Souphanouvong University Journal of Multidisciplinary Research anddevelopment
2025, Vol. 11, Special Issue, 58-66
https://doi.org/10.69692/SUJMRD11Special58

A Study of Digital Literacy Knowledge and Understanding Among Personnel within the Communications Department, Ministry of Public Security

Phaythoon KEOPHASOUK*[1], Xaythavy Louangvilay[2]

Department of Computer Engineering and Information Technology, Faculty of Engineering, National University of Laos, Lao PDR

***Correspondence:** Department of Computer Engineering and Information Technology, Faculty of Engineering, National University of Laos, Lao PDR. Tel: +856 20 2099336376,*
E-mail: Phaythoon68@gmail.com

Article Info:

Submitted: November 20, 2025
Revised: December 10, 2025
Accepted: December 18, 2025

Abstract

Digital technology is evolving rapidly, and the transformation toward organizations that utilize digital systems to support operational processes has become both a goal and a challenge for the Government of the Lao PDR. In alignment with this national policy, the Communications Department of the Ministry of Public Security has adopted a direction that emphasizes digital transformation. To successfully achieve this goal, personnel within the department must be adequately prepared to use digital systems. This research aims to study the level of digital literacy among employees of the Communications Department of the Ministry of Public Security. The study focuses on three objectives: (1) to examine behavior in using digital technology, (2) to assess skills in using digital technology, and (3) to analyze awareness of risks and cyber-attacks. The research employed a qualitative approach using questionnaires as the data collection instrument. The sample group consisted of 212 employees, including 59 women, representing 27.83% of the sample. Statistical techniques, including mean ($\bar{x}$) and standard deviation (SD), were used to analyze and present the data.

The results regarding digital technology usage behavior revealed that Facebook is the most commonly used social media platform. Communication is primarily conducted via WhatsApp, including file transfers. Flash drives are commonly used for transferring large data files, while MS Word is the most frequently used tool for document management. Google Drive is the preferred cloud storage platform. Employees regularly use computers for more than 30 minutes per session and frequently utilize artificial intelligence tools in their work.

Keywords: Digital, Digital Literacy, Digital Transformation, Cyber Security, Cyber Attacks

1. ພາກສະໜໍ

ການພັດທະນາຢ່າງໄວວາຂອງເຕັກໂນໂລຊີດິຈິຕອນໄດ້ສ້າງຄວາມຕ້ອງການໃໝ່ຢ່າງບໍ່ເຄີຍມີມາກ່ອນ ຕໍ່ຄວາມສາມາດດ້ານດິຈິຕອນຂອງບຸກຄະລາກອນພາກລັດ ໂດຍສະເພາະໃນຂະແໜງການທີ່ມີຄວາມອ່ອນໄຫວສູງເຊັ່ນ ການບັງຄັບໃຊ້ກົດໝາຍ ແລະ ຄວາມປອດໄພສາທາລະນະ (Gil-García et al., 2018; Bertot et al., 2016). ກະຊວງປ້ອງການຄວາມສະຫງົບ ໃນຖານະເປັນໜ່ວຍງານຫຼັກທີ່ຮັບຜິດຊອບຕໍ່ການຮັກສາຄວາມສະຫງົບສຸກຂອງປະຊາຊົນ ແລະ ຄວາມເປັນລະບຽບຮ້ອຍຂອງສັງຄົມ ຈຳເປັນຕ້ອງຮັບປະກັນໃຫ້ບຸກຄະລາກອນໂດຍສະເພາະກົມສື່ສານຕ້ອງມີຄວາມຮູ້ ແລະ ຄວາມເຂົ້າໃຈດ້ານດິຈິຕອນຢ່າງເໝາະສົມ ເພື່ອຮອງຮັບກັບຄວາມທ້າທາຍໃນຍຸກສະໄໝໃໝ່. ຄວາມຮູ້ທາງດ້ານດິຈິຕອນ (Digital Literacy) ຖືກນິຍາມວ່າເປັນຄວາມສາມາດໃນການໃຊ້ເຕັກໂນໂລຊີສານສື່ສານເພື່ອຄົ້ນຫາ, ປະເມີນ, ສ້າງສັນ ແລະ ສື່ສານຂໍ້ມູນຢ່າງມີປະສິດທິພາບ (Shopova, 2014; Carretero et al., 2017). ສຳລັບພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ຄວາມຮູ້ດ້ານດິຈິຕອນບໍ່ພຽງແຕ່ໝາຍເຖິງທັກສະພື້ນຖານທາງເທັກນິກເທົ່ານັ້ນ ແຕ່ຍັງຄອບຄຸມໄປເຖິງຄວາມສາມາດທີ່ສຳຄັນອື່ນໆ ເຊັ່ນ ຄວາມຕະໜັກຮູ້ດ້ານຄວາມປອດໄພທາງໄຊເບີ, ການບໍລິຫານເນື້ອຫາດິຈິຕອນ, ການໃຊ້ສື່ສັງຄົມ

ຢ່າງຮັບຜິດຊອບ ແລະ ການປົກປ້ອງຄວາມລັບ ແລະ ຂໍ້ມູນສ່ວນບຸກຄົນ (Janssen & van den Hoven, 2015; Van Dijk, 2020).

ໃນຫຼາຍໆປະເທດ, ພາລະບົດບາດຂອງກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບສຸກ ມີໜ້າທີ່ເປັນຈຸດເຊື່ອມໂຍງລະຫວ່າງອົງການກັບສາທາລະນະ ໂດຍຄວບຄຸມຊ່ອງທາງການສື່ສານ, ຕອບກັບຄຳຖາມຈາກປະຊາຊົນ, ເຜີຍແຜ່ຂໍ້ມູນສຳຄັນໃນຍາມສຸກເສີນ ແລະ ຮັກສາພາບລັກຂອງອົງກອນໃນພື້ນທີ່ດິຈິຕອນຫຼາຍແພລັດຟອມ (Mergel, 2013; Criado et al., 2013). ຄວາມສາມາດດ້ານດິຈິຕອນຂອງພວກເຂົາ ສົ່ງຜົນໂດຍກົງຕໍ່ປະສິດທິຜົນຂອງການປະຕິບັດພາລະກິດ, ຄວາມເຊື່ອໝັ້ນຂອງສາທາລະນະ, ແລະ ການຮັບມືກັບຄວາມທ້າທາຍດ້ານຄວາມປອດໄພທີ່ເຄື່ອນຍ້າຍເຂົ້າສູ່ພື້ນທີ່ດິຈິຕອນຫຼາຍຂຶ້ນ (Mossberger et al., 2013).

ເຖິງແມ່ນວ່າຄວາມສຳຄັນຂອງຄວາມຮູ້ດ້ານດິຈິຕອນໄດ້ຖືກຮັບຮູ້ຢ່າງກວ້າງຂວາງ ແຕ່ຍັງມີຊ່ອງວ່າງຢ່າງຊັດເຈນໃນການເຂົ້າໃຈລະດັບຄວາມຮູ້ ແລະ ຄວາມສາມາດຕົວຈິງຂອງບຸກຄະລາກອນ (Rodríguez-Bolívar, 2017; Norris, 2016). ການຫັນເປັນດິຈິຕອນໃນວຽກງານດ້ານຄວາມປອດໄພສາທາລະນະ ໄດ້ເພີ່ມຕົວຂຶ້ນຢ່າງໄວວາຢ່າງເຫັນໄດ້ຊັດເຈນ (Brown & Korff, 2009; Wirtz et al., 2019). ແພລັດຟອມສື່ສັງຄົມໄດ້ກາຍເປັນຊ່ອງທາງຫຼັກໃນການສື່ສານໃນຍາມສຸກເສີນ ແລະ ການປະສານກັບປະຊາຊົນ, ຊຶ່ງຕ້ອງການໃຫ້ບຸກຄະລາກອນຝ່າຍສື່ສານ ມີຄວາມຊຳນານໃນການໃຊ້ຟັງຊັນສະເພາະຂອງແພລັດຟອມ ແລະ ກົນລະຍຸດການຜະລິດເນື້ອຫາ. ການແຜ່ກະຈາຍຂອງຂ່າວປອມ ແລະ ຂໍ້ມູນບິດເບືອນ ກາຍເປັນອຸປະສັກທີ່ຮ້າຍແຮງ ເຊິ່ງຕ້ອງອາໄສທັກສະໃນການກວດສອບຂໍ້ມູນຢ່າງວ່ອງໄວ ແລະ ຖືກຕ້ອງ (Wardle & Derakhshan, 2017; Lewandowsky et al., 2012). ມິຕິດ້ານຄວາມປອດໄພທາງໄຊເບີ ເປັນອີກທັກສະແກ່ຄວາມຕ້ອງການຄວາມຮູ້ດ້ານດິຈິຕອນ. ພະນັກງານກົມສື່ສານ ຈຳເປັນຕ້ອງເຂົ້າໃຈຫຼັກການຄວາມປອດໄພທາງໄຊເບີພື້ນຖານ, ສາມາດຈຳແນກໄພຄຸກຄາມທີ່ອາດເກີດຂຶ້ນ, ແລະ ປົກປ້ອງຂໍ້ມູນອັນລະອຽດອ່ອນຂອງອົງກອນ (Sasse et al., 2001; Anderson & Moore, 2006). ນອກຈາກນັ້ນ ການນຳເອົາເຕັກໂນໂລຊີໃໝ່ໆ ເຊັ່ນ ປັນຍາປະດິດ (AI) ແລະ ການວິເຄາະຂໍ້ມູນຂະໜາດໃຫຍ່ (Big Data) ໄດ້ສ້າງຄວາມທ້າທາຍໃໝ່ຕໍ່ການພັດທະນາຄວາມຮູ້ດ້ານດິຈິຕອນ, ຊຶ່ງຕ້ອງການໃຫ້ບຸກຄະລາກອນພາຍໃນກົມສື່ສານ ມີຄວາມເຂົ້າໃຈພື້ນຖານກ່ຽວກັບການເຮັດວຽກຂອງເທັກໂນໂລຊີເຫຼົ່ານັ້ນ ແລະ ຜົນກະທົບທາງຈັນຍາບັນ.

ເຫັນໄດ້ຄວາມສຳຄັນດັ່ງກ່າວບົດຄົ້ນຄວ້ານີ້ຈຶ່ງໄດ້ແນ່ໃສ “ສຶກສາຄວາມຮູ້ຄວາມເຂົ້າໃຈໃນການນຳໃຊ້ເທັກໂນໂລຊີດິຈິຕອນ(Digital Literacy) ຂອງນາຍ ແລະ ພົນຕຳຫຼວດຂອງກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ” ໂດຍມີຈຸດ ປະສົງຄື:

1) ເພື່ອສຶກສາພຶດຕິກຳການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ

2) ເພື່ອສຶກສາທັກສະການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ

3) ເພື່ອສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ

2. ວິທີການຄົ້ນຄວ້າ

ໃນການຄົ້ນຄວ້າໃນຄັ້ງນີ້ ທີມງານພວກເຮົາໄດ້ນຳໃຊ້ການຄົ້ນຄວ້າແບບຄຸນນະພາບໂດຍການສ້າງແບບສອບຖາມ ເຊິ່ງມີຈຳນວນກຸ່ມຕົວຢ່າງຈຳນວນ 212 ເປັນຍິງ 59 ຄົນ ເທົ່າກັບ 27.83%. ລະດັບຄວາມເຊື່ອໝັ້ນ 95% ນຳໃຊ້ ຈາກຂໍ້ມູນທີ່ຕ້ອງການສຳຫຼວດຜູ້ຄົ້ນຄວ້າໄດ້ສ້າງແບບສອບຖາມໂດຍໄດ້ມີການປຶກສາ ແລະ ກວດ ແກ້ຈາກຜູ້ຊ່ຽວຊານທີ່ຢູ່ໃນຂົງເຂດກຳລັງປ້ອງກັນຄວາມສະຫງົບ ແລະ ຜູ້ຊ່ຽວຊານຈາກ ຄະນະວິສະວະກຳສາດ, ມະຫາວິທະຍາໄລແຫ່ງຊາດ, ແບບສອບຖາມໃນບົດຄົ້ນຄວ້ານີ້ປະກອບມີ IV ພາກດັ່ງນີ້:

1) ພາກທີ I ຂໍ້ມູນທົ່ວໄປຂອງກຸ່ມຕົວຢ່າງເຊິ່ງປະກອບມີ: ເພດ, ອາຍຸ, ວຸທິການສຶກສາ, ຊັ້ນຕຳແໜ່ງ ແລະ ອື່ນໆ

2) ພາກທີ II ພຶດຕິກຳການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ເຊັ່ນ ສາມາດນຳໃຊ້ AI, ສາມາດສ້າງເນື້ອຫາດິຈິຕອນ, ແລະ ອື່ນໆ

3) ພາກທີ III ທັກສະການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນເຊັ່ນ: ສາມາດນຳໃຊ້ AI, ສາມາດສ້າງເນື້ອຫາດິຈິຕອນ, ສາ ມາດນຳໃຊ້ google Sheets, ສາມາດນຳໃຊ້ MS Offices, ສາມາດສ້າວການ/ເຊື່ອມຕໍ່ Hotspot/Bluetooth ແລະ ອື່ນໆ

4) ພາກທີ IV ການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ ປະກອບມີບັນດາຄຳຖາມເຊັ່ນ: ການຕັ້ງລະຫັດຜ່ານທີ່ປອດໄພ ແລະ ການຮັກສາຂໍ້ມູນສ່ວນຕົວ, ການປ່ຽນລະຫັດຜ່ານຂອງຂ້ອຍເປັນປະຈຳ, ການຮູ້ເທົ່າທັນ Call center ແລະ ອື່ນໆ

ແບບສອບຖາມທີ່ສ້າງຂຶ້ນໄດ້ຜ່ານຜູ້ຊ່ຽວຊານ ແລະ ອົງການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງກໍ່ຄືກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ເພື່ອກວດສອບຄວາມເໝາະສົມທາງດ້ານເນື້ອຫາເພື່ອຮັບປະກັນໃຫ້ໄດ້ຂໍ້ມູນຄົບຖ້ວນຕາມທີ່ໄດ້ກຳນົດໄວ້ສະນັ້ນເມື່ອແບບສອບຖາມບໍ່ຄົບຖ້ວນ ຫຼື ມີການດັດແກ້ຈຶ່ງມີຄຳເຫັນຂອງຜູ້ຊ່ຽວຊານ 3 ທ່ານ.

ຈຸດປະສົ່ງທີ 2 ແລະ 3 ແມ່ນເປັນແບບສອບຖາມເປັນແບບຄຳຖາມປາຍປິດ ດ້ວຍວິທີການວັດລະດັບຂອງ (Likert Scale) ເຊິ່ງແບ່ງລະດັບການວັດ ແລະ ເກນການໃຫ້ຄະແນນອອກເປັນ 5 ລະດັບຕັ້ງແຕ່ຄະແນນໜ້ອຍສຸດຄື 1 ແລະ ສູງ ສຸດຄື 5 ຕາມລຳດັບດັ່ງນີ້:

ຫຼາຍທີ່ສຸດ	=	5	ຄະແນະ
ຫຼາຍ	=	4	ຄະແນະ
ປານກາງ	=	3	ຄະແນະ
ໜ້ອຍ	=	2	ຄະແນະ
ໜ້ອຍທີ່ສຸດ	=	1	ຄະແນະ

ນອກຈາກນັ້ນຜູ້ຄົ້ນຄວ້າຍັງໄດ້ກຳນົດເກນຂອງຄ່າສະເລ່ຍໄວ້ 5 ລະດັບຕາມລຳດັບຊັ້ນ (class interval) ເຊິ່ງສາມາດຄຳນວນຫາຄວາມກວ້າງຂອງແຕ່ລະຊັ້ນໄວ້ດັ່ງນີ້:

ຄວາມກວ້າງຂອງຊັ້ນ = (ຄະແນນສູງສຸດ - ຄະແນນຕ່ຳສຸດ)/ ຈຳນວນຊັ້ນ *(1)*

= (5-1)/5

= 0.80

ຜູ້ຄົ້ນຄວ້າໄດ້ກຳນົດຄວາມໝາຍຂອງຄ່າສະເລ່ຍໄວ້ດັ່ງນີ້

ຄະແນນລະຫວ່າງ	4.20 - 5.00	ໝາຍເຖິງ	ຫຼາຍທີ່ສຸດ
ຄະແນນລະຫວ່າງ	3.40 – 4.19	ໝາຍເຖິງ	ຫຼາຍ
ຄະແນນລະຫວ່າງ	2.60 - 3.39	ໝາຍເຖິງ	ປານກາງ
ຄະແນນລະຫວ່າງ	1.80 – 2.59	ໝາຍເຖິງ	ໜ້ອຍ
ຄະແນນລະຫວ່າງ	1.00 - 1.79	ໝາຍເຖິງ	ໜ້ອຍທີ່ສຸດ

ການຫາຄ່າສະເລ່ຍຂອງຄວາມເຫັນດີມີດັ່ງນີ້%:

$$\overline{X} = \frac{n1x1 + n2x2 + n3x3 + n4x4 + n5x5}{n}$$

(2)

$\overline{X}$ ໝາຍເຖິງຄວາມສະເລ່ຍຂອງຄວາມເພິ່ງພໍໃຈ

n1-n5 ໝາຍເຖິງຈຳນວນກຸ່ມຕົວຢ່າງທີ່ເລືອກຄວາມເພິ່ງພໍໃຈໃນແຕ່ລະລະດັບ

1-5 ໝາຍເຖິງຄະແນນແຕ່ລະລະດັບ

n ໝາຍເຖິງກຸ່ມຕົວຢ່າງທັງໝົດ

ແລະ ຄ່າບ່ຽງແບນ ມາດຕະຖານ (Standard Derivation: SD) ດັ່ງໃນສົມຜົນທີ (3) ດັ່ງລຸ່ມນີ້:

$$D = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2} \quad (3)$$

SD ຄ່າບ່ຽງແບນ ມາດຕະຖານ

x_i ໝາຍເຖິງຈຳນວນກຸ່ມຕົວຢ່າງທີ່ເລືອກຄວາມເພິ່ງພໃຈໃນແຕ່ລະລະດັບ

$\overline{x}$ ໝາຍຄ່າສະເລ່ຍ

n ໝາຍເຖິງກຸ່ມຕົວຢ່າງທັງໝົດ

ໃນການຄົ້ນຄວ້າໃນຄັ້ງນີ້ ໄດ້ໃຊ້ໂປຣແກຣມວິເຄາະທາງສະຖິຕິ ຄືໂປຣແກຣມ SPSS(Statistical Package for the Social Sciences) ເຊິ່ງເປັນໂປຣແກຣມທີ່ມີປະສິດທິພາບສູງໃນການວິເຄາະຂໍ້ມູນທາງສະຖິຕິ ແລະ ສະແດງຜົນການວິເຄາະຂໍ້ມູນດ້ວຍຮູບແບບຕາຕະລ່າງ ຫຼື ເສັ້ນສະແດງປະເພດຕ່າງໆໄດ້ບໍ່ວ່າຈະເປັນແບບ 1 ມິຕິ 2 ມິຕິ ແລະ 3 ມິຕິ(1D, 2D and 3D). ນອກຈາກນີ້ ຜູ້ຄົ້ນຄວ້າຍັງໃຊ້ໂປຣແກຣມ Microsoft Excel ເກັບກຳແລະ ໃນການຮວບຮ່ວມຂໍ້ມູນຕື່ມອີກ.

3. ຜົນໄດ້ຮັບ

ຜົນໄດ້ຮັບຂອງການຄົ້ນຄວ້າຕາມແຕ່ລະຈຸດປະສົງດັ່ງນີ້:

1) ເພື່ອສຶກສາພຶດຕິກຳການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຂອງ ພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະ ຫງົບ ຜົນການທົດລອງໄດ້ຊີ້ໃຫ້ເຫັນວ່າ ພະນັກງານກົມສື່ສານນິຍົມໃຊ້ social media ແມ່ນ facebook ກວມເອົາ 80% ແລະ x(twitter) 20%, ການຕິດຕໍ່ສື່ສານ ແມ່ນນຳໃຊ້ WhatsApp ກວາມເອົາ 82.20% ຮອງລົງມາ ແມ່ນ ນຳໃຊ້ facebook ກວາມເອົາ 11.10% Instagram ແລະ ອື່ນໆ ຕາມລຳດັບ, ສຳຫຼັບການໂອນຍ້າຍຂໍ້ມູນໃຫຍ່ ຈະນຳໃຊ້ USB(Flat Drive) ກວາມເອົາ 44.40% ນຳໃຊ້ Hard Drive 26.70% ນຳໃຊ້ ຕົວອື່ນໆ ແລະ Cloud ຕາມລຳດັບ, ການນຳໃຊ້ການເກັບຂໍ້ມູນແບບອອນລາຍ(Cloud Storage) ແມ່ນນຳໃຊ້ Google Drive ກວາມເອົາ 64.40% ນຳໃຊ້ Microsoft 17.80% ນຳໃຊ້ ແພລດຟອມອື່ນໆ ແລະ Apple ຕາມລຳດັບ, ສຳຫຼັບວຽກງານເອກກະສານແມ່ນນຳໃຊ້ MS Word ກວາມເອົາ 68.90% ອື່ນໆ 17.8% MS Excel 11.10% ນອກນັ້ນແມ່ນ MS PowerPoint. ຄວາມຖີ່ຂອງການນຳໃຊ້ ຄອມພິວເຕີ ແມ່ນຍຳໃຊ້ທຸກໆວັນ ກວາມເອົາ 73.30% 3-4ຄັ້ງ/ອາທິດ ກວາມເອົາ 13.30% 1-2 ຄັ້ງ/ອາທິດ ແລະ ອື່ນໆ ຕາມລຳດັບ, ໃນການນຳໃຊ້ແຕ່ລະຄັ້ງແມ່ນ ຫຼາຍກວ່າ 30 ນາທີ ກວາມເອົາ 80.00%, ສຳຫຼັບ ການນຳໃຊ້ AI ແມ່ນນຳໃຊ້ ChatGPT ກວາມເອົາ 44.40% ອື່ນໆ 28.90% Gemini 20.00% ຕາມລຳດັບ. ສຳຫຼັບການນຳໃຊ້ AI ແມ່ນ ມີຈຸດປະສົງຄື ຫາຂໍ້ມູນ 62.20% ໃຊ້ເພື່ອອື່ນໆ 24.40% ຕາມລຳດັບ ດັ່ງສະແດງໃນຮູບທີ 1

2) ຈາກຜົນຂອງການຄົ້ນຄວ້າ ທີມຄົ້ນຄວ້າຂອງພວກເຮົາເຫັນໄດ້ວ່າ ຄວາມສາມາດ ຫຼື ທັກສະຂອງການນຳໃຊ້ເຕັກໂນໂລຊີດິຕອນເຫັນວ່າ ພະນັກງານພາຍໃນກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ໄດ້ນຳໃຊ້ ເປັນປະຈຳ ເຊິ່ງມັນໄດ້ສະແດງໃຫ້ເຫັນຄື: ຄວາມສາມາດໃນການສ້າງ/ເຊື່ອມຕໍ່ Bluetooth/Hotspot ມີຜູ້ຕອບ ລະດັບ 5 ຫຼາຍທີ່ສຸດ ຢູ່ທີ 108 ຄົນ ກວາມເອົາ 51.16% $\overline{X}$ =4.23 SD=43.90 ຢູ່ໃນລະດັບດີຫຼາຍ, ການນຳໃຊ້ Computer ເພື່ອປະຕິບັດວຽກເຫັນວ່າຜູ້ຕອບແບບສອບຖາມເລືອກລະດັບ 5 ຫຼາຍກວ່າໝູ່ 118 ຄົນ ກວາມເອົາ 55.81% $\overline{X}$ = 4.13 SD=45.40 ຢູ່ໃນລະດັບ ໃຊ້ປະຈຳ, ການນຳໃຊ້ Software MS Office(Words, Excel, PowerPoint) ສຳຫຼັບວຽກຫ້ອງການ ແມ່ນເລືອກລະດັບ 5 ຫຼາຍກວ່າໝູ່ $\overline{X}$ =4.23, 4.00, 3.88 ຕາມລຳດັບ SD=44.59, 34.97, 31.10 ຕາມລຳດັບ ຢູ່ໃນລະດັບ ໃຊ້ປະຈຳ. ສຳຫຼັບການນຳໃຊ້ Google Doc ເຫັນວ່າ ໃຊ້ປະຈຳ ໂດຍກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດ ຢູ່ທີ 74 ຄົນ ກວາມເອົາ 34.88% $\overline{X}$ =3.84 SD=32.81, google sheet ເລືອກ ລະດັບ 3 ຫຼາຍທີ່ສຸດຢູ່ທີ 74 ຄົນ ເທົ່າກັບ 34.88% $\overline{X}$ =3.65 SD=31.10 ຢູ່ໃນລະດັບ ໃຊ້ປານກາງ, ສາມາດໃຊ້ແພລດຟອມປະຊຸມອອນໄລນ໌ (Zoom, Teams, Google Meet) ເຫັນວ່າກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 4 ແລະ 3 ຫຼາຍທີ່ສຸດເທົ່າກັນ ຢູ່ທີ 64 ຄົນ ກວາມເອົາ 30.23% $\overline{X}$ =3.70 SD=27.58 ຢູ່ໃນລະດັບ ໃຊ້ປານກາງ, ສາມາດເຄື່ອງມືສ້າງເນື້ອຫາດິຈິຕອນ (Canva, CapCut, Google Sites, etc.) ເຫັນວ່າ ໃຊ້ປານກາງ ໂດຍກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 3 ຫຼາຍທີ່ສຸດ ຢູ່ທີ 69 ຄົນ ກວາມເອົາ 32.55% $\overline{X}$ =3.74 SD=23.54, ສຳຫຼັບການຄົ້ນຫາຂໍ້ມູນທີ່ມີຄຸນນະພາບຈາກແຫຼ່ງທີ່ເຊື່ອຖືໄດ້ ເຫັນວ່າກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 4 ຫຼາຍທີ່ສຸດເທົ່າກັນ ຢູ່ທີ 99 ຄົນ ກວາມເອົາ 46.51% $\overline{X}$ =3.90 SD=35.31 ຢູ່ໃນລະດັບ ໃຊ້ປະຈຳ, ການແຍກຂ່າວຈິງອອກຈາກຂ່າວປອມໄດ້ ເຫັນວ່າກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 4 ຫຼາຍທີ່ສຸດເທົ່າກັນ ຢູ່ທີ 79 ຄົນ ກວາມເອົາ 37.20% $\overline{X}$ =3.93 SD=32.81 ຢູ່ໃນລະດັບ ໃຊ້ປະຈຳ, ສາມາດນຳໃຊ້ AI (ChatGPT, Copilot, Canva Magic Write) ເຫັນວ່າກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດເທົ່າກັນ ຢູ່ທີ 74 ຄົນ ກວາມເອົາ 34.88% $\overline{X}$ =3.93 SD=32.81 ຢູ່ໃນລະດັບ ໃຊ້ປະຈຳ, ສຳຫຼັບສາມາດນຳໃຊ້ເຄື່ອງມື AI (ChatGPT, Copilot, Canva Magic Write) ໃນການເຮັດວຽກປະຈຳວັນ ເລືອກ ລະດັບ 3

ຫຼາຍທີ່ສຸດເທົ່າກັນ ຢູ່ທີ 74 ຄົນ ກວາມເອົາ 34.88% $\overline{X}$ =3.79 SD=32.81 ຢູ່ໃນລະດັບ ໃຊ້ປານກາງ ແລະ ສຳຫຼັບ ການນຳຂໍ້ມູນທີ່ໄດ້ ຈາກອິນເຕີເນັດໄປໃຊ້ຢ່າງມີຈັນຍາບັນ ເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດ ເທົ່າກັນ ຢູ່ທີ 94 ຄົນ ກວາມເອົາ 44.19% $\overline{X}$ =4.14 SD=42.50 ຢູ່ ໃນລະດັບ ໃຊ້ປະຈຳ ຜົນດັ່ງກ່າວໄດ້ສະແດງໃຫ້ເຫັນໃນຮູບທີ 2.

3) ສຳຫຼັບສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ ເພື່ອສຶກສາພຶດຕິກຳການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຂອງ ພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ເຫັນໄດ້ວ່າ ທ່ານ ຕັ້ງລະຫັດຜ່ານທີ່ປອດໄພ ແລະ ການຮັກສາຂໍ້ມູນສ່ວນຕົວ ເຫັນວ່າ ກຸ່ມ ຕົວຢ່າງສາມາດຕະນັກໄດ້ເຖິງໄພຄຸກຄາມ ແລະ ຄວາມສ່ຽງຂອງການ ໂຈມຕີທາງໄຊເບີມັນໄດ້ຊີ້ໃຫ້ເຫັນ ໃນການປ້ອງກັນແຕ່ງເຊັ່ນ: ການ ປ່ຽນລະຫັດຜ່ານຂອງຂ້ອຍເປັນປະຈຳ ແມ່ນໄດ້ເຮັດ ຢູ່ໃນລະດັບຫຼາຍທີ່ ສຸດ ເລືອກລະດັບ 5 ຈຳນວນ 143 ຄົນ ເທົ່າກັບ 67.43% $\overline{X}$ =4.53 SD=58.92, ນອກຈາກນັ້ນມີການໃຊ້ລະຫັດທີ່ແຕກຕ່າງກັນໃນແຕ່ລະ ບັນຊີ ເຂົ້າໃຈຄວາມສ່ຽງຂອງການໃຊ້ລະຫັດຜ່ານທີ່ອ່ອນແອ. ຜູ້ຕອບ ແບບສອບຖາມສາມຮູ້ທັນ ແລະ ຫຼີກລ້ຽງການຄລິກລິ້ງ ຫຼື ເນື້ອຫາທີ່ ອາດມີໄວຣັດ ໂດຍ ເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດເທົ່າກັບ ຢູ່ທີ 99 ຄົນ ກວາມເອົາ 46.51% $\overline{X}$ =3.98 SD=34.79 ຢູ່ໃນລະດັບ ຫຼາຍ, ສຳຫຼັບ ຄວາມສາມາດແຍກຂ່າວຈິງອອກຈາກຂ່າວປອມໄດ້ ເຫັນວ່າເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດເທົ່າກັບ ຢູ່ທີ 108 ຄົນ ກວາມເອົາ 51.15% $\overline{X}$ =4.26 SD=43.49 ຢູ່ໃນລະດັບ ຫຼາຍທີ່ສຸດ, ສຳຫຼັບການຫຼີກເວັ້ນການ Post/Share ຂໍ້ມູນສ່ວນຕົວ, ການເຄື່ອນໄຫວຂອງຕົນເອງ ແລະ ອື່ງ ກອນເຫັນວ່າຜູ້ຕອບແບບສອບຖາມເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດເທົ່າກັບ ຢູ່ທີ 113 ຄົນ ກວາມເອົາ 53.49% $\overline{X}$ =4.28 SD=45.80 ຢູ່ໃນລະດັບ ຫຼາຍທີ່ສຸດ, ຄວາມສາມາດຈຳແນກຂ່າວປອມ ຫຼື ຂໍ້ມູນຫຼອກລວງ ທີ່ ຖືກສ້າງມາຈາກ AI ເຫັນວ່າ ຢູ່ໃນລະດັບ ຫຼາຍ ໂດຍກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ 5 ຫຼາຍທີ່ສຸດ ຢູ່ທີ 99 ຄົນ ເທົ່າກັບ 46.51 $\overline{X}$ =4.09 SD=37.64. ສຳຫຼັບຄວາມສາມາດຈຳແນກອີເມວປອມ (phishing email) ໄດ້ນັ້ນ ເຫັນວ່າ ຜູ້ຕອບແບບສອບຖາມເລືອກ ລະດັບ 5 ຫຼາຍ ທີ່ສຸດ ຢູ່ທີ 79 ຄົນ ເທົ່າກັບ 39.20% $\overline{X}$ =3.84 SD=28.45 ຢູ່ໃນ ລະດັບ ຫຼາຍ, ການຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີການຂອງ Call Center ຢູ່ ໃນລະດັບ ຫຼາຍ ໂດຍຜູ້ຕອບ ເລືອກ ລະດັບ 5 ຢູ່ທີ 104 ຄົນກວາມເອົາ 48.83% $\overline{X}$ =4.07 SD=39.83 ແລະ ການຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີ ການຂອງ Scammer ເຫັນວ່າກຸ່ມຕົວຢ່າງເລືອກ ລະດັບ ຫຼາຍທີ່ສຸດ ຈຳນວນ 84 ຄົນກວາມເອົາ 39.53% $\overline{X}$ =4.07 SD=37.32 ຢູ່ໃນ ລະດັບຫຼາຍ ດັ່ງສະແດງໃຫ້ເຫັນຮູບສະແດງຜົນ ຮູບທີ 3.

4) ວິພາກຜົນ

ຈາກຜົນ ການສຶກສາ ທັກສະການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ຜົນຂອງ ການຄົ້ນຄວ້າໄດ້ສະແດງເຫັນ ໃນເສັ້ນສະແດງ ໃນຮູບທີ 2. ເຫັນໄດ້ວ່າ ລະດັບຄວາມຄິດເຫັນໃນທັກສະຂອງການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຂອງກຸ່ມປະຊາກອນ $5-1$ ເຊິ່ງ 5 ໝາຍ ດີຫຼາຍ, 4 ໝາຍເຖິງ ໃຊ້ປະ ຈຳ, 3 ໝາຍເຖິງ ໃຊ້ປານກາງ, 2 ໝາຍເຖິງໃຊ້ໜ້ອຍ ແລະ 1 ໝາຍເຖິງ ບໍ່ເຄີຍໃຊ້ ເຫັນວ່າ ທັກສະ ຂອງ ກຸ່ມຕົວຢ່າງ ຢູ່ໃນລະດັບ ໃຊ້ເປັນຈະຈຳ ໂດຍ $\overline{X}$=3.91, SD=6.63. ສຳຫຼັບຜົນຂອງການສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ ຂອງພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ຜົນຂອງການຄົ້ນຄວ້າໄດ້ສະແດງເຫັນ ໃນເສັ້ນສະແດງ ໃນຮູບທີ 3. ເຫັນໄດ້ວ່າລະດັບຄວາມຄິດເຫັນໃນທັກ ສະຂອງການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຂອງກຸ່ມປະຊາກອນ $5-1$ ເຊິ່ງ 5 ໝາຍເຖິງ ຫຼາຍທີ່ສຸດ, 4 ໝາຍເຖິງ ຫຼາຍ, 3 ໝາຍເຖິງ ປານກາງ , 2 ໝາຍເຖິງ ໜ້ອຍ ແລະ 1 ໝາຍເຖິງ ບໍ່ເຄີຍໃຊ້ ຜົນການຄົ້ນຄວ້າ ເຫັນວ່າ ຢູ່ໃນລະດັບ ຫຼາຍ $\overline{X}$=4.09, SD=8.37 ຖ້າທຽບໃສ່ຜົນການ ຄົ້ນຄວ້າຂອງທ່ານ ນາງ ນະພາສຸ ຂຽວວັນ(NAPASU KIAWWAN, 2023). ທີ່ໄດ້ສຶກສາ ປັດໃຈທີ່ມີຄວາມສຳພັນກັບການພັດທະນາຄວາມ ສາມາດດ້ານດິຈິຕອນຂອງເຈົ້າໜ້າທີຕຳຫຼວດສະພາ ສຳນັກງານເລຂາ ສະພາຜູ້ແທນລາດສະດອນ ແຫ່ງປະເທດໄທ ທີ່ໄດ້ໄດ້ນຳໃຊ້ ກຸ່ມຕົວຢ່າງ 128 ຄົນ ນຳໃຊ້ຄ່າ ສະເລ່ຍ $\overline{X}$ ແລະ SD. ຈາກຜົນຂອງການຄົ້ນຄວ້າ ຂອງເພີ່ນເຫັນວ່າ ດ້ານ ຄວາມຮູ້ ຢູ່ໃນລະດັບ ຫຼາຍ $\overline{X}$ =3.70 SD=0.61, ດ້ານທັກສະ ເຫັນວ່າຢູ່ໃນລະດັບ ຫຼາຍ $\overline{X}$ =3.72 SD=0.73, ດ້ານ ທັດສະນະຄະຕິ ເຫັນວ່າຢູ່ໃນລະດັບ ຫຼາຍ $\overline{X}$ =3.92 SD=0.69. ບົດຄົ້ນຄວ້າຂອງທ່ານ ໄຊຍາ ບຸນຍາລັດ ພ້ອມດ້ວຍໝູ່ ຄະນະ(Chaiya et al., 2023) ໄດ້ຄົ້ນຄວ້າ ການພັດທະນາຕົວຊີ້ວັດ ການພັດທະນາທັກສະດິຈິຕອນ ສຳລັບບຸກຄະລາກອນ ກົມທະຫານ ສື່ສານ ກະຊວງປ້ອງກັນປະເທດໄທ ໂດຍນຳໃຊ້ ກຸ່ມຕົວຢ່າງ 407 ຄົນ ເຫັນວ່າ ທັກສະດິຈິຕອນ ຂອງກຳລັງພົນ ກົມການທະຫານສື່ສານ ກະຊວງປ້ອງກັນປະເທດໄທ ຢູ່ໃນລະດັບ ຫຼາຍ $\overline{X}$ =4.41 SD=0.61. ເຫັນວ່າທັກສະຄວາມຮູ້ທາງດ້ານການນຳໃຊ້ ດິຈິຕອນຂອງພະນັກງານ ກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ມີຢູ່ໃນລະດັບດີ ເມື່ອ ທຽບໃສ່ກັບບັນດາປະເທດອ້ອມຂ້າງ ຫຼື ພາກພື້ນ. ສະນັ້ນກົມ ສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ແມ່ນມີຄວາມພ້ອມທາງດ້ານບຸກຄະລາ ກອນ ເພື່ອຫັນເປັນດິຈິຕອນຕາມແນວທາງນະໂຍບາຍຂອງປະເທດ

5. ສະຫຼຸບ

ໃນສຶກສາຄວາມຮູ້ຄວາມເຂົ້າໃຈໃນການນຳໃຊ້ດິຈິຕອນ ($Digital\ Literacy$) ຂອງພະນັກງານພາຍໃນກົມສື່ສານ ກະຊວງ ປ້ອງກັນຄວາມສະຫງົບ ໂດຍເປັນການຄົ້ນຄວ້າລັກສະນະຄຸນນະພາບ ເຊິ່ງນຳໃຊ້ແບບສອບຖາມ ເພື່ອຈຸດປະສົງ; 1) ເພື່ອສຶກສາພຶດຕິກຳການ ນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ 2) ເພື່ອສຶກສາທັກສະການນຳໃຊ້ເຕັກໂນ ໂລຊີດິຈິຕອນ 3) ເພື່ອສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີ ທາງໄຊເບີ ໂດຍມີກຸ່ມຕົວຢ່າງ 212 ເປັນຍິງ 59 ຄົນ ເທົ່າກັບ 27.83% ໄດ້ນຳໃຊ້ເຕັກນິກທາງສະຖິຕິໂດຍນຳໃຊ້ຄ່າສະເລ່ຍ $(\overline{X})$ ແລະ ຄ່າປ່ຽງ ແບນມາດຕະຖານ(SD) ເພື່ອບົ່ງຊີ້ຄວາມຄິດເຫັນຂອງກຸ່ມຕົວຢ່າງ. ຈາກການຄົ້ນຄວ້າເຫັນວ່າ ພຶດຕິກຳການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ຊີ້ ໃຫ້ເຫັນວ່າ $Social\ media$ ທີນິຍົມໃຊ້ທີ່ສຸດແມ່ນ $facebook,$ ການສື່ສານນິຍົມໃຊ້ $WhatApp$ ລວມທັງການໂອນຍ້າຍ $file$ ຂໍ້ມູນ , ສຳຫຼັບ $file$ ຂໍ້ມູນໃນປະລິມານຫຼາຍແມ່ນນຳໃຊ້ $Flat\ Drive,$ ການຈັດການເອກະສານແມ່ນນຳໃຊ້ $MS\ Word$ ຫຼາຍທີ່ສຸດ, ສຳຫຼັບ ການເກັບຂໍ້ມູນເທິງ $Cloud$ ໄດ້ນຳໃຊ້ $Google\ Drive,$ ໄດ້ນຳໃຊ້ ຄອມພິວເຕີເປັນປະຈຳ ແລະ ໃຊ້ແຕ່ລະຄັ້ງຫຼາຍກວ່າ 30 ນາທີ, ໄດ້ນຳໃຊ້ AI ເຂົ້າໃນວຽກງານເປັນປະຈຳ. ສຳຫຼັບ ຄວາມສາມາດ ຫຼື ທັກສະຂອງ ການນຳໃຊ້ເຕັກໂນໂລຊີດິຕອນເຫັນວ່າ ຈັດຢູ່ໃນການໄດ້ນຳໃຊ້ ເປັນ

ປະຈຳ ເຊັ່ນ: ຄວາມສາມາດໃນການ ສ້າງ/ເຊື່ອມຕໍ່ $Bluetooth/Hotspot$ ມີ $\overline{X} = 4.23$ SD =43.90, ການນຳໃຊ້ Computer ເພື່ອປະຕິບັດວຽກ $\overline{X} = 4.13$ $SD = 45.40$, ການນຳໃຊ້ Software MS Office(Words, Excel, PowerPoint) ສຳຫຼັບວຽກຫ້ອງການ $\overline{X} = 4.23, 4.00, 3.88$ ຕາມລຳດັບ $SD =$ $44.59, 34.97, 31.10$ ຕາມລຳດັບ, ສຳຫຼັບການນຳໃຊ້ Google Doc ເຫັນວ່າ $\overline{X} = 3.84$ $SD = 32.81$, $google\ sheet$ $\overline{X} =$ 3.65 $SD = 31.10$, ຄວາມສາມາດໃຊ້ແຜລດຟອມປະຊຸມອອນໄລນ໌ (Zoom, Teams ,Google Meet) $\overline{X} = 3.70$ $SD = 27.58$, ຄວາມສາມາດເຄື່ອງມືສ້າງເນື້ອຫາດິຈິຕອນ (Canva, CapCut, Google Sites,etc.) $\overline{X} = 3.74$ $SD = 23.54$, ສຳຫຼັບການຄົ້ນຫາຂໍ້ມູນທີ່ມີຄຸນນະພາບຈາກແຫຼ່ງທີ່ເຊື່ອຖືໄດ້ $\overline{X}$=3.90 SD=35.31. ສຳຫຼັບສຳຫຼັບສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ ເຫັນໄດ້ວ່າຢູ່ໃນລະດັບ ຫຼາຍ ເຊັ່ນ: ການຕັ້ງລະຫັດຜ່ານທີ່ປອດໄພ ແລະ ການຮັກສາຂໍ້ມູນສ່ວນຕົວ ການຕະນັກໄດ້ເຖິງໄພຄຸກຄາມ ແລະ ຄວາມສ່ຽງຂອງການໂຈມຕີທາງໄຊເບີມັນໄດ້ຊີ້ໃຫ້ເຫັນ $\overline{X}$ =4.53 SD=58.92, ນອກຈາກນັ້ນມີການໃຊ້ລະຫັດທີ່ແຕກຕ່າງກັນໃນແຕ່ລະບັນຊີ ເຂົ້າໃຈຄວາມສ່ຽງຂອງການໃຊ້ລະຫັດຜ່ານທີ່ອ່ອນແອ. $\overline{X}$ =3.98 SD=34.79, ສຳຫຼັບຄວາມສາມາດແຍກຂ່າວຈິງອອກຈາກຂ່າວປອມ ໄດ້ $\overline{X}$ =4.26 SD=43.49,ການຫຼີກເວັ້ນການ Post/Share ຂໍ້ມູນສ່ວນຕົວ, ການເຄື່ອນໄຫວຂອງຕົນເອງ ແລະ ອົງກອນ $\overline{X}$ =4.28 SD=45.80, ຄວາມສາມາດຈຳແນກຂ່າວປອມ ຫຼື ຂໍ້ມູນຫຼອກລວງ ທີ່ຖືກສ້າງມາຈາກ AI $\overline{X}$ =4.09 SD=37.64. ສຳຫຼັບຄວາມສາມາດຈຳແນກອີເມວປອມ (phishing email) ໄດ້ນັ້ນ $\overline{X}$ =3.84 SD=28.45, ການຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີການຂອງ Call Center $\overline{X}$ =4.07 SD=39.83 ແລະ ການຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີການຂອງ Scammer $\overline{X}$ =4.07 SD=37.32 ຢູ່ໃນລະດັບ. ເຫັນໃຊ້ວ່າພະນັກງານກົມສື່ສານ ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ແມ່ນມີຄວາມສາມາດນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ ແລະ ມີການຕະໜັກຮູ້ເຖິງໄພຄຸກຄາມ, ຄວາມສ່ຽງຂອງການໂຈມຕີທາງໄຊເບີ

6. ຂໍ້ຂັດແຍ່ງ

ຂ້າພະເຈົ້າໃນນາມຜູ້ຄົ້ນຄວ້າວິທະຍາສາດ ຂໍປະຕິຍານຕົນວ່າ ຂໍ້ມູນທັງໝົດທີ່ມີໃນບົດຄວາມວິຊາການດັ່ງກ່າວນີ້ ແມ່ນບໍ່ມີຂໍ້ຂັດແຍ່ງທາງຜົນປະໂຫຍດກັບພາກສ່ວນໃດ ແລະ ບໍ່ ໄດ້ເອື້ອປະໂຫຍດໃຫ້ກັບພາກສ່ວນໃດພາກສ່ວນໜຶ່ງ, ກໍລະນີມີການລະເມີດ ໃນຮູບການໃດໜຶ່ງ ຂ້າພະເຈົ້າມີຄວາມຍິນດີ ທີ່ຈະຮັບຜິດຊອບແຕ່ພຽງຜູ້ດຽວ.

7. ຄຳຂອບໃຈ (ຖ້າມີ, ຖ້າບໍ່ມີ ແມ່ນໃຫ້ເອົາອອກໄດ້)

ຂໍຂອບໃຈ ພາກວິຊາວິສະວະກຳຄອມພິວເຕີ ແລະ ເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ, ຄະນະວິສະວະກຳສາດ, ມະຫາວິທະຍາໄລແຫ່ງຊາດ ທີ່ ໄດ້ສິດສອນໃຫ້ຄວາມຮູ້ ແລະ ຂໍຂອບໃຈມາຍັງ ກົມກອງໂດຍສະເພາະ ກົມສື່ສານ, ກະຊວງປ້ອງກັນຄວາມສະຫງົບ ທີ່ໄດ້ສະໜອງຂໍ້ມູນ ແລະ ຊ່ວຍເຫຼືອໃນການຄົ້ນຄວ້າໃນຄັ້ງນີ້.

8. ເອກະສານອ້າງອີງ

Anderson, R., & Moore, T. (2006). The economics of information security. **Science*, 314*(5799), 610-613.

Bertot, J. C., Estevez, E., & Janowski, T. (2016). Universal and contextualized public services: Digital public service innovation framework. *Government Information Quarterly, 33*(2), 211-222.

Boonyarat, C. (2023). *Indicators Development of Digital Skills for Personnel of Signal Department*, Phuket Rajabhat University Academic Journal Volume 19 No. 1

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of Internet surveillance. *European Journal of Criminology, 6*(2), 119-134.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The digital competence framework for citizens*. Publications Office of the European Union.

Criado, J. I., Sandoval-Almazan, R., & Gil-Garcia, J. R. (2013). Government innovation through social media. *Government Information Quarterly, 30*(4), 319-326.

Gil-García, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. *Public Management Review, 20*(5), 633-646.

Helsper, E. J., & Eynon, R. (2013). Distinct skill pathways to digital engagement. *European Journal of Communication, 28*(6), 696-713.

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly, 32*(4), 363-368.

Lewandowsky, S., Ecker, U. K., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful

debiasing. *Psychological Science in the Public Interest, 13*(3), 106-131.

KIAWWAN, N. (2023). Factors Relating to Development of Digital Competency of the Parliamentary Police Officer of the Secretariat of the House of Representatives [Master Thesis] Sukhothai Thammathirat University

Mergel, I. (2013). Social media adoption and resulting tactics in the U.S. federal government. *Government Information Quarterly, 30*(2), 123-130.

Mossberger, K., Wu, Y., & Crawford, J. (2013). Connecting citizens and local governments? Social media and interactivity in major U.S. cities. *Government Information Quarterly, 30*(4), 351-358.

Norris, D. F. (2016). *E-government... not e-governance not e-democracy not now! not ever?* In *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance (pp. 339-340).

Rodríguez-Bolívar, M. P. (2017). Governance models for the delivery of public services through the Web 2.0 technologies: A political view in large Spanish municipalities. *Social Science Computer Review*, *35*(2), 203-225.

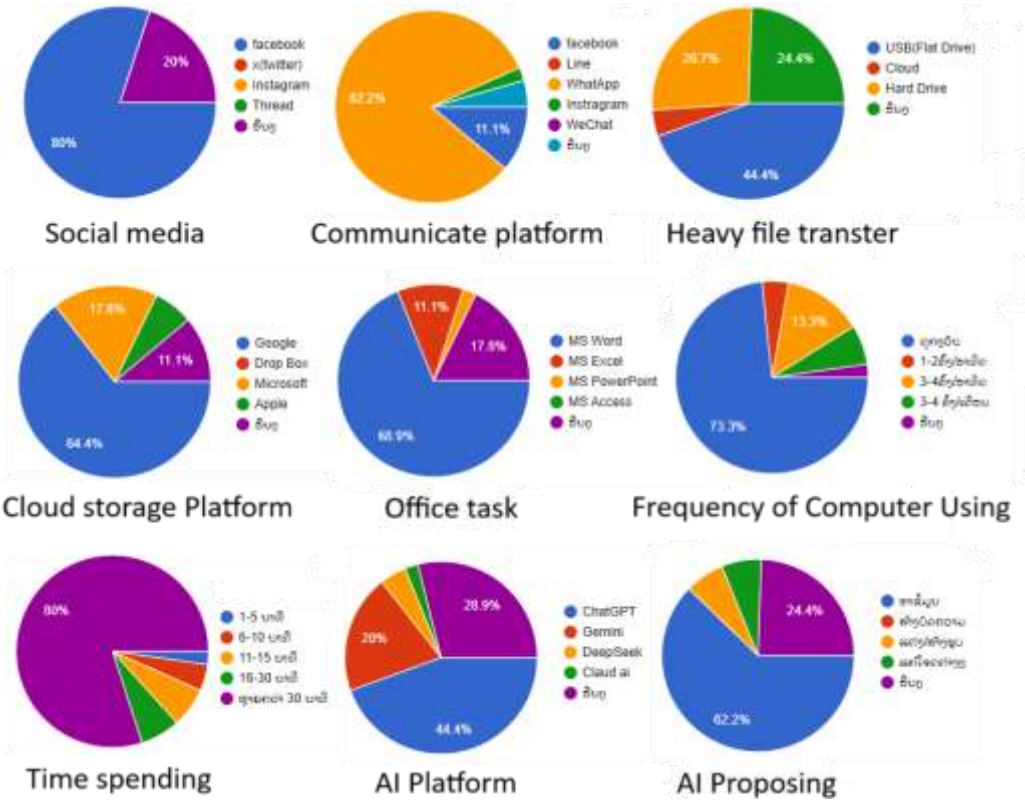
Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Shopova, T. (2014). Digital literacy of students and its improvement at the university. *Journal on Efficiency and Responsibility in Education and Science, 7*(2), 26-32.

Van Dijk, J. A. G. M. (2020). *The digital divide*. Polity Press.

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector applications and challenges. *International Journal of Public Administration, 42*(7), 596-615.



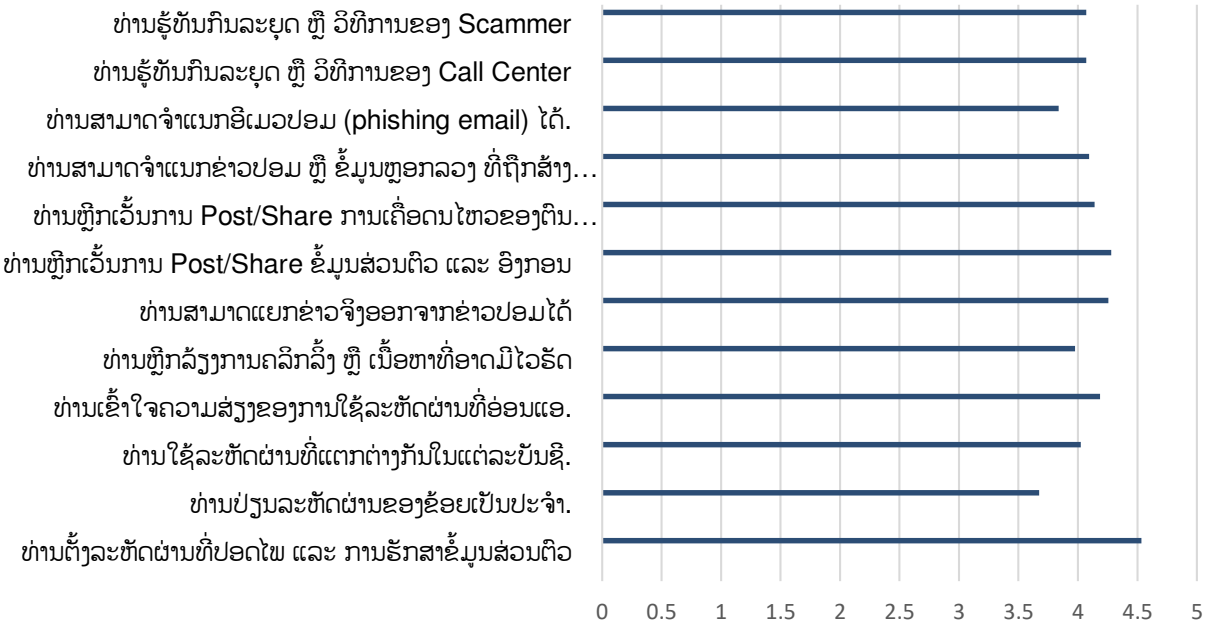
ຮູບທີ 1: ສະແດງຜົນພຶດຕິກຳການໃຊ້ Digital

ຕາຕະລາງທີ 1. ສະແດງການເກັບຜົນການສຶກສາທັກສະການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ

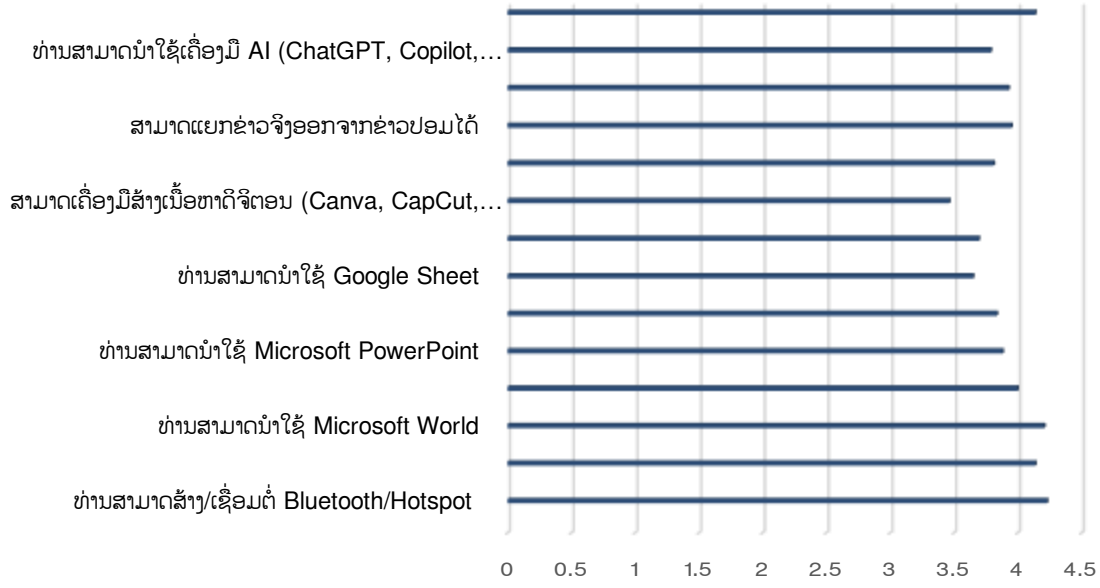
ລາຍການ	ລະດັບຄວາມຄິດເຫັນ					ລວມ	$\bar{X}$	SD	ຕີຄວາມໝາຍ
	5	4	3	2	1				
ທ່ານສາມາດສ້າງ/ເຊື່ອມຕໍ່ Bluetooth/Hotspot	108	54	44	0	5	212	4.23	43.90	ດີຫຼາຍ
ທ່ານສາມາດໃຊ້ Computer ເພື່ອປະຕິບັດວຽກງານ	118	49	20	5	20	212	4.14	45.40	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ Microsoft World	113	59	20	10	10	212	4.21	44.59	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ Microsoft Excel	94	54	44	10	10	212	4.00	34.97	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ Microsoft PowerPoint	79	59	54	10	10	212	3.88	31.10	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ Google Doc	74	54	69	5	10	212	3.84	32.81	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ Google Sheet	49	69	74	10	10	212	3.65	31.10	ໃຊ້ປານກາງ
ສາມາດໃຊ້ແພລດຟອມປະຊຸມອອນໄລນ໌ (Zoom, Teams, Google Meet)	59	64	64	15	10	212	3.70	27.58	ໃຊ້ປານກາງ
ສາມາດເຄື່ອງມືສ້າງເນື້ອຫາດິຈິຕອນ (Canva, CapCut, Google Sites, etc.)	44	59	69	30	10	212	3.47	23.54	ໃຊ້ປານກາງ
ສາມາດຄົ້ນຫາຂໍ້ມູນທີ່ມີຄຸນນະພາບຈາກແຫຼ່ງທີ່ເຊື່ອຖືໄດ້	49	99	49	5	10	212	3.81	37.81	ໃຊ້ປະຈຳ
ສາມາດແຍກຂ່າວຈິງອອກຈາກຂ່າວປອມໄດ້	69	79	54	5	5	212	3.95	35.31	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ AI (ChatGPT, Copilot, Canva Magic Write) ເພື່ອຫາຂໍ້ມູນໄດ້ຢ່າງມີປະສິດທິພາບ	74	69	54	10	5	212	3.93	32.81	ໃຊ້ປະຈຳ
ທ່ານສາມາດນຳໃຊ້ເຄື່ອງມື AI (ChatGPT, Copilot, Canva Magic Write) ໃນການເຮັດວຽກປະຈຳວັນ	69	54	74	5	10	212	3.79	32.81	ໃຊ້ປານກາງ

ສາມາດນຳຂໍ້ມູນທີ່ໄດ້ຈາກອິນເຕີເນັດໄປໃຊ້ຢ່າງມີຈັນຍາບັນ	94	84	15	10	10	212	4.14	42.50	ໃຊ້ປະຈຳ
ສະເລ່ຍ							4.14	6.63	ໃຊ້ປະຈຳ

ຮູບທີ 2: ແສງແດງຜົນທັກສະການນຳໃຊ້ເຕັກໂນໂລຊີດິຈິຕອນ



ຮູບທີ 3: ແສງແດງຜົນການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ



ຕາຕະລາງທີ 2. ຜົນຂອງການສຶກສາການຮັບຮູ້ ຄວາມສ່ຽງ ແລະ ການໂຈມຕີທາງໄຊເບີ

ລາຍການ	ລະດັບຄວາມຄິດເຫັນ					ລວມ	$\bar{X}$	SD	ຕີຄວາມໝາຍ
	5	4	3	2	1				
ທ່ານຕັ້ງລະຫັດຜ່ານທີ່ປອດໄພ ແລະ ການຮັກ ສາຂໍ້ມູນສ່ວນຕົວ	143	39	30	0	0	212	4.53	58.92	ຫຼາຍທີ່ສຸດ
ທ່ານປ່ຽນລະຫັດຜ່ານຂອງຂ້ອຍເປັນປະຈຳ.	54	64	69	20	5	212	3.67	28.45	ປານກາງ
ທ່ານໃຊ້ລະຫັດຜ່ານທີ່ແຕກຕ່າງກັນໃນແຕ່ ລະບັນຊີ.	89	54	54	15	0	212	4.02	35.31	ຫຼາຍ
ທ່ານເຂົ້າໃຈຄວາມສ່ຽງຂອງການໃຊ້ລະຫັດ ຜ່ານທີ່ອ່ອນແອ.	113	35	59	0	5	212	4.19	46.33	ຫຼາຍ
ທ່ານຫຼີກລ້ຽງການຄລິກລິ້ງ ຫຼື ເນື້ອຫາທີ່ ອາດມີໄວຣັດ	99	49	35	20	10	212	3.98	34.79	ຫຼາຍ
ທ່ານສາມາດແຍກຂ່າວຈິງອອກຈາກຂ່າວ ປອມໄດ້	108	59	35	10	0	212	4.26	43.49	ຫຼາຍທີ່ສຸດ
ທ່ານຫຼີກເວັ້ນການ Post/Share ຂໍ້ມູນສ່ວນ ຕົວ ແລະ ອື່ງກອນ	113	54	39	0	5	212	4.28	45.80	ຫຼາຍທີ່ສຸດ
ທ່ານຫຼີກເວັ້ນການ Post/Share ການ ເຄື່ອດນໄຫວຂອງຕົນເອງ ແລະ ອື່ງກອນ	104	54	39	10	5	212	4.14	39.84	ຫຼາຍ
ທ່ານສາມາດຈຳແນກຂ່າວປອມ ຫຼື ຂໍ້ມູນ ຫຼອກລວງ ທີ່ຖືກສ້າງມາຈາກ AI	99	59	35	15	5	212	4.09	37.64	ຫຼາຍ
ທ່ານສາມາດຈຳແນກອີເມວປອມ (phishing email) ໄດ້.	79	54	49	25	5	212	3.84	28.45	ຫຼາຍ
ທ່ານຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີການຂອງ Call Center	104	39	54	10	5	212	4.07	39.84	ຫຼາຍ
ທ່ານຮູ້ທັນກົນລະຍຸດ ຫຼື ວິທີການຂອງ Scammer	84	79	35	10	5	212	4.07	37.32	ຫຼາຍ
ສະເລ່ຍ							4.09	8.37	ຫຼາຍ