สื่อใหม่ ภัยเดิม เพิ่มเสี่ยง: พิศวาสอาชญากรรมกับการบริหารอาชญากรรมหลอกลวงของรัฐสมัยใหม่

New Media, Old Threat but Higher Risk: Romance Scam and the Seduction Crime Management of Modern State

ปัทชา ศึกษากิจ[A], วิชญาดา อำพนกิจวิวัฒน์[B], สรชา สุเมธวานิชย์[C], เขมชาติ ตนบุญ[D] และ ทศพล ทรรศนกุลพันธ์[E]
[A]ศูนย์โอมิกส์ด้านวิทยาศาสตร์สุขภาพคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ 110 ถ.อินทวโรรส ตำบลศรีภูมิ อำเภอเมือง จ.เชียงใหม่ 50200
[B]นักวิจัยอิสระ [C]นักวิจัยอิสระ [D]นักวิจัยอิสระ
[E]คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200

Pathacha Suksakit[A], Wichayada Amponkitwivat[B], Sorracha Sumethavanich[C],
Khemmachart Tonboon[D] and Tossapon Tassanakunlapan[E]
[A] Omics Center for Health Sciences: OCHS, Faculty of Medicine, Chiang Mai University, 110 Intawaroros Road, Si Phum, Muang, Chiang Mai 50200
[B] Independent Researcher, [C] Independent Researcher, [D] Independent Researcher
[E] Faculty of Law, Chiang Mai University, 239 Huay Kaew Road, Muang District, Chiang Mai, Thailand, 50200

Corresponding author E-mail : pathacha.s@gmail.com
Received: September 30, 2019; Revised: May 1, 2020; Accepted: May 8, 2020

บทคัดย่อ

การศึกษาพิศวาสอาชญากรรมที่กระทำผ่านสื่อใหม่โดยเฉพาะระบบปฏิบัติการในอินเตอร์เน็ต อาทิ เครือข่ายสังคมออนไลน์ เว็บบอร์ดในเว็บไซต์หาคู่ และอีเมล์ ก็เพื่อเข้าใจถึงภัยคุกคามที่มาพร้อมกับโอกาสที่เกิดขึ้นในชุมชนออนไลน์ ความเสี่ยงที่ปรากฏมาจากข้อจำกัดในการดำเนินคดีเพื่อปราบปรามอาชญากรและเยียวยาผู้เสียหาย อันจำเป็นต้องสร้างแนวทางป้องปรามพิศวาสอาชญากรรมในอนาคต โดยผลการศึกวิจัยพบ จุดอ่อนที่เหยื่อเผยข้อมูลส่วนบุคคล รูปแบบกลยุทธ์ที่อาชญากรใช้หลอกลวง ซึ่งเกิดในพื้นที่ไซเบอร์ที่ไร้พรมแดน แต่การดำเนินคดีพิศวาส

อาชญากรรมมีอุปสรรคจากขอบเขตอำนาจศาลของรัฐสมัยใหม่ ทำให้หลายกรณีรัฐอาจบ่งชี้ตัวผู้กระทำความผิดได้ แต่มิอาจบังคับใช้กฎหมายข้ามรัฐไปจับกุมผู้กระทำผิดในรัฐอื่น จนกลุ่มผู้เสียหายรวมตัวกันตอบโต้เองและนำไปสู่การใช้ความรุนแรงต่ออาชญากรในลักษณะก่ออาชญากรรมเสียเอง ปรากฏการณ์ดังกล่าวบ่งชี้ให้เห็นว่าพิศวาสอาชญากรรมในโลกไซเบอร์ต้องการมาตรการป้องกันปราบปรามอาชญากรรมที่ต้องก้าวข้ามข้อจำกัดของรัฐสมัยใหม่ หาไม่แล้วก็จะกระตุ้นให้ผู้เสียหายลุกขึ้นมาตอบโต้โดยผิดกฎหมาย

คำสำคัญ: อินเตอร์เน็ต, พิศวาสอาชญากรรม, กระบวนการยุติธรรมทางอาญา

Abstract

The study of Romance Scam in New Media and Internet Operative Systems; Social Networks, web boards, dating websites and e-mail, is for understanding the threats and opportunities which came from the emerging of Online-Community. The risks come from the limitation to prosecute criminals and remedy the victim so the construction of guideline to prevent further romance scams is needed. The research has shown the inferior that victim usually show their sensitive personal data on cyberspace, the tactic that criminal employ to seduce target on Cyberspace. However, the limitations to prosecute criminals and remedy the victim come from the obstacles relating to the jurisdiction of the Modern State. In many cases State official can identify the convicts but unable to enforce the law across territory. Thus, the reprisal group which gathering victims and active citizen to retaliate the criminal has occurred in a form of violent method. This phenomena reflects that Romance Scam revolts and demands a new measure which could step over many obstacles from the legal principle of Modern State. Otherwise, the cyberspace would be a battle field between the criminals and the violent netizen movements which could generate threats to the security of online community.

Key words: Internet, Romance Scam, Criminal Procedure

บทนำ

ปัจจุบันการติดต่อสื่อสารด้วยเทคโนโลยีสมัยใหม่ที่มีการพัฒนาอย่างไม่หยุดนิ่งได้เข้ามามีอิทธิพลกับชีวิตส่วนใหญ่ของมนุษย์ ทำให้ผู้คนทั่วโลกสามารถติดต่อสื่อสารกันได้ในเวลาเพียงไม่กี่วินาที ข้อมูลถูกส่งต่อกันแบบเรียลไทม์ และเปลี่ยนพฤติกรรมของมนุษย์ในพื้นที่กายภาพ (Physical Space) กับพื้นที่ไซเบอร์ (Cyber Space) มีความทับซ้อนกันอย่างสลับซับซ้อนจนก้าวข้ามข้อจำกัดของเวลา รวมถึงข้อจำกัดในเรื่องการสร้างความสัมพันธ์ของผู้คนในต่างสถานที่ ผู้คนส่วนใหญ่หันเข้าสู่โลกออนไลน์มากกว่าแทนที่จะออกไปมีปฏิสัมพันธ์กับผู้อื่น และเลือกที่จะสื่อสารกันผ่านสื่อออนไลน์มากกว่า ความเปลี่ยนแปลงอย่างหนึ่งที่เห็นได้ชัดคือการค้นหา “เพื่อน” หรือ “คนรัก” ผ่านเครือข่ายสังคมออนไลน์ จากอดีตที่ต้องพบปะแบบเห็นหน้ากันก่อนจึงจะสามารถสานสัมพันธ์ในรูปแบบอื่นๆ ต่อไปได้ ปัจจุบันสามารถค้นหาความสัมพันธ์ใหม่ๆ และติดต่อกันได้ผ่านเครือข่ายสังคมออนไลน์โดยไม่ต้องเจอ “ตัวจริง” ย่อมเกิดช่องโหว่ให้เกิดการกระทำความผิดโดยอาศัย “ความรัก ความห่วงใย หรือความเหงา” เป็นตัวแปรสำคัญในการก่ออาชญากรรมที่เรียกว่า “พิศวาสอาชญากรรม”

1. พิศวาสอาชญากรรมคืออะไร? ทำไมต้องพิศวาส?

พิศวาสอาชญากรรม (Romance Scam) หรือหลายคนเรียกว่า “การหลอกลวงรัก” และเป็นที่รู้จักกันในต่างประเทศด้วยชื่อของ Love Scam, Online Dating Romance Scam, Sweethearts Scam หรือ 419 Scam ไม่ว่ามันจะถูกเรียกในชื่อใดก็ตามถือว่าเป็นอาชญากรรมในโลกไซเบอร์ที่ผู้เสียหายสูญเงินมากเป็นอันดับต้นๆ ของเหล่าอาชญากรรมไซเบอร์เมื่อเทียบกับจำนวนผู้เสียหาย อาชญากรเหล่านี้เรียกว่า “นักต้มตุ๋น” (Romance Scammer) พฤติการณ์พื้นฐานคือการ “หลอกลวง” จากการสร้างความสัมพันธ์รักออนไลน์ ผ่านเครือข่ายสังคมออนไลน์ที่ชอบด้วยกฎหมาย เช่น Facebook, Instagram, และ Dating Website/Application เป็นต้น

พฤติการณ์ของพิศวาสอาชญากรรม สามารถอธิบายได้ 3 ขั้นตอนง่ายๆ คือ *ขั้นแรก* สร้างโปรไฟล์ปลอมอย่างละเอียดรอบคอบ ด้วยการใช้ภาพถ่ายของบุคคลอื่นโดยไม่ได้รับอนุญาต เรียบเรียงคำโปรยที่สวยหรูเกี่ยวกับงานอดิเรก และสิ่งอื่นๆ ให้ดูน่าสนใจในเชิงชู้สาว *ขั้นที่สอง* เริ่มการสนทนาติดต่อกับเหยื่อ ด้วยการใช้กลยุทธ์เทคนิคทางจิตวิทยาจนเหยื่อหลงเชื่อ จากการสร้างภาพต่อเหยื่อว่าเป็นคนที่น่าเชื่อถือ มั่นคง และโรแมนติก แม้บางครั้งจะใช้เวลานานถึง 6-8 เดือนก็ตาม จนกระทั่งเป้าหมายไว้ใจในความสัมพันธ์รักดังกล่าว *ขั้นที่สาม* นักต้มตุ๋นจะเริ่มแสดงออกถึงความ

ต้องการของตน เช่น มีการพูดคุยเรื่องเงินบ่อยขึ้น มีการสร้างสถานการณ์หลอกให้เหยื่อโอนเงิน ไม่ว่าเป็นถูกปล้นขณะท่องเที่ยว เกิดเหตุฉุกเฉินที่โรงพยาบาล หรือต้องการเงินเพื่อเดินทางไปพบเหยื่อ เป็นต้น หรือหลอกล่อให้เหยื่อยกสิ่งของมีค่าให้กับตน ซึ่งวิธีการของนักต้มตุ๋นมักจะมาพร้อมคำสัญญาต่างๆ เช่น สัญญาว่าจะมาแต่งงานด้วย สัญญาว่าจะมาสร้างครอบครัวกับเหยื่อ สัญญาว่าจะสร้างธุรกิจร่วมกัน โดยเหยื่อไม่มีทางรู้ทันคำลวงของนักต้มตุ๋น และเมื่อเหยื่อยอมโอนเงินให้แก่นักต้มตุ๋นแล้ว เหยื่อจะติดอยู่ในวงจรของการหลอกลวงไปอย่างไม่จบสิ้นจนกว่าเหยื่อจะหมดศักยภาพทางการเงิน หรือเหยื่อหยุดส่งเงินด้วยเหตุผลใดๆ ก็ตาม

“ความพิศวาส” หรือ ความรัก ความหลงใหล และไว้ใจในความสัมพันธ์ระหว่างเหยื่อกับ “คนรัก” ในโลกออนไลน์ที่นักต้มตุ๋นใช้เป็นเครื่องมือในการหลอกลวงให้เหยื่อเกิดความเสียหายทั้งด้านทรัพย์สินและด้านจิตใจ (Double Hit) ซึ่งการเยียวยาความเสียหายทางจิตใจถือเป็นสิ่งที่ยากเกินจะประเมินค่า หลายคนเสียใจมากเมื่อทราบว่าตนถูกหลอกไม่ใช่เพราะสูญเงินไป แต่เป็นการเสีย “คนรัก” ไป เนื่องจากพวกเขาเชื่อจริงๆ ว่าการโอนเงินนั้นเป็นการแสดงความช่วยเหลือต่อคนรัก เพื่อพัฒนาความสัมพันธ์ของพวกเขาทั้งคู่ ด้วยความสูญเสียจากพื้นฐานของความพิศวาสนี้ทำให้เหยื่อหลายคนรู้สึกอายจนไม่กล้าเข้าแจ้งความ และไม่เชื่อว่ากฎหมายจะสามารถช่วยให้พวกเขาหลุดพ้นออกจากความสูญเสียดังกล่าวได้ มากกว่านั้นบางคนถลำลึกจนกลายเป็นเหยื่อของการฟอกเงินร่วมด้วย The Office of Fair Trading กล่าวว่า การหลอกลวงนี้ถือเป็นภัยเงียบ เพราะเหยื่อไม่ได้มองว่านั่นคือผู้กระทำความผิด และจะรู้ตัวก็ต่อเมื่อการหลอกลวงนั้นสิ้นสุดไปแล้ว[1] ซึ่งก่อให้เกิดอันตรายทางจิตวิทยาไม่ว่าจะเป็น ความอับอาย ความละอาย ความอึดอัดลำบากใจ ความสะเทือนใจ ความหดหู่ ความโศกเศร้า ความรู้สึกอยากฆ่าตัวตาย ความวิตกกังวล และการสูญเสียความไว้วางใจ เป็นต้น จากงานวิจัยของ Markus Jakobsson (2016)[2] พบว่า เหยื่อส่วนใหญ่มักถอนตัวออกจากกิจกรรมประจำโดยเฉพาะกิจกรรมที่เกี่ยวข้องกับอินเตอร์เน็ต เนื่องจากรู้สึกสูญเสียความไว้วางใจ และอับอายอย่างมากโดยที่ไม่บอกให้ใครทราบเกี่ยวกับเรื่องที่เกิดขึ้น ถือเป็นเรื่องอัปยศและยากที่จะเล่าเรื่องราวหรือประสบการณ์นั้นออกมา

---

[1] Office of Fair Trading, “Helping People Affected by Scams: A Toolkit for Practitioners,” Office of Fair Trading, October 29, 2018, http://www.oft.gov.uk/shared_oft/reports/consumer_protection/400585_OFT_ Scams Toolkit_ful1.pdf

[2] Ting-Fang Yen, and Markus Jakobsson, “Case Study: Romance Scams,” In *Understanding Social Engineering Based Scams* (New York: Springer, 2016), 103-113

2. สถานการณ์ปัจจุบันของพิศวาสอาชญากรรม

ก่อนอื่นต้องเกริ่นก่อนว่าอาชญากรรมลักษณะดังกล่าวไม่ได้เพิ่งเกิดขึ้นเมื่อมีแอปพลิเคชันหาคู่ หรือเครือข่ายสังคมออนไลน์ ในต่างประเทศเรื่องราวเหล่านี้เริ่มเกิดขึ้นตั้งแต่ทศวรรษ 1970 ด้วยการส่งจดหมายและแฟกซ์ กลุ่มเป้าหมายของการส่งจดหมายมักเป็นผู้ชายที่ซื้อนิตยสารผู้ใหญ่[3] โดยระยะเวลาในการสร้างความผูกพันกับเหยื่ออาจกินเวลามากถึง 8 เดือน อาชญากรกลุ่มนี้มักแสร้งว่ามีเงินจำนวนมากแต่มีเหตุผลบางอย่างที่ไม่สามารถเอาเงินเหล่านั้นออกมาได้ เช่น ทรัพย์สินนั้นที่ไม่มีใครครอบครอง, ถูกโกง, ไร้ทายาท เป็นต้น เหยื่อจะได้รับค่าตอบแทนอย่างสูงเพียงแค่ช่วยพวกเขาให้พ้นจากปัญหาต่างๆ จากเจ้าหน้าที่รัฐหรือคนในครอบครัว ซึ่งอาชญากรกลุ่มนี้เป็นกลุ่มชาวไนจีเรีย หรือเป็นรู้จักกันในชื่อ “419 scam”[4] การเข้าถึงอินเตอร์เน็ต รวมถึงการมีเครือข่ายสังคมออนไลน์ และแอปพลิเคชันทั้งหลายนั้นกลายเป็นสื่อกลางที่เปิดโอกาสให้เกิดการหลอกลวงสะดวกและแพร่หลายยิ่งขึ้น เพราะอาชญากรสามารถใช้อินเตอร์เน็ตในการเข้าถึงเป้าหมาย และเรียนรู้เป้าหมายได้ง่ายดาย ทั้งยังสะดวกต่อการอำพรางตัวตน ส่งผลให้อาชญากรรมดังกล่าวกระจายออกไปอย่างรวดเร็วแปรผันตามการหลั่งไหลของข้อมูลในโลกอินเตอร์เน็ต จนกระทั่งในปี 2010 The International Mass Marketing Fraud Working Group ประกาศให้ Romance Scam กลายเป็นภัยคุกคามทั่วโลกซึ่งจากเดิมเป็นปัญหาแค่ในอเมริกาเหนือ[5]

การร้องเรียนเรื่อง Romance Scam ในประเทศแคดาดา เพิ่มขึ้นอย่างรวดเร็วตั้งแต่ ค.ศ. 2008 โดยมีอัตราเพิ่มขึ้น 1,500% และมีค่าเสียหายเฉลี่ยคนละ 11,000 ดอลลาร์แคนาดา[6] ในปี ค.ศ. 2012 คณะกรรมการการแข่งขันและผู้บริโภคของออสเตรเลีย (the Australian Competition and Consumer Commission (ACCC))[7] รายงานว่ามีผู้ที่ตกเป็นเหยื่อของ Romance Scam

---

[3] นิตยสารผู้ใหญ่ หมายถึง หนังสือที่มีเนื้อหาล่อแหลม หนังสือโป๊

[4] Whitty Monica T, “Anatomy of the Online Dating Romance Scam." *Security Journal*, 28, No. 4 (2015): 443-55.

[5] Int’l Mass-Marketing Fraud Working Group, “Mass-Marketing Fraud: A Treat Assessment,” Int’l Mass-Marketing Fraud Working Group, accessed October, 29, 2018, www.ice.gov/doclib/cornerstone/pdf/immfa.pdf

[6] Lauren La Rose, “Online romance scam can hurt hearts and wallets,” The Canadian Press, accessed Mar 7, 2019, http://www.thestar.com/life/2011/10/06/online_romance_scams_can_hurt _hearts_and_wallets.html.

[7] Australian Competition and Consumer Commission (ACCC), *Dating and romance scams:*

ทั้งสิ้น 2,110 คน และสูญเงินไปเกือบ 20.9 ล้านดอลลาร์ออสเตรเลีย และปีเดียวกันในสหราชอาณาจักรพบว่ามีผู้ตกเป็นเหยื่อประมาณ 500,000 คน[8] นอกจากนั้นรายงานการรวบรวมทางสถิติในปี ค.ศ. 2011 – 2016 ของ The FBI’s Internet Crime Complaint Center (IC3) พบมูลค่าความเสียหายเพิ่มขึ้นหลายเท่าตัวจาก 50,399,563 ดอลลาร์สหรัฐในปีค.ศ. 2011 เป็นจำนวน 219,807,760 ดอลลาร์สหรัฐภายในระยะเวลา 5 ปี[9] ข้อมูลทางสถิติของไอซ์แลนด์เหนือตั้งแต่เดือนพฤศจิกายน ค.ศ. 2018 ถึงเดือนพฤษภาคม ค.ศ. 2019 ประเทศสูญเงินไปกับเหล่าอาชญากรลวงรักเหล่านี้ราว 1.8 ล้านยูโร[10]

รายงานของตำรวจมาเลเซีย (The Royal Malaysian Police) ใน ค.ศ. 2013 ได้รับการร้องเรียนจากผู้เสียหายจำนวน 1,095 คน ที่มีมูลค่าความเสียหายถึง 35.69 ล้านริงกิต ซึ่งเพิ่มขึ้นจากปีก่อนหน้า 23.8% ที่มีผู้เสียหายจำนวน 814 คน ในมูลค่าความเสียหาย 33.61 ล้านริงกิต[11] นอกจากนั้นข้อมูลล่าสุดในไตรมาสแรกของปีค.ศ. 2019 ของประเทศสิงคโปร์ พบจำนวนผู้เสียหายกรณีพิศวาสอาชญากรรมที่แจ้งความกับตำรวจเพิ่มขึ้น 6% (จาก 288 ราย เป็น 306 ราย) จากช่วงเวลาเดียวกันของปีที่แล้ว และสูญเงินเพิ่มขึ้นถึง 46% คิดเป็นมูลค่า 17.1 ล้านดอลลาร์สิงคโปร์[12]

Defining the harm (Australia: ACCC, 2013)

[8] Internet Crime Complaint Center, “Annual Reports 2014 Internet Crime Report,” Internet Crime Complaint Center.

[9] Internet Crime Complaint Center “Annual Reports 2011-2014 Internet Crime Report,” Internet Crime Complaint Center.

[10] The Irish Times, “Woman loses more than £300,000 in romance scam,” accessed June 23, 2019, https://www.irishtimes.com/news/ireland/irish-news/woman-loses-more-than-300-000-in-romance-scam-1.3934854

[11] Hamsi Ahmad Safwan, Farrah Diana Saiful Bahry, Siti Noraini Mohd Tobi, and Maslin Masrom, “Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem,” *Journal of Management Research* 7, no. 2 (2015): 169.

[12] Nabilah Awang, “Internet love scammers target those who are emotionally vulnerable, say police,” Today, accessed September 15, 2019, https://www.todayonline.com/singapore/internet-love-scammers-reap-surging-sums-they-target-vulnerable-police.

สำหรับประเทศไทยนั้นพบตัวเลขที่ชัดเจนของอาชญากรรมดังกล่าวเพียงไม่กี่ปีก่อนหน้านี้ โดยข้อมูลจาก พ.ต.อ. ภาณุวัฒน์ ร่วมรักษ์ รองผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) ได้เปิดเผยว่าในปี พ.ศ. 2558 ที่ เฉพาะคดีเกี่ยวกับ Romance Scam ถูกร้องเรียนเข้ามาถึง 80 คดี มูลค่าความเสียหายสูงถึง 150 ล้านบาท ยังไม่นับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และเหยื่อที่ไม่กล้าเข้าแจ้งความอีกเป็นจำนวนมาก[13] และในระยะเวลาเพียงเกือบ 3 เดือน ตั้งแต่วันที่ 22 มิถุนายน ถึงวันที่ 5 กันยายน พ.ศ. 2561 พบว่ามีจำนวนคดีพิศวาสอาชญากรรมเกิดขึ้น 107 คดี มูลค่าความเสียหายสูงถึง 72 ล้านบาท ตามรายงานสถิติการรับแจ้งเหตุของศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) ด้วยความร่วมมือจากสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และสำนักงานตำรวจแห่งชาติ[14] และข้อมูลล่าสุดตั้งแต่วันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีเหยื่อหลงเชื่อและโอนเงิน จำนวน 332 ราย เป็นเงินกว่า 193 ล้านบาท[15] ข้อมูลเหล่านี้เป็นเพียงสถิติที่วัดได้จากการเก็บข้อมูลตัวเลข เพื่อทำให้ “คนนอก” ได้มองเห็นสภาพความสูญเสียในแต่ละปีที่เหยื่อต้องหมดทรัพย์สินไปกับภัยเงียบนี้ หากมองอีกมุมหนึ่งที่เหยื่อเหล่านี้ที่ได้รับผลกระทบทางจิตใจที่ไม่สามารถประมวลออกมาให้เป็นตัวเลขได้นั้นย่อมเป็นสิ่งที่ยากเกินจะเยียวยาในเรื่องดังกล่าวหากรัฐปราศจากมาตรการป้องกันล่วงหน้า

3. ความเปลี่ยวเหงาที่นำไปสู่การตกเป็น “เหยื่อ”

ผู้คนจำนวนมากหันเข้าสู่โลกออนไลน์แทนการออกไปมีปฏิสัมพันธ์กับผู้อื่นในโลกกายภาพ และเลือกที่จะสื่อสารเรื่องส่วนตัวกันผ่านสื่อออนไลน์มากกว่า เพราะพวกเขาสามารถระบาย หรือได้พูดคุยกับคนที่ไม่รู้จักตัวตนของพวกเขาโดยอาจไม่ต้องเปิดเผยตัวตนที่แท้จริงอันทำให้พวกเขารู้สึกสบายใจกว่า[16] การทำงานของแอปพลิเคชันสร้างเครือข่ายสังคมออนไลน์ด้วย

---

[13] Rabbit finance Magazine, “Romance Scam หลอกรักออนไลน์ ภัยร้ายของสาวโสด!,” Rabbit finance Magazine, สืบค้นเมื่อวันที่ 25 พฤศจิกายน 2561, https://finance.rabbit.co.th/blog/romance-scam-and-single-ladies.

[14] ผู้จัดการออนไลน์, “ปปง.-สตม. ร่วมส่งมอบคืนเงินเหยื่อแก๊ง Romance Scam,” Mgonline, สืบค้นเมื่อวันที่ 25 พฤศจิกายน 2561, https://mgronline.com/uptodate/detail/9610000089364.

[15] แนวหน้า, “ปปง.เผยตั้งศปก.ปปง. 1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน” แนวหน้า, สืบค้นเมื่อวันที่ 31 พฤษภาคม 2562, https://www.naewna.com/local/417058.

[16] David Ludden, “Does Using Social Media Make You Lonely?,” Psychology Today, สืบค้น

อัลกอริทึม (Algorithm) ที่จับคู่ให้ผู้ใช้งานสามารถพบเจอผู้คนที่รู้จัก หรือดึงกลุ่มของคนที่มีความคิดและความชอบที่เหมือนหรือคล้ายกันเข้ามาพบเจอกัน โดยเฉพาะเครือข่ายที่เป็นการสร้างชุมชนบนโลกออนไลน์ในลักษณะการใส่ข้อมูลส่วนตัวให้คนอื่นมาสนใจแบบมองมาที่ฉัน (Look at me) ผ่านการแบ่งปันพื้นฐานข้อมูลเฉพาะบุคคลไม่ว่าจะเป็น ค่านิยม สไตล์บุคลิกภาพ ทัศนคติ ความสนใจ เชื้อชาติ เพศสภาวะ และตำแหน่งที่อยู่นั้นสร้างความเสี่ยงให้กับผู้ใช้มากขึ้นจากการเผยข้อมูลอ่อนไหวของตนให้คนแปลกหน้าซึ่งอาจจะเป็นอาชญากรที่มองหาเหยื่อ ทั้งนี้อาจกล่าวได้ว่าด้วยการทำงานของอัลกอริทึมนั้นเสมือนบังคับให้ผู้ใช้งานเปิดเผยข้อมูลในอินเตอร์เน็ตอย่างเลี่ยงมิได้

ปัจจัยทางสังคมวัฒนธรรม เศรษฐกิจ และการเมืองทำให้เกิดปรากฏการณ์ “ความเหงา” ผลจากการสำรวจของมหาวิทยาลัยมหิดลในปี พ.ศ. 2562 พบว่าสถิติความเหงาของคนไทยมีจำนวนกว่า 26.75 ล้านคน หรือคิดเป็น 40.4% โดยสถานภาพหย่าร้างเป็นกลุ่มคนที่ประสบภาวะความเหงาสูงสุดถึง 50% ซึ่งมี 44.3% ของกลุ่มคนเหงาทั้งหลายได้เลือกใช้โซเชียลมีเดีย เป็นกิจกรรมเพื่อจัดการความเหงาเหล่านั้น เพราะสามารถเข้าถึงง่าย และสามารถสร้างความรู้สึกร่วมกับสังคมเสมือนบนออนไลน์ได้ทุกที่ ทุกเวลา เป็นหนึ่งในวิธีแก้เหงาที่เสียค่าใช้จ่ายน้อยที่สุด[17]

ด้วย “ความเหงา” ที่มาพร้อมกับการขาดทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital literacy) มักนำไปสู่ความสูญเสียจากพิศวาสอาชญากรรม เนื่องจากเหยื่อส่วนใหญ่มักมองข้ามความสำคัญของการนำข้อมูลส่วนบุคคล หรือวิถีชีวิต (Lifestyle) เข้าสู่โลกดิจิทัล ไม่ว่าจะเป็น การแสดงข้อมูลชื่อ อายุ การทำงาน สถานะทางสังคม สถานะสมรส งานอดิเรก ความชื่นชอบส่วนตัว การแสดงความคิดเห็น ภาพถ่าย สเตตัส และการแชร์ข้อมูลต่างๆ สิ่งเหล่านั้นเสมือนเป็นเหรียญสองด้าน ด้านหนึ่งทำให้คนเราได้มีปฏิสัมพันธ์ร่วมกับเพื่อนและคนที่รู้จัก แต่อีกด้านหนึ่งสิ่งนั้นอาจนำภัยเข้ามาใกล้ตัว Romance Scammer จะใช้วิธีประเมิน และเรียนรู้เป้าหมายผ่านข้อมูลส่วนบุคคล การแสดงความคิดเห็น ภาพถ่าย สเตตัส และการแชร์ข้อมูลที่คนคนหนึ่งโพสต์ลงบนโลกออนไลน์ เพื่อให้การหลอกลวงนั้นประสบผลสำเร็จสูงสุด

เมื่อวันที่ 26 พฤศจิกายน 2561, https://www.psychologytoday.com/intl/blog/talking-apes/201801/does-usingsocial-media-make-you-lonely.

[17] Marketeer, “Lonely Marketing: “เหงา” ที่แบรนด์ต้องช่วยเป็นเพื่อน” Marketeer, สืบค้นเมื่อวันที่ 2 กันยายน 2562, https://marketeeronline.co/archives/105589.

จากการศึกษาพบว่าลักษณะของผู้ที่ตกเป็นเหยื่อ และสูญเงินเป็นจำนวนมากนั้นเป็นไปในแนวทางเดียวกันทั่วโลก คือ **1. เพศหญิง** จากสถิติในประเทศไทยตั้งแต่ปีพ.ศ. 2560-2561 พบว่า เพศหญิงตกเป็นเหยื่อมากถึง 85.61% เพศชาย 10.97% เพศอื่น 3.87% ซึ่งสอดคล้องกับอีกหลายประเทศในโลก ตัวอย่างเช่น สหราชอาณาจักรในปีค.ศ. 2017 มีเพศหญิงตกเป็นเหยื่อ 63% และเพศชาย 37%[18] ปีเดียวกันในประเทศฮ่องกงมีเพศหญิงตกเป็นเหยื่อ 93.62% และเพศชาย 6.38%[19] และประเทศออสเตรเลียในปีค.ศ. 2018 มีเพศหญิงตกเป็นเหยื่อ 79.5% เพศชาย 20.3% และเพศอื่น 0.3%[20] **2. มีอายุเฉลี่ย 40-60 ปี** ทั้งนี้เพราะช่วงอายุดังกล่าวเป็นช่วงที่มีทรัพย์สิน/เงินเก็บสะสมอยู่พอสมควร ทำให้กลุ่มอายุนี้จะมีโอกาสเสียทรัพย์มากกว่าวัยอื่นๆ อย่างไรก็ตาม พบกลุ่มอายุที่น้อยกว่าตกเป็นเหยื่อด้วยเช่นกัน คืออายุตั้งแต่ 25 ปีขึ้นไป แต่จำนวนความเสียหายของทรัพย์สินไม่มากนัก ในอเมริกาพบว่า ผู้เสียทรัพย์มากที่สุดมีอายุ 40-69 ปี[21] เช่นเดียวกับออสเตรเลียมีอายุ 55–64 ปี[22] และประเทศอังกฤษมีอายุ 50 ปีขึ้นไป[23] **3. สถานภาพหย่าร้าง/หม้าย** ด้วยความโดดเดี่ยวเปลี่ยวเหงา และการผิดหวังจากความรักครั้งเก่า หรือการสูญเสียคนรักไป รวมทั้งความต้องการมีชีวิตรักที่สมบูรณ์นำไปสู่ความเสี่ยงของการตกเป็นเหยื่อได้อย่างง่ายดาย **4. เป็นคนใจอ่อน** คนเหล่านี้จะถูกชักจูงได้ง่ายจากนักต้มตุ๋น เพราะร้อยแปดเหตุผลและสถานการณ์ที่เหล่าอาชญากรได้รวมตัวกันปฏิบัติการหลอกลวงนั้นถูกวางแผนไว้หลายขั้นตอน

---

[18] Action Fraud, “Victims lost £41 million to romance fraud in 2017,” Action Fraud, accessed November 17, 2018, https://www.actionfraud.police.uk/news/victims -lost-41-million-to-romance-fraud-in-2017.

[19] The Hong Kong Police, “Snapshot of romance scam,” Hong Kong Police Force, accessed January 22, 2019, https://www.police.gov.hk/info/img/cpb/adcc/180517_en.pdf

[20] ACCC, “Scam statistics: dating & romance in 2018,” ACCC, accessed September 25, 2019, https://www. scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=13&date=2018.

[21] Emma Fletcher, “Romance scams rank number one on total reported losses,” Federal Trade Commission, accessed March 13, 2019, https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-lossesd.

[22] ACCC, “Scam statistics: dating & romance in 2018,” ACCC, accessed September 25, 2019, https://www. scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=13&date=2018.

[23] Eleanor Rose, “A Global Network of Scammers is Targeting Older People—Here’s How to Avoid Becoming a Victim,” accessed December 15, 2018, https://www.readersdigest.ca/home-garden/money/romance-scams-and-financial-fraud/

ให้มีความแนบเนียนมากที่สุด ทั้งนี้เหยื่อหลายคนยอมโอนเงินให้เพราะความสงสาร และคิดว่า “คนรัก” กำลังเดือดร้อน และต้องการความช่วยเหลือ ซึ่งเป็นไปได้ยากที่จะไม่ยื่นมือเข้าช่วยหากตนเองสามารถช่วยเหลือได้

4. ข้อจำกัดของกระบวนการยุติธรรมและ การทำให้ “เหยื่อ” ไม่ใช่ “เหยื่อ”

เมื่อขบวนการ Romance Scam ส่วนใหญ่เป็นลักษณะของการกระทำความผิดนอกราชอาณาจักร อีกทั้งเกิดขึ้นในโลกไซเบอร์ซึ่งเป็นโลกนิรนามที่สามารถอำพรางตัวตนได้อย่างง่ายดายทั้งการไม่ลงทะเบียนชื่อจริง และการใช้ VPN (Virtual Private Network)[24] ซึ่งยากต่อการติดตามตัวผู้กระทำผิดมารับโทษ ด้วยข้อจำกัดทางกระบวนการยุติธรรมไม่ว่าจะเป็น ข้อจำกัดของเจ้าหน้าที่ในการเก็บรวบรวมหลักฐาน รวมทั้งองค์ความรู้ในวิธีการและขั้นตอนในการสืบหาพยานหลักฐาน การเลือกใช้กฎหมายในการดำเนินคดี ระยะเวลาในการดำเนินคดี เป็นต้น

ด้วย “ความไม่รู้กฎหมาย” ของเหยื่อ และข้อจำกัดทั้งบุคลากรและงบประมาณของกระบวนการยุติธรรม รวมถึงองค์ความรู้ของผู้ปฏิบัติหน้าที่ทำให้การร้องเรียนกรณีพิศวาสอาชญากรรมเป็นเรื่องยาก ตั้งแต่จุดเริ่มต้นในกระบวนการคือ เมื่อเหยื่อเลือกเข้าแจ้งความร้องทุกข์ที่สถานตำรวจท้องที่ พร้อมหลักฐานเพียงภาพถ่ายข้อความการสนทนาระหว่างตนเองกับนักต้มตุ๋นและเลขที่บัญชีของผู้รับเงินโอนเท่านั้น แต่ถูกเจ้าหน้าที่ฯ ตอบกลับว่า *“ก็คุณเป็นคนโอนเงินให้เค้าเอง” “ทำไมถึงเชื่อคนง่าย?” “มันเกิดขึ้นเพราะคุณโลภเอง”*[25] ซึ่งเป็นการตอกย้ำความรู้สึกด้านลบทางจิตใจ และหมดที่พึ่งทางกระบวนการยุติธรรม ทั้งนี้อาจเป็นเพราะเจ้าหน้าที่ตำรวจ มิได้ความรู้ความเข้าใจเกี่ยวกับกรณีดังกล่าวอีกทั้งเป็นการกระทำความผิดบนโลกไซเบอร์ที่ต้องสืบจาก Traffic Data, IP Address, และ Hush Value เป็นต้น ซึ่งถือว่าเป็นเรื่องค่อนข้างใหม่สำหรับเจ้าหน้าที่ตำรวจในยุคก่อนดิจิทัล จึงไม่สามารถเข้าใจถึงเหตุแห่งคดีที่เหยื่อต้องการสื่อได้อันส่งผล

---

[24] VPN หรือ เครือข่ายส่วนตัวเสมือน เป็นฟังก์ชันที่สร้างขึ้นเพื่อให้ผู้ใช้อินเตอร์เน็ตรับส่งข้อมูลได้ปลอดภัยมากขึ้น เพราะมีการเข้ารหัสข้อมูลทั้งหมด ผู้ที่ไม่มีพาสเวิร์ดก็จะไม่สามารถเข้าถึงข้อมูลนี้ได้ เปรียบเหมือนการสร้างอุโมงค์ส่วนตัวขึ้นท่ามกลางเครือข่ายอินเทอร์เน็ตสาธารณะ ทำให้ IP address ที่ปรากฏในการใช้งาน จะเป็น IP address จากผู้ให้บริการเครือข่าย VPN ไม่ใช่เจ้าของแอคเคาท์ และผู้ใช้งาน VPN ยังสามารถตั้งค่าให้ตัวตนผู้ใช้งานไปโผล่ที่ประเทศอื่นที่ไม่ใช่ประเทศที่ตนเองใช้งานอินเทอร์เน็ตอยู่ ดังนั้นสามารถใช้ VPN เป็นเครื่องมือปกปิดตัวตนได้

[25] ผู้ไม่ประสงค์ออกนาม, ผู้เสียหายจากการถูกล่อลวงแบบพิศวาสอาชญากรรม สัมภาษณ์เมื่อวันที่ 7 เมษายน 2562

ต่อการรับฟังข้อเท็จจริง การสืบหาพยานหลักฐาน และการเลือกใช้ตัวบทกฎหมาย นอกจากนี้ยังมีข้อจำกัดด้านระยะเวลาในการแสวงหาพยานหลักฐานตามพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) มาตรา 26[26] ที่กำหนดให้เจ้าของระบบคอมพิวเตอร์จัดเก็บข้อมูลไว้เพียง 90 วัน ดังนั้นทำให้การทำสำนวนในชั้นสอบสวนเพื่อส่งไปยังอัยการจึงเป็นเรื่องยากลำบาก บางคดีกว่าเรื่องจะถึงอัยการใช้เวลาถึง 4 ปี[27] ซึ่งเกิดจากการขาดองค์ความรู้การจัดการในเรื่องดังกล่าวของเจ้าหน้าที่เอง

หากมองพิศวาสอาชญากรรมตามกรอบทฤษฎีปีระมิดของกฎหมายละเมิด (Pyramid of Tort Law) ของ Professor Dr. David M. Engel นั้นจะเห็นได้ว่าอุปสรรคและต้นทุนในการใช้กระบวนการยุติธรรมข้างต้นนั้นทำให้กรณีพิศวาสอาชญากรรมไม่ถึง 10% ที่คดีเหล่านี้จะผ่านจากชั้นตำรวจไปถึงอัยการ และมีเพียง 2% เท่านั้นที่จะรอดไปถึงศาลทำให้เหยื่อตัดสินใจไม่เข้าร้องทุกข์หรือยุติการดำเนินคดีไปเสียกลางคัน[28] อีกทั้งด้วยกรอบคิดทางวัฒนธรรมจารีตสังคมไทยเดิมที่ทำให้คนคิดว่าเรื่อง “ความสัมพันธ์รักใคร่” เป็นเรื่องส่วนตัวไม่ควรแสดงออกและพึงรักษากริยาอาการสงวนท่าที ซ้ำร้ายหากต้องการมีคู่เป็นชาวต่างชาติ สังคมก็จะตีตราว่าอยากได้สามีฝรั่ง[29] ส่งผลให้เหยื่อหลายคนมองว่าการถูกให้หลอกรักเป็นเรื่องน่าอายแล้ว ทั้งยังถูกหลอกให้เสียทรัพย์กับคนที่ตนคิดว่าเป็น “คนรัก” นั้นยิ่งน่าอับอายมากกว่า อีกทั้งยังไม่ได้รับความเข้าใจและความเห็นใจจากคนรอบข้าง และคิดว่าสิ่งที่เกิดขึ้นเป็นเวรกรรม ทำให้เหยื่อหลายคนไม่กล้าแจ้ง

---

[26] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่2) 2560 มาตรา 26

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มบริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร เมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรนี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

[27] อัยการ สัมภาษณ์เมื่อวันที่ 16 มกราคม 2562 ณ สำนักงานอัยการสูงสุด

[28] เรื่องเดียวกัน

[29] วันดี สันติวุฒิเมธี, “มองทะลุม่านมายาคติ “หญิงไทยกับสามีฝรั่ง”: เมื่อสิ่งที่เห็น อาจไม่ใช่สิ่งที่เป็น,” The 101 World, สืบค้นเมื่อวันที่ 4 เมษายน 2562, https://www.the101.world/the-myth-of-thai-wifeand-her-foreign-husband/

ความเพื่อดำเนินคดีกับผู้กระทำความผิด เช่นเดียวกับการศึกษาของ Monica Whitty[30] พบว่ามีเหยื่อเพียง 10% เท่านั้นที่มีการแจ้งความ ส่วนหนึ่งเป็นเพราะอับอายและลำบากใจเมื่อทราบว่าตนเองตกเป็นเหยื่อของการหลอกลวงนี้ ประกอบกับขาดความรู้เกี่ยวกับขั้นตอน และสถานที่ของการแจ้งความเมื่อถูกหลอกลวง และเข้าใจว่าการแจ้งความไม่ได้เกิดประโยชน์ใดเพราะไม่น่าจะดำเนินคดีกับอาชญากรได้

5. ปฏิบัติการจากลูกแกะสู่พญาราชสีห์

เหตุผลส่วนหนึ่งของการเกิดชุมชนออนไลน์ทั้งในและต่างประเทศ เพื่อเตือนภัยและโต้กลับเหล่านักต้มตุ๋นนั้นเกิดจากการถูกเพิกเฉยจากรัฐ เพราะรัฐมองว่าการสูญเงินของเหยื่อเหล่านี้เป็นการให้โดยเสน่ห์หา อีกทั้งพฤติการณ์ที่เป็นอาชญากรรมข้ามชาตินั้นยากเกินกว่าจะหาต้นต่อและตัวผู้กระทำความผิดมาดำเนินคดี รวมทั้งการชดใช้ค่าเสียหาย ดังนั้นการรวมกลุ่มกันของผู้ที่เคยตกเป็นเหยื่อนี้นับเป็นอีกวิธีหนึ่งที่อาจมีส่วนช่วยให้ผู้ที่มีความเสี่ยงและหน่วยงานรัฐตระหนักถึงภัยเงียบนี้ ในประเทศไทยมีเพจใน Facebook ที่ชื่อว่า “ภัยผู้หญิงในโลกออนไลน์” โดยกิจกรรมหลักของเพจนี้มีดังนี้

(1) กระจายข้อมูลรอบด้านเกี่ยวกับ Romance Scam ให้แก่ประชาชน และผู้ที่สนใจประเด็นดังกล่าว อาทิ การอัพเดทข่าวสารการหลอกลวงที่เกิดขึ้นประจำวัน การให้ข้อมูลกลยุทธ์การหลอกลวง การเตือนภัยและแจ้งข้อมูลโปรไฟล์ปลอม รวมถึงชี้แนะวิธีการตรวจสอบโปรไฟล์ปลอม เป็นต้น

(2) เป็นเสมือนแหล่งรวบรวมข้อมูลของโปรไฟล์ปลอมที่นักต้มตุ๋นสร้างขึ้น โดยเฉพาะโปรไฟล์ที่อยู่ใน Facebook เพื่อให้คนทั่วไปสามารถตรวจสอบได้จากข้อมูลที่ผู้ดูแลเพจฯ อัพเดทอย่างต่อเนื่อง รวมทั้งส่งข้อความเตือนบุคคลที่เป็นเพื่อนกับโปรไฟล์ปลอมทั้งหลาย เพื่อมิให้คนเหล่านั้นตกเป็นเหยื่อ และเป็นผู้แจ้งรายงานโปรไฟล์ปลอมแก่เว็บไซต์ Facebook

(3) ให้คำปรึกษากับผู้ที่ต้องการความช่วยเหลือเกี่ยวกับพิศวาสอาชญากรรม โดยเฉพาะการรับมือกับสถานการณ์ที่เกิดขึ้น เพราะเหยื่อหลายคนไม่ทราบว่าต้องทำอย่างไรต่อไปเมื่อตระหนักได้ว่าตนถูกหลอก โดยผู้ดูแลเพจฯ จะคอยอธิบายขั้นตอนรูปแบบการหลอกลวง และสิ่งที่

[30] Whitty Monica T, “Mass-Marketing Fraud: A Growing Concern,” *IEEE Security & Privacy* 13, no. 4 (2015): 84-87.

จะเกิดขึ้นต่อไป แนะนำการปฏิบัติตนเพื่อไม่ให้เหยื่อสูญเสียทรัพย์สินเพิ่มไปมากกว่านี้ เช่น มีผู้ให้เลขที่บัญชี หรือรูปถ่ายบัตรประชาชนแก่ “คู่รัก” (นักต้มตุ๋น) และกังวลว่าตนจะสูญเงินในบัญชี รวมถึงกลายเป็นส่วนหนึ่งของขบวนการอาชญากรรมด้วยความรู้เท่าไม่ถึงการณ์ ดังนั้นผู้ดูแลเพจฯ จะคอยแนะนำเหยื่อว่าควรทำอย่างไรบ้าง (ปิดบัญชี แจ้งความ) เป็นต้น อีกทั้งในกรณีที่ผู้เสียหายโอนเงินไปแล้วผู้ดูแลเพจฯ จะช่วยในขั้นตอนการเตรียมเอกสารเพื่อแจ้งความ บอกสถานที่แจ้งความ และพาผู้เสียหายไปแจ้งความ (หากผู้เสียหายต้องการ)

(4) เป็นตัวกลางในการเชื่อมต่อระหว่างผู้เสียหายกับภาครัฐ ทั้งการหาข้อมูลของนักต้มตุ๋น เช่น ส่งข้อมูลเลขที่บัญชีของนักต้มตุ๋นให้กับกรมสอบสวนคดีพิเศษ (DSI) และตำรวจท่องเที่ยว เพื่อขยายผลต่อไป รวมถึงการติดตามผู้เสียหายในกรณีที่ภาครัฐจับตัวผู้กระทำความผิดได้แต่ไม่สามารถติดต่อผู้เสียหายได้

(5) เหล่าสมาชิกในเพจนี้จะร่วมมือกัน “โต้กลับ” ด้วยการหลอกเอาข้อมูลเลขบัญชีของผู้รับโอนเงิน และเบอร์โทรศัพท์นักต้มตุ๋น เมื่อหลายคนทราบว่าตนเองถูกหลอกก็จะพยายามคุยกับนักต้มตุ๋นไปเรื่อยๆ เพื่อเก็บข้อมูลของคนคนนั้นให้มากที่สุด และบางครั้งสมาชิกในเพจก็แสร้งว่าเป็นเหยื่อเพื่อหลอกเอาข้อมูลจากเหล่าอาชญากรเหล่านั้น ซึ่งข้อมูลต่างๆ จะถูกส่งต่อให้กับเจ้าหน้าที่รัฐเพื่อทำการสืบสวนและจับกุมต่อไป

ข้อมูลต่างๆ ภายในเพจนั้นส่วนใหญ่ได้มาจากการเก็บรวบรวมเรื่องราวเกี่ยวกับพิศวาสอาชญากรรมของทีม “ภัยผู้หญิงในโลกออนไลน์” และได้รับการแบ่งปันข้อมูลจากบรรดาเหยื่อที่ถูกหลอกและติดตามเพจดังกล่าว หรือที่เรียกกันว่า “ลูกเพจ” ในปีพ.ศ. 2560-2561 มีเหยื่อที่ติดต่อให้ข้อมูลและขอความช่วยเหลือจากเพจดังกล่าวมากกว่า 300 คน[31] จากความพยายามและความร่วมมือกันทั้งหลายเหล่านี้นำไปสู่การจับกุมผู้ร่วมกระทำผิดในประเทศอยู่หลายคดี แม้ว่าจะไม่สามารถขยายผลไปถึงนักต้มตุ๋นผู้ที่ทำการพูดคุยกับเหยื่อ แต่สามารถจับกุมผู้ร่วมขบวนได้ เช่น ผู้เปิดบัญชีรับเงิน ผู้โทรศัพท์แจ้ง และผู้ถอนเงินออกจากบัญชี เป็นต้น

การรวมกลุ่มรูปแบบดังกล่าวเกิดขึ้นในต่างประเทศเช่นกัน งานวิจัยของ Andreas Zingerle และ Linda Kronman[32] ระบุว่ามีกลุ่มที่ชื่อ “Scambaiters” ซึ่งเป็นชุมชนออนไลน์ที่

[31] ผู้ดูแลเพจภัยผู้หญิงออนไลน์ สัมภาษณ์เมื่อวันที่ 17 มกราคม 2562 ณ เซ็นทรัลปิ่นเกล้า

[32] Zingerle Andreas and Linda Kronman, “Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud,” In *2013 International Conference on Cyberworlds*, (2013): 352-55.

ตั้งขึ้นเพื่อโต้กลับกลุ่ม พิศวาสอาชญากรรมเสมือนเป็นศาลเตี้ยที่มีการให้ข้อมูลและเฝ้าระวังภัยการหลอกลวงในโลกอินเตอร์เน็ตโดยเฉพาะคดีพิศวาสอาชญากรรม ซึ่งดำเนินการภายใต้เว็บไซต์ 2 เว็บ คือ 419eater.com และ thescambaiter.com โดยสมาชิกกลุ่มจะช่วยกันตรวจสอบและสืบหาอีเมลหลอกลวง และใช้เทคนิควิศวกรรมสังคม (Social Engineering) อันเกิดจากการนำเอาความรู้ทาง จิตวิทยา สังคมศาสตร์ รัฐศาสตร์ วิทยาศาสตร์คอมพิวเตอร์ รวมไปถึงการศึกษา การออกแบบการแก้ไข และการวางแผนพฤติกรรมมนุษย์มาประยุกต์ใช้ เพื่อให้ได้มาซึ่งข้อมูลที่สามารถใช้รายงานหรือเตือนผู้ที่อาจตกเป็นเหยื่อได้ การทำงานหลักๆ ของกลุ่มนี้มีอยู่ 7 สิ่งสำคัญดังนี้

(1) The Scam Alerters เป็นการระบุและรายงานการหลอกลวงออนไลน์ เพื่อเพิ่มการตระหนักรู้โดยทั่วไปถึงการหลอกลวงทางอินเตอร์เน็ต พวกเขาจะเตือนทั้งแบบรายบุคคลและเป็นกลุ่มแก่ผู้ที่เสี่ยงต่อการหลอกลวงด้วยการให้ข้อมูลที่มีรายละเอียดและเชื่อถือได้ ผ่านช่องทางเว็บไซต์และฟอรัม (Forum) หลายแห่งที่คอยให้ข้อมูลผู้ที่จะตกเป็นเหยื่อ เช่น romancescam.com (เน้นเฉพาะเรื่องหลอกลวงรักออนไลน์) scamvictimsunited.com (ดูแลเหยื่อของการฉ้อโกง) scamwarners.com และ 419eater.com หลายๆ ฟอรัมทำหน้าที่เป็นแพลตฟอร์มในการตรวจและหารือเกี่ยวกับอีเมลไม่พึงประสงค์ต่างๆ ผลก็คือ ทำให้ผู้ที่อาจตกเป็นเหยื่อหลายคนได้รับแจ้งเตือนเกี่ยวกับการหลอกลวงรูปแบบใหม่ๆ และเตือนให้ระวังอีเมลที่ยื่นข้อเสนอที่ดีเกินกว่าจะเป็นจริงได้ และสำหรับผู้ที่เคยตกเป็นเหยื่อแพลตฟอร์มนี้จะให้ข้อมูลเกี่ยวกับคำถามที่พบบ่อยและคำแนะนำเพิ่มเติม

(2) The Trophy Hunters เป็นอีกกิจกรรมหนึ่งที่กลุ่ม Scambaiters จะเป็นผู้ตอบกลับอีเมลหลอกลวงโดยทราบว่า scammer เป็นผู้เขียนอีเมลนั้น พวกเขาจะใช้กลลวงต่างๆ ตลบหลังเหล่านักต้มตุ๋น ให้เหมือนว่าพวกเขาเป็นเหยื่อจริงๆ เพื่อล่อเอาข้อมูลต่างๆ จากนักต้มตุ๋น ไม่ว่าจะเป็นรูปภาพ ข้อความการสนทนา เสียง หรือวิดีโอ เพื่อใช้เป็นหลักฐาน

(3) The Website Reporters ซึ่งมีหน้าที่ตรวจสอบเว็บไซต์ที่นักต้มตุ๋นปลอมขึ้นมาเพื่อให้ตนเองดูเป็นมืออาชีพ และดูน่าเชื่อถือว่าเว็บไซต์ที่อ้างนั้นมีตัวตนจริง เช่น บริษัท เว็บขายของออนไลน์ ธนาคาร องค์กรการกุศล กลุ่มศาสนา หรือบริษัท IT เป็นต้น โดยพวกเขาจะพิสูจน์เว็บไซต์เหล่านี้ด้วยการเชื่อมโยงรายการ DNS[33] กับฐานข้อมูลผู้หลอกลวง จากนั้นจะทำการบันทึก

[33] Domain Name System หรือ Domain Name Server คือ ระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม (Domain Name) และทำหน้าที่ในการแปลงชื่อโดเมนเนมดังกล่าวเป็นหมายเลขไอพีแอดเดรส

กิจกรรมที่ผิดกฎหมายและรายงานการค้นพบดังกล่าวไปยังผู้ให้บริการ (Hosting Provider) เพื่อนำเว็บไซต์ดังกล่าวออกหรือสกัดกั้นเว็บนั้นไป 'artist against 419' (AA419) ริเริ่มขึ้นเมื่อปี 2003 เป็นชุมชนอินเตอร์เน็ตที่ใหญ่ที่สุดในโลกที่อุทิศตนเพื่อหยุดกิจกรรมหลอกลวงเหล่านี้และมีฐานข้อมูลเกี่ยวกับการฉ้อโกงบนเว็บไซต์มากที่สุด และในปี 2007 กลุ่ม AA419 ได้ร่วมมือกับหน่วยตำรวจเพื่อแจ้งการฉ้อโกงในเขตกรุงลอนดอน

(4) The Bank Guards เป็นหน้าที่ของสมาชิกกลุ่ม Scambaiters บางคนที่มีความเชี่ยวชาญพิเศษในการสังเกตและรายงานบัญชีธนาคารปลอม หรือบัญชีที่มีเงินเข้าออกมากอย่างผิดสังเกต เพราะเชื่อว่านักต้มตุ๋นยอมเสียเงินอย่างถูกกฎหมายเพื่อจัดการกับบัญชีเหล่านี้ หรือบางครั้งหลอกให้เหยื่อเปิดบัญชีเพื่อรับเงินโอน พวกเขาจะเก็บข้อมูลและรายงานอาชญากรรมดังกล่าวต่อเจ้าหน้าที่ธนาคารให้ทำการอายัดบัญชีและดำเนินการตามกฎหมาย

(5) The Romance Scam Seekers โดยปกติพวก Scammer มักสร้างโปรไฟล์ปลอมเพื่อหาเหยื่อทั้งชาย และหญิงในเว็บหาคู่ ซึ่งกลุ่ม Scambaiters จะเฝ้าระวังและสอดส่องในเว็บไซต์หาคู่ต่างๆ เพื่อเตือนผู้ที่อาจตกเป็นเหยื่อ หรือเหยื่อ บางครั้งแกล้งเป็นเหยื่อเพื่อให้นักต้มตุ๋นส่งข้อมูลต่างๆ มาให้ และเก็บรูปภาพและรวบรวมคำพูดหวานๆ ที่ Scammer ใช้เป็นประจำเพื่อจัดทำเอกสารชี้แจงแนวทางปฏิบัติของกลุ่ม Scammer และโพสเตือนคนอื่นๆ ในฟอรัม เช่น scamdigger.com หรือทำเป็นหนังสือเล่มเล็กๆ ชื่อ 'Hello Sweaty' เป็นต้น นอกจากนั้นยังพยายามกีดกันนักต้มตุ๋นออกจากเว็บหาคู่

(6) The Safari Agents เป็นทีมที่คอยพยายามล่อให้พวกนักต้มตุ๋นออกมาจากพื้นที่ทำงานของตนเอง โดยการแสร้งว่าทีม Scambaiters เป็นเหยื่อและจะไปเที่ยวแถบใกล้ๆ กับไนจีเรีย และพักอยู่โรงแรมแถวนั้น จากนั้นจะหว่านล้อมให้นักต้มตุ๋นออกมาเจอที่โรงแรม ผ่านการใช้เว็บไซต์ safarihotelsgroup.com (เป็นเว็บไซต์ของกลุ่ม Scambaiters ที่อ้างว่าเป็นตัวแทนธุรกิจขนาดเล็กที่ดำเนินกิจการแบบครอบครัว และมีเครือข่ายโรงแรมราคาประหยัดในแอฟริกาตะวันตก) พวกเขาใช้เว็บโรงแรมเป็นเครื่องมือล่อเพื่อดักจับนักต้มตุ๋น และทำให้เชื่อว่ามีเหยื่ออยู่ที่โรงแรมนั้นจริงๆ

(IP Address) เพื่อนำหมายเลขไอพีดังกล่าวไปติดต่อยัง Sever อื่น ๆ ที่ต้องการต่างๆ

(7) The Inbox Divers จะเป็นทีมที่สามารถเข้าถึงข้อมูลบัญชีอีเมลของเหล่านักต้มตุ๋นและผู้อาจตกเป็นเหยื่อได้ไม่ว่าจะด้วยวิธีใดก็ตาม ทั้งนี้ทำหน้าที่เข้าไปเก็บข้อมูลการสนทนาต่างๆ และส่งข้อความเตือนทั้งผู้อาจตกเป็นเหยื่อและเหยื่อว่า *“คุณกำลังถูกหลอกจากบุคคลเหล่านี้”*

อย่างไรก็ตามการปฏิบัติการที่ไม่ได้อยู่ภายใต้การดูแล และคุ้มครองของรัฐนั้นมีความลำบากอยู่มากพอสมควร อาทิ ในประเทศไทย เพจที่ตั้งขึ้นเพื่อใช้โต้กลับเหล่าอาชญากรรม ถูกรายงานจนต้องปิดเพจไปหลายครั้ง และต้องเริ่มนับหนึ่งใหม่ทุกครั้งที่เริ่มเปิดเพจใหม่ ทำให้การกระจายข่าวสารไม่ต่อเนื่อง และขาดการติดต่อกับคนที่ต้องการความช่วยเหลือ ปัจจุบันเพจ “ภัยผู้หญิงในโลกออนไลน์” เปลี่ยนชื่อเป็น “ภัยผู้หญิงในโลกออนไลน์ 2” และยังคงทำกิจกรรมอย่างต่อเนื่อง ส่วนกิจกรรมที่เกิดในต่างประเทศ เช่น การล่อนักต้มตุ๋นออกมาพบกับทีม Scambaiters และการแฮกข้อมูล โดยไม่ได้อยู่ภายใต้การคุ้มครองของเจ้าหน้าที่รัฐย่อมก่อให้เกิดการเผชิญกับความเสี่ยงอันตรายต่างๆ อย่างไม่จำเป็น

6. ความพยายามในการหามาตรการแก้ไขของรัฐ

หากกล่าวถึงมูลค่าความเสียหายทางการเงินที่สูงลิบลิ่วต่อจำนวนผู้เสียหายในหลายประเทศ เช่น ประเทศสิงคโปร์มีคดีสูญเงินไปกว่า 2.4 ล้านดอลลาร์สิงคโปร์ (ประมาณ 53,235,600 บาท) จากเหยื่อเพียงหนึ่งคน [34] และในประเทศไทยมีผู้โอนเงินไป 26 ครั้งรวมกว่า 33 ล้านบาทจากเหยื่อเพียงหนึ่งคนเช่นกัน[35] ความเสียหายทางการเงินนี้ทำให้ต่างประเทศมีความตระหนักปัญหาดังกล่าว

ในปีค.ศ. 2012-2013 ตำรวจนครบาลสหราชอาณาจักร ได้พยายามจัดการป้องกันปัญหาดังกล่าวโดยการจัดอบรมหลักสูตร “London City Police National Fraud Course”[36] ซึ่งเป็น

---

[34] Nabilah Awang, “Internet love scammers target those who are emotionally vulnerable, say police,” Today, accessed September 15, 2019, https://www.todayonline.com/singapore/internet-love-scammers-reap-surging-sums-they-target-vulnerable-police.

[35] Rabbit finance Magazine, “Romance Scam หลอกรักออนไลน์ ภัยร้ายของสาวโสด!,” Rabbit finance Magazine, สืบค้นเมื่อวันที่ 25 พฤศจิกายน 2561, https://finance.rabbit.co.th/blog/romance-scam-and-single-ladies.

[36] Research Excellence Framework 2014. “Confronting online dating scams: working with police and the industry.” 36 Communication Cultural and Media Studies. (University of Leicester, 2014)

หลักสูตรเข้มข้น 3 สัปดาห์ ด้วยการฝึกตำรวจ 30-50 คน ให้สามารถจัดการและรับมือกับคดีการหลอกลวงหลายรูปแบบในอินเตอร์เน็ต การฝึกแบ่งออกเป็น 2 ช่วงคือ การอบรม และการให้คำแนะนำเกี่ยววิธีการที่ดีกว่าที่ตำรวจต้องใช้จัดการกับผู้ที่ตกเป็นเหยื่อของ Romance Scams เช่น การพิจารณาถึงผลกระทบที่จะตามมา, ผลกระทบทางจิตใจ และการกลับไปเป็นเหยื่อซ้ำแล้วซ้ำเล่า โดยมีผู้เชี่ยวชาญด้านดังกล่าวคือ Monica T. Whitty ได้แนะนำทางที่ดีที่สุดของการสืบสวนสอบสวนเหยื่อ และการให้การสนับสนุนอย่างต่อเนื่องสำหรับการดำเนินคดีอาญาระหว่างประเทศ Monica กล่าวว่า *"เหยื่อมักให้การปฏิเสธในขั้นต้น และต้องการกำลังใจที่จะยอมรับว่าความสัมพันธ์ของพวกเขาเป็นเรื่องที่หลอกลวง นอกจากนั้นเหยื่อยังต้องการการสนับสนุนจากครอบครัวแต่พวกเขาไม่เคยได้รับเลย"*[37] Monica T. Whitty ร่วมกับหน่วยงานอาชญากรรมร้ายแรงแห่งสหราชอาณาจักร (SOCA) ส่งจดหมายถึงเหยื่อ 50 ราย ในละเวกนั้นเพื่อหวังว่าจะขัดขวางไม่ให้พวกเหยื่อโอนเงินให้กับ Scammer และออกทีวี และวิทยุเพื่อเตือนให้ประชาชนตระหนักถึงภัยดังกล่าว นอกจากนั้นยังร่วมกันเตรียมความพร้อมของเหยื่อพิศวาสอาชญากรรมเมื่อต้องขึ้นศาลในประเทศกานา และเตรียมหลักฐานงานวิจัยต่างๆ เพื่อต่อสู้กับข้อโต้แย้งของอาชญากรที่ว่า "เหยื่อมีความบกพร่องทางจิต" สิ่งที่เกิดขึ้นไม่ใช่การกระทำความผิดกฎหมายของเหล่าอาชญากร อีกทั้งมีการจัดตั้งหน่วย Establishment of the Economic Crime Unit ขึ้นเมื่อปี ค.ศ. 2012 ตามคำแนะนำของนักวิชาการในมหาวิทยาลัยสหราชอาณาจักร เพื่อให้ผู้บังคับใช้กฎหมายเข้าใจถึงความสูญเสียของผู้ที่ตกเป็นเหยื่อ ซึ่งนำไปสู่การชดใช้ความเสียหายอย่างแท้จริง รวมถึงหน่วยงาน International Mass Marketing Fraud Working Group ซึ่งเป็นการรวมกลุ่มของตัวแทนหน่วยงานบังคับใช้กฎหมายทั่วโลก เพื่อแลกเปลี่ยนข้อมูลและกลยุทธ์ในการป้องกันเรื่องดังกล่าว เช่น Serious Organised Crime Agency, FBI, Federal Trade Authority, Secret Service, the Royal Canadian Mounted Police, Netherlands Police, the Queensland Police, Ghanaian police and Nigerian Police เป็นต้น

ล่าสุดสำนักงานตำรวจของสิงคโปร์ได้จัดตั้งศูนย์ Anti-Scam (Anti-Scam Centre) ขึ้นเมื่อเดือนมิถุนายน ค.ศ. 2019 เพื่อรับมือ และจัดการปัญหาของนักต้มตุ๋นเหล่านี้ ด้วยความร่วมมือระหว่างกองกำลังตำรวจสิงคโปร์ (The Singapore Police Force) กับธนาคารใหญ่ 3 แห่ง คือ DBS, OCBC และ United Overseas Bank ภายใต้ศูนย์ฯ ธนาคารสามารถระงับบัญชีที่ต้องสงสัย

[37] เรื่องเดียวกัน

ได้ภายใน 2-3 วัน (ซึ่งก่อนหน้านี้ต้องใช้เวลาดำเนินการถึง 2 สัปดาห์) ผลจากมาตรการดังกล่าวทำให้บัญชีธนาคาร 815 บัญชีที่เชื่อมโยงกับการหลอกลวงถูกระงับและกู้เงินคืนมาได้กว่า 850,000 ดอลลาร์สิงคโปร์ หรือคิดเป็น 35% ของจำนวนเงินกว่า 2.4 ล้านดอลลาร์สิงคโปร์ อีกทั้งยังมีการร่วมมือกับบริษัทโทรคมนาคมยักษ์ใหญ่ในสิงคโปร์ โดยส่งการแจ้งเตือนไปทันทีเพื่อให้ยุติสายโทรศัพท์ของนักต้มตุ๋น (Scammer) ศูนย์ดังกล่าวได้เรียนรู้จากกรณีศึกษาที่คล้ายคลึงกัน และการแก้ปัญหาจากหลายประเทศ เช่น แคนาดา จีน ไต้หวัน และฮ่องกง[38-39]

ไม่เพียงแต่การตื่นตัวของเหล่าประเทศที่ประชาชนได้รับผลกระทบจากความสูญเสียของอาชญากรรมหลอกลวงรักออนไลน์เท่านั้น แต่เริ่มมีการจัดการปัญหาจากประเทศที่กล่าวได้ว่าเป็นจุดพักพิงและรวมกลุ่มเพื่อก่ออาชญากรรมการหลอกลวงรักในโลกออนไลน์ด้วย ในบทความวิจัยของ Ahmad Safwan Hamsi และคณะ[40] แสดงให้เห็นว่า ประเทศมาเลเซียได้มีการศึกษาวิจัยถึงช่องโหว่ของนโยบายในประเทศที่เอื้อให้เกิดการใช้พื้นที่เพื่อก่ออาชญากรรม และจัดการกับ 5 ประเด็นปัญหา ดังนี้ **1. การใช้วีซ่านักเรียนผิดวัตถุประสงค์** ถือเป็นช่องโหว่หลักจากนโยบายการเป็นศูนย์กลางของการศึกษาโลกของมาเลเซียที่เปิดรับผู้คนจากนานาประเทศด้วยการให้วีซ่านักเรียนเป็นจำนวนมาก ทำให้คนไนจีเรียเข้าประเทศด้วยวีซ่านักเรียนคิดเป็น 8% ผู้วิจัยจึงเสนอให้สถานทูตควรร่วมมืออย่างใกล้ชิดกับตำรวจมาเลเซียและหน่วยงานตรวจคนเข้าเมืองเพื่อรายงานสถานะของนักเรียน และอัพเดทข้อมูลให้ทันสมัยอยู่เสมอ ทำให้ในปี ค.ศ. 2013 กระทรวงศึกษาธิการได้เข้ามามีส่วนร่วมในการจัดการเรื่องนี้โดยเริ่มมีการตรวจสอบและติดตามนักเรียน/นักศึกษาต่างประเทศให้เข้มงวดมากขึ้นกว่าเดิม[41] **2. ข้อบกพร่องของระบบธนาคาร** เกิด

[38] Charmaine Ng, “Police set up anti-scam centre, suspicious bank accounts can now be frozen in a few days,” The Straitstimes, accessed September 5, 2019, https://www.straitstimes.com/singapore/courts-crime/police-sets-up-anti-scam-centre-working-with-banks-to-disrupt-scammers.

[39] Nabilah Awang, “Internet love scammers target those who are emotionally vulnerable, say police,” Today, accessed September 15, 2019, https://www.todayonline.com/singapore/internet-love-scammers-reap-surging-sums-they-target-vulnerable-police.

[40] Hamsi Ahmad Safwan, et al. “Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem,” *Journal of Management Research*, 7 No. 2 (2015): 169-181.

[41] Reauters, “US: American women targeted as Malaysia becomes Internet scam haven,”

จากการเปิดบัญชีทำได้ง่ายๆ โดยการทำธุรกรรมออนไลน์ ซึ่งอาชญากรอาจขโมยข้อมูลส่วนบุคคลของเหยื่อเพื่อใช้การยืนยันตัวตน เช่น เลขบัตรประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลทางการเงินอื่นๆ เป็นต้น ซึ่งมาเลเซียได้พยายามแก้ปัญหาด้วยการใช้เทคโนโลยีไบโอเมตริก (Biometrics) เพื่อยืนยันตัวตนของระบบธนาคาร สำนักข่าว The Associated Press รายงานว่ามีการพัฒนาใช้การตรวจจับเสียง (Speaker Recognition) ในธนาคารเพื่อตรวจจับอาชญากรและปกป้องผู้บริโภค ด้วยการใช้กรองเสียงระหว่างการพูดคุยโทรศัพท์กับธนาคาร โดยระบบจะทำการจับคู่กับเสียงของอาชญากรที่มีอยู่ในระบบ **3. การแก้ไขพระราชบัญญัติกฎหมายไซเบอร์ในปัจจุบัน** ซึ่งประเด็นนี้ต้องยอมรับก่อนว่าตำรวจมาเลเซียยังขาดแคลนทรัพยากรและผู้เชี่ยวชาญในการรับมือกับปัญหาดังกล่าว และยังปล่อยให้มีการฟ้องร้องคดีทางอาญาอยู่เป็นจำนวนมาก ดังนั้นรัฐบาลมาเลเซียจึงได้เพิ่มเติมกฎหมายหลายฉบับเพื่อจัดการกับอาชญากรรมไซเบอร์ โดยกำหนดฐานความผิดเกี่ยวกับกระทำผิดโดยคอมพิวเตอร์เพิ่มเติม **4. เว็บเดท/เว็บหาคู่ เครือข่ายสังคมออนไลน์** Scammer ส่วนใหญ่มักใช้ช่วงเวลาที่เหยื่ออ่อนแอและกำลังมองหารักแท้ในโลกออนไลน์ในการขโมยข้อมูลส่วนตัวหรือหลอกลวงเหยื่อ ดังนั้นควรเริ่มจากผู้ใช้บริการเองด้วยการป้องกันตนเองให้พ้นจากกลุ่มอาชญากร ด้วยการหลีกเลี่ยงการเปิดเผยความลับที่เป็นข้อมูลส่วนบุคคลทั้งหลายในช่วงระยะแรกที่สนทนากัน เช่น ไม่ควรเปิดเผยข้อมูลทุกอย่างในโปรไฟล์ ตรวจสอบประวัติของคู่สนทนาให้แน่ชัด ระวังการให้ความช่วยเหลือทางการเงินทุกชนิด สร้างรหัสผ่านให้รัดกุม จำไว้เสมอว่าต้องแยกแยะระหว่างความรักและการเงินออกจากกัน และหากรู้ตัวหรือสงสัยว่ากำลังถูกหลอกให้รีบแจ้งความ/ร้องทุกข์โดยเร็วที่สุด นอกจากนั้นในมาเลเซียมีหน่วยงานเฉพาะที่สืบสวนเกี่ยวกับเรื่องนี้คือ Bukit Aman Commercial Crime Investigations Department (CCID) **5. การควบคุมสถานการณ์ของรัฐบาล** โดย Hamsi มองว่าเรื่องดังกล่าวรัฐบาลไม่สามารถเข้าไปจัดการและควบคุมได้ เนื่องจากการใช้งานอินเตอร์เน็ตเป็นสิ่งที่ควบคุมได้ยากและเกินความรับผิดชอบของรัฐบาล ดังนั้นเขาจึงเสนอทางออกว่าควรให้มีการจำกัดการใช้งานบนโลกออนไลน์เช่นเดียวกับประเทศจีนเพื่อเป็นระบบคัดกรองและควบคุมปัญหาอาชญากรรมดังกล่าว

The Star Online, accessed October 25, 2018, http://www.thestar.com.my/News/Nation/2014/07/09/Internet-scam-US-women-Nigerians-Malaysia.

สำหรับในประเทศไทยมีความพยายามในการจัดการกรณีดังกล่าวเช่นกัน ด้วยการเพิ่มภารกิจด้านการปราบปรามให้กับหน่วยงานต่างๆ เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) (TCSD) ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) และกองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ เป็นต้น ทั้งนี้การเพิ่มภารกิจ แต่ไม่มีการเพิ่มทรัพยากรทั้งงบประมาณ อุปกรณ์ บุคลากร และองค์ความรู้ย่อมเป็นเรื่องยากลำบากจะบริหารจัดการปัญหาเหล่านี้อย่างมีประสิทธิภาพ อันเป็นข้อจำกัดของกระบวนการยุติธรรมที่ต้องได้รับการแก้ไขปรับปรุง

บทส่งท้าย

การปราบปรามการหลอกลวงในโลกไซเบอร์เป็นเรื่องที่มีความยุ่งยากอยู่มากจากข้อจำกัดของกระบวนการยุติธรรมแบบรัฐสมัยใหม่ ไม่ว่าจะโดยการจับกุม หรือการดำเนินคดี เนื่องจากอาชญากรมักเป็นชาวต่างชาติที่อยู่คนละประเทศกับเหยื่อ อีกทั้งการติดตามสืบสวนทางไซเบอร์เป็นเรื่องที่ยากและใช้เวลานานพอสมควร แม้ว่าจะมีความพยายามในการบังคับใช้กฎหมาย เช่น พยายามที่จะกำหนดให้มีการเปลี่ยนแปลงวิธีการโอนเงินให้รัดกุมมากยิ่งขึ้นผ่านบริษัทต่างๆ เช่น Western Union และ MoneyGram เป็นต้น แต่ยังพบว่าอาชญากรที่มีทักษะสูงในการหาช่องโหว่ทางกฎหมายเพื่อทำหลอกลวงดังกล่าว ทั้งนี้ถือว่าการกระทำดังกล่าวเป็นการแก้ปัญหาที่ปลายเหตุ ดังนั้นจากวลีที่ว่า *“การป้องกันอันตรายคือการเอาตัวออกห่างจากอันตราย”* น่าจะเป็นทางออกที่ดีสำหรับเรื่องดังกล่าว ด้วยการสร้างความตระหนักรู้ให้กับประชาชนให้ทราบว่าสิ่งนี้เป็นอันตราย เพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อ อีกทั้งควรมีการสร้างมาตรการป้องปรามด้วยความร่วมมือของผู้ดูแลระบบเครือข่ายออนไลน์ต่างๆ ด้วยการสร้างการรักษาความปลอดภัยในระบบ และแจ้งเตือนแก่ผู้ใช้งานเมื่อทราบว่าโปรไฟล์นั้นเป็นโปรไฟล์ปลอมเพื่อลดจำนวนโปรไฟล์ของอาชญากรในเว็บไซต์นั้น

References

ACCC. “Scam statistics: Dating & romance in 2018.” The Australian Competition and Consumer Commission. Accessed September 25, 2019. https://www.scam watch.gov.au/about-scamwatch/scam-statistics?scamid=13&date =2018.

Action Fraud. “Victims lost £41 million to romance fraud in 2017.” Action Fraud. Accessed November 17, 2018. https://www.actionfraud.police.uk/news/victims -lost-41-million-to-romance-fraud-in-2017.

Australian Competition and Consumer Commission (ACCC). “Dating and romance scams: Defining the harm” The Australian Competition and Consumer Commission. Accessed June 4, 2019. https://www.accc.gov.au/media-release/almost-90-million-reported-lost-to-scams-in-2013.

Charmaine Ng. “Police set up anti-scam centre, suspicious bank accounts can now be frozen in a few days.” The Straitstimes. Accessed September 5, 2019. https://www.straitstimes.com/singapore/courts-crime/police-sets-up-anti-scam-centre-working-with-banks-to-disrupt-scammers.

David Ludden. “Does using social media make you lonely?.” Psychology Today. Accessed November 26, 2018. https://www.psychologytoday.com/intl /blog/talking-apes/201801/does-usingsocial-media-make-you-lonely.

Eleanor Rose. “A global network of scammers is targeting older people—here’s how to avoid becoming a victim.” Accessed December 15, 2018. https://www.readersdigest.ca/home-garden/money/romance-scams-and-financial-fraud/.

Emma Fletcher. “Romance scams rank number one on total reported losses.” Federal Trade Commission. Accessed March 13, 2019. https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-lossesd.

Hamsi Ahmad Safwan, et al. “Cybercrime over internet love scams in Malaysia: a discussion on the theoretical perspectives, Connecting Factors and Keys to the Problem.” *Journal of Management Research* 7, no. 2 (2015): 169-181.

Int’l Mass-Marketing Fraud Working Group. “Mass-marketing fraud: a treat assessment.” Int’l Mass-Marketing Fraud Working Group. Accessed October 29, 2018. www.ice.gov/doclib/cornerstone/pdf/immfa.pdf.

Internet Crime Complaint Center. “Annual reports 2011-2014 internet crime report.” Internet Crime Complaint Center.

Internet Crime Complaint Center. “Annual reports 2014 internet crime report.” Internet Crime Complaint Center.

Lauren La Rose. “Online romance scam can hurt hearts and wallets.” The Canadian Press. Accessed Mar 7, 2019. http://www.thestar.com/life/2011/10/06/online_romance_scams_can_hurt_hearts_and_wallets.html.

Marketeer. “Lonely Marketing: ‘เหงา’ ที่แบรนด์ต้องช่วยเป็นเพื่อน.” Marketeer. สืบค้นเมื่อวันที่ 2 กันยายน 2562 https://marketeeronline.co/archives/105589.

Nabilah Awang. “Internet love scammers target those who are emotionally vulnerable, say police.” Today. Accessed September 15, 2019. https://www.todayonline.com/singapore/internet-love-scammers-reap-surging-sums-they-target-vulnerable-police.

Office of Fair Trading. “Helping People Affected by Scams: A Toolkit for Practitioners.” Office of Fair Trading. Accessed October 29, 2018. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/400585_OFT_Scams Toolkit_ful1.pdf.

Rabbit finance Magazine. “Romance Scam หลอกรักออนไลน์ ภัยร้ายของสาวโสด!.” Rabbit finance Magazine. สืบค้นเมื่อวันที่ 25 กันยายน 2561 https://finance.rabbit.co.th/blog/romance-scam-and-single-ladies.

Reauters. “US: American women targeted as Malaysia becomes Internet scam haven.” The Star Online. Accessed October 25, 2018. http://www.thestar.com.my/News/ Nation/2014/07/09/Internet-scam-US-women-Nigerians-Malaysia.

Research Excellence Framework 2014. “Confronting online dating scams: Working with police and the industry.” 36 Communication Cultural and Media Studies. University of Leicester, 2014.

The Hong Kong Police. “Snapshot of romance scam.” Hong Kong Police Force. Accessed January 22, 2019. https://www.police.gov.hk/info/img/cpb/adcc/180517_en.pdf.

The Irish Times. “Woman loses more than £300,000 in romance scam.” The Irish Times. Accessed June 23, 2019. https://www.irishtimes.com/news/ireland/irish-news/woman-loses-more-than-300-000-in-romance-scam-1.3934854.

Ting-Fang Yen, and Markus Jakobsson. “Case Study: Romance Scams.” In *Understanding Social Engineering Based Scams*, New York: Springer, 2016.

Wandi Santiwutthimathi. “มองทะลุม่านมายาคติ ‘หญิงไทยกับสามีฝรั่ง’: เมื่อสิ่งที่เห็น อาจไม่ใช่สิ่งที่เป็น.” *The 101 World,* สืบค้นเมื่อวันที่ 4 เมษายน 2562. https://www.the 101.world/the-myth-of-thai-wifeand-her-foreign-husband/.

Whitty Monica T. “Anatomy of the Online Dating Romance Scam.” *Security Journal* 28, No.4 (2015): 443-55.

Whitty Monica T. “Mass-Marketing Fraud: A Growing Concern.” *IEEE Security & Privacy* 13, No.4 (2015): 84-87.

Zingerle Andreas and Linda Kronman. “Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud.” In 2013 *International Conference on Cyberworlds*, 2013.

แนวหน้า. “ปปง.เผยตั้งศปก.ปปง. 1ปี พบเหยื่อคดีโรแมนซ์สแกน 332 ราย เสียหาย 193 ล้าน,” *แนวหน้า,* สืบค้นเมื่อวันที่ 31 พฤษภาคม 2562, https://www.naewna. com/local/417058.

ผู้จัดการออนไลน์. “ปปง.-สตม. ร่วมส่งมอบคืนเงินเหยื่อแก๊ง Romance Scam.” *ผู้จัดการออนไลน์,* 6 กันยายน 2561. สืบค้นเมื่อวันที่ 25 พฤศจิกายน 2561, https://mgronline.com/uptodate/ detail/9610000089364.