 3: ກົດເຫຼັກ ແລະ ການປ້ອງກັນຕົນເອງ

3 ສິ່ງທີ່ຕ້ອງເຮັດ (Do's)

ອັບເດດຊອບແວ

ໝັ່ນອັບເດດລະບົບປະຕິບັດ ການ (OS) ແລະ ແອັບພລິເຄ ເຊີນໃຫ້ເປັນເວີເຊີນຫຼ້າສຸດສະ ເໝີ ເພື່ອປິດຊ່ອງໂຫວ່ຄວາມ ປອດໄພ.

ໃຊ້ແອນຕີໄວຣັສ

ຕິດຕັ້ງ ແລະ ໃຊ້ງານໂປຣ ແກຣມປ້ອງກັນໄວຣັສທີ່ມີຊື່ ສຽງ ແລະ ໜ້າເຊື່ອຖື ເພື່ອ ສະແກນຫາຟາຍ ອັນຕະລາຍ.

ສຳຮອງຂໍ້ມູນ

ເຮັດການສຳຮອງຂໍ້ມູນ (Backup) ທີ່ສຳຄັນໄວ້ໃນ External Drive ຫຼື Cloud Storage ທີ່ປອດ ໄພເປັນປະຈຳ.

3 ສິ່ງທີ່ຫ້າມເຮັດ (Don'ts)

ຢ່າຄລິກລິ້ງແປກປອມ

ຫ້າມກົດລິ້ງ ຫຼື **ດາວໂຫຼດ ຟາຍແນບຈາກອີເມວ** ຫຼື **SMS** ທີ່ສົ່ງມາຈາກຄົນທີ່ ທ່ານບໍ່ຮູ້ຈັກຢ່າງເດັດຂາດ.

ຢ່າໃຊ້ Wi-Fi ສາທາລະນະ

ຫຼີກເວັ້ນການເຮັດທຸລະກຳ ທາງການເງິນ ຫຼື ລັອກອິນ ເຂົ້າບັນຊີສຳຄັນ ຜ່ານ Wi-Fi ສາທາລະນະທີ່ບໍ່ມີລະຫັດ ຜ່ານ.

ຢ່າແບ່ງປັນຂໍ້ມູນ ສ່ວນຕົວ

ຢ່າໂພສຮູບພາບປີ້ຍົນ, ບັດ ປະຊາຊົນ, ເບີໂທລະສັບ ຫຼື ຂໍ້ມູນລະອຽດອ່ອນອື່ນໆ ລົງໃນສື່ສັງຄົມອອນລາຍ.

ການສ້າງລະຫັດຜ່ານ (Password) ທີ່ປອດໄພ

- **ຄວາມຍາວເໝາະສົມ:** ຄວນມີຄວາມຍາວຢ່າງໜ້ອຍ 12 ຕົວອັກສອນຂຶ້ນໄປ.
- **ປະສົມປະສານຕົວອັກສອນ:** ປະກອບດ້ວຍ ຕົວອັກສອນໃຫຍ່ (A-Z), ຕົວອັກສອນນ້ອຍ (a-z), ຕົວເລກ (0-9) ແລະ ສັນຍະລັກພິເສດ ເຊັ່ນ: @, #, $, %.
- **ຫຼີກເວັ້ນຂໍ້ມູນສ່ວນຕົວ:** ຫ້າມໃຊ້ວັນເດືອນປີເກີດ, ເບີໂທລະສັບ, ຫຼື ຊື່ຕົວເອງ ຊື່ພໍ່ແມ່ ເພາະເດົາໄດ້ງ່າຍ.
- **ຫ້າມໃຊ້ລະຫັດຊ້ຳ:** ຫ້າມໃຊ້ລະຫັດຜ່ານດຽວກັນໃນທຸກໆເວັບໄຊ.

ການນຳໃຊ້ Password Manager

Password Manager ຄືຫຍັງ?

ຄືເຄື່ອງມື ຫຼື ແອັບພລິເຄເຊີນທີ່ຊ່ວຍສ້າງ ລະຫັດຜ່ານທີ່ຍາກ ແລະ ຊັບຊ້ອນ ພ້ອມທັງ ເກັບຮັກສາລະຫັດຜ່ານທັງໝົດຂອງທ່ານໄວ້ ໃນລະບົບເຂົ້າລະຫັດທີ່ປອດໄພ.

ປະໂຫຍດຫຼັກ

ທ່ານບໍ່ຈຳເປັນຕ້ອງຈື່ລະຫັດຜ່ານຫຼາຍສິບ ບັນຊີອີກຕໍ່ໄປ, ຈື່ພຽງແຕ່ "Master Password" ດຽວເພື່ອກວດສອບ ແລະ ໃຊ້ງານລະຫັດຜ່ານອື່ນໆ ໄດ້ຢ່າງສະດວກ.

ພາກທີ 4 ການສັງເກດເວັບໄຊປອດໄພ

ວິທີການສັງເກດເວັບໄຊແທ້ ແລະ ເວັບໄຊປອມທີ່ຫຼອກລວງຂໍ້ມູນ

ຄວາມແຕກຕ່າງລະຫວ່າງ HTTP ແລະ HTTPS

ຄຸນລັກສະນະ	HTTP (ບໍ່ປອດໄພ)	HTTPS (ປອດໄພ)
ການສົ່ງຂໍ້ມູນ	ສົ່ງເປັນຂໍ້ຄວາມທຳມະດາ (Plain Text)	ມີການເຂົ້າລະຫັດຂໍ້ມູນ (Encrypted)
ຄວາມປອດໄພ	ອາດຖືກດັກຈັບຂໍ້ມູນໄດ້ງ່າຍ	ປ້ອງກັນການດັກຈັບຂໍ້ມູນລະຫວ່າງທາງ
ຮູບສັນຍະລັກ	ບໍ່ມີຮູບກະແຈ (ຂຶ້ນເຕືອນ Not Secure)	ມີຮູບກະແຈລັອກສີຂຽວ ຫຼື ສີເທົາ
ການນຳໃຊ້	ເວັບໄຊອ່ານຂໍ້ມູນທົ່ວໄປ	ເວັບໄຊການເງິນ, ທຸລະກຳ ແລະ ໂຊຊຽວມີເດຍ


Not secure
testwebsite.com


https://www.netban2k.com
Your connection is not Secure
https://www.netbanks.cc
Secure Connection
1,600 × 840

ວິທີກວດສອບລິ້ງແປກປອມ

- **ກວດສອບຕົວສະກົດ URL:** ແຮັກເກີມັກໃຊ້ຊື່ທີ່ຄ້າຍຄືກັນ ເຊັ່ນ: g00gle.com ແທນທີ່ຈະເປັນ google.com.
- **ໃຊ້ວິທີ Hover ເບິ່ງລິ້ງ:** ເອົາເມົາສໄປຊີ້ໃສ່ລິ້ງ (ໂດຍບໍ່ຕ້ອງກົດ) ເພື່ອເບິ່ງວ່າປາຍທາງແທ້ຈິງແມ່ນຫຍັງ.
- **ໃຊ້ເວັບໄຊກວດສອບ:** ນຳເອົາ URL ໄປກວດສອບຜ່ານເວັບໄຊ ເຊັ່ນ **virustotal.com** ເພື່ອຫາໄວຣັສ ແລະ ມັນແວ.

ตาตะลางสะຫຼຸบ: ไพຄุกถาม vs ວິທີป้ องกัน

ปะเพดไพคุกถาม	แมวทางการป้องกัน และ รับมือ
Phishing / ลิงปอม	ห้ามคลิกลิงแปกปะหลาด และ กวดสอบ URL (โดเมม) ของเวับไซให้ละอียดก่อมป้อมละหัดสะเหมี.
แก้งคอเซ้มเต	ตั้งสะติ, บ่ให้ข้มูมส่วมต็ว หื ข้มูมทางการเงิมทางโทละสับ และ วางสาย เพื่อโทกวดสอบกับหม่วยงามโดยก็ง.
Ransomware / เม็าแอ	อับเดดละบ็บปะติบัดการ (OS) ให้เป็มเวิเซิ่มหล้าสุด และ สำรองข้มูม (Backup) ไว้ใม Cloud หื External Hard Drive สะเหมี.
การถืกแร็กบัมชิ	ตั้งละหัดผ่ามให้ถาดเดิยาก

ພາກທີ5 ຄວາມເປັນສ່ວນຕົວໃນສື່ສັງຄົມ

ການຕັ້ງຄ່າ ແລະ ປົກປ້ອງຄວາມເປັນສ່ວນຕົວໃນ Facebook, TikTok, Instagram

ການຕັ້ງຄ່າຄວາມເປັນສ່ວນຕົວ (Privacy Settings)

ຈຳກັດຜູ້ເຂົ້າເຖິງ

ຕັ້ງຄ່າໃຫ້ສະເພາະ "ໝູ່ເພື່ອນ (Friends)" ເທົ່ານັ້ນທີ່ສາມາດເຫັນໂພສ ຫຼື ຂໍ້ມູນສ່ວນຕົວຂອງທ່ານ ຫຼີກເວັ້ນການຕັ້ງເປັນ "ສາທາລະນະ (Public)".

ການຄວບຄຸມການແທັກ

ເປີດໃຊ້ງານລະບົບກວດສອບໂພສ (Profile Review) ກ່ອນທີ່ຮູບພາບ ຫຼື ໂພສທີ່ໝູ່ເພື່ອນແທັກມາ ຈະປະກົດເທິງໜ້າໂປຣຟາຍຂອງທ່ານ.

ພາກທີ6 ການຈັດການກັບບັນຫາເມື່ອເກີດຂຶ້ນ

ຂັ້ນຕອນການປະຕິບັດຕົວຈິງເມື່ອທ່ານ ຫຼື ບັນຊີຂອງທ່ານຖືກແຮັກ

1. ຕັດການເຊື່ອມຕໍ່

ຕັດອິນເຕີເນັດ ຫຼື Wi-Fi ທັນທີ ຫາກສົງໄສວ່າ ຄອມພິວເຕີຕິດເມົ່າແວ.

2. ປ່ຽນລະຫັດຜ່ານ

ທຳການປ່ຽນລະຫັດຜ່ານຂອງບັນຊີ ທັງໝົດ ໂດຍເລີ່ມຈາກອີເມວຫຼັກ.

3. ກວດສອບບັນຊີ

ກວດເບິ່ງການເຄື່ອນໄຫວທາງ ການເງິນ ແລະ ອຸປະກອນທີ່ ກຳລັງລັອກອິນ.

4. ແຈ້ງເຕືອນຄົນອ້ອມຂ້າງ

ໂພສແຈ້ງເຕືອນໝູ່ເພື່ອນວ່າບັນຊີຂອງທ່ານ ຖືກແຮັກ ເພື່ອບໍ່ໃຫ້ຖືກຫຼອກລວງຕໍ່.

ຂັ້ນຕອນການປະຕິບັດເມື່ອ ບັນຊີ Facebook ຖືກແຮັກ

1. ແຈ້ງ Facebook ຜ່ານໜ້າ "ບັນຊີຖືກບຸກລຸກ"

ເຂົ້າໄປທີ່: **facebook.com/hacked** **ເພື່ອແຈ້ງ Facebook**

2. ກູ້ຄືນບັນຊີ (ຖ້າແຮັກເກີ້ປ່ຽນລະຫັດຜ່ານ)

ຖ້າລະຫັດຜ່ານຖືກປ່ຽນແລ້ວ ແລະ ທ່ານບໍ່ສາມາດເຂົ້າໄດ້:

ໃຊ້ຟັງເຊັ່ນ **"ລືມລະຫັດຜ່ານ" (Forgot Password)** ໃນໜ້າເຂົ້າສູ່ລະບົບ

3. ແຈ້ງເຕືອນຄົນໃກ້ຊິດ

ບອກໝູ່ເພື່ອນ ຫຼື ຄອບຄົວຜ່ານຊ່ອງທາງອື່ນ (ເຊັ່ນ: WhatsApp, ຫຼື ໂທຫາ) ວ່າ ບັນຊີ Facebook ຂອງທ່ານຖືກແຮັກ.

ຂັ້ນຕອນການປະຕິບັດເມື່ອ ບັນຊີ Facebook ຖືກແຮັກ

4. ກວດສອບຄວາມປອດໄພຂອງອີເມວ ແລະ ແອັບອື່ນໆ

ຖ້າທ່ານໃຊ້ລະຫັດຜ່ານດຽວກັນກັບອີເມວ ຫຼື ເວັບໄຊອື່ນ, ໃຫ້ **ປ່ຽນລະຫັດຜ່ານທັນທີ.**

5. ເມື່ອເຂົ້າບັນຊີຄືນໄດ້ແລ້ວ

ເມື່ອທ່ານສາມາດເຂົ້າບັນຊີໄດ້ແລ້ວ ໃຫ້ດຳເນີນການດັ່ງນີ້ທັນທີ:

- ປ່ຽນລະຫັດຜ່ານ: ໃຊ້ລະຫັດທີ່ຍາກ ແລະ ບໍ່ຊ້ຳກັບບ່ອນອື່ນ.
- ເປີດໃຊ້ງານການຢືນຢັນຕົວຕົນ 2 ຊັ້ນ (Two-Factor Authentication - 2FA):

ການແຈ້ງເຫດ ແລະ ແຈ້ງຄວາມໄພໄຊເບີ

ເກັບກຳຫຼັກຖານ

ຖ່າຍຮູບໜ້າຈໍ (Screenshot) ຂໍ້ຄວາມຫຼອກລວງ, ຫຼັກຖານການໂອນເງິນ, URL ເວັບໄຊປອມ ແລະ ເບີໂທລະສັບຂອງມິດສາຊີບໄວ້ທັງໝົດ.

ແຈ້ງໜ່ວຍງານທີ່ກ່ຽວຂ້ອງ

ຕິດຕໍ່ທະນາຄານຂອງທ່ານທັນທີເພື່ອລະງັບບັນຊີ, ແລະ ເຂົ້າແຈ້ງຄວາມກັບເຈົ້າໜ້າທີ່ຕຳຫຼວດພະແນກຕ້ານອາຊະຍາກຳທາງເທັກໂນໂລຊີ.

ໂທລະສັບສາຍດ່ວນ:: 1533

ກົມຄວາມປອດໄພໄຊເບີ (Department of Cybersecurity - LaoCERT)

ໃຫ້ທຶນໂດຍ
ສະຫະພາບ ເອີຣົບ

Lao Journalists Association

ຂອບໃຈ