คำถาม - คำตอบเกี่ยวกับการบริการให้/ให้ยืมอุปกรณ์และเครื่องมือเทคโนโลยีสารสนเทศและการสื่อสารสำหรับคนพิการ

1. คำถาม : หากต้องการยืมหรือขออุปกรณ์สำหรับคนพิการต้องทำอย่างไร

คำตอบ : จะต้องยื่นแบบคำขอพร้อมเอกสาร ณ หน่วยงาน/จุดบริการรับแบบคำขอ โดยส่วนกลาง (กทม.) ณ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ส่วนภูมิภาค (ต่างจังหวัด) ณ สำนักงานสถิติจังหวัด หรือสำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์ทุกจังหวัด โดยต้องมีเอกสาร ดังนี้

(1) กรณีที่คนพิการยื่นเอง สำเนาบัตรประจำตัวคนพิการ (ออกโดยกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์) สำเนาทะเบียนบ้าน และสำเนาเอกสารการเปลี่ยนชื่อ (ถ้ามี)

(2) กรณีผู้ปกครอง ผู้พิทักษ์ ผู้อนุบาล หรือผู้ดูแลคนพิการ เป็นผู้ยื่นแบบคำขอแทนคนพิการ สำเนาบัตรประชาชน สำเนาทะเบียนบ้าน สำเนาเอกสารการเปลี่ยนชื่อ (ถ้ามี) ของคนพิการและผู้ยื่นคำขอแทน และหลักฐานแสดงว่าได้รับมอบอำนาจจากคนพิการ

ทั้งนี้ สามารถติดต่อสอบถามข้อมูลเพิ่มเติมได้ที่ เบอร์โทร 0 2142 1337 หรือ 0 2141 7042 ตลอดเวลาราชการ

2. คำถาม : ใครบ้างที่มีสิทธิขอหรือยืมอุปกรณ์ได้

คำตอบ : คนพิการ โดยแบ่งเป็น 7 ประเภท ได้แก่

1. ความพิการทางการมองเห็น
2. ความพิการทางการได้ยินและสื่อความหมาย
3. ความพิการทางการเคลื่อนไหวหรือทางร่างกาย
4. ความพิการทางจิตใจหรือพฤติกรรม
5. ความพิการทางสติปัญญา
6. ความพิการทางการเรียนรู้
7. ความพิการทางออทิสติก

3. คำถาม : อุปกรณ์ที่ให้/ให้ยืมมีอะไรบ้าง

คำตอบ : <u>รายการอุปกรณ์สำหรับการให้แบบไม่ต้องมีสัญญายืมหรือเสียค่าใช้จ่ายใดๆ ได้แก่</u>

1. โปรแกรมสำหรับแปลสื่อสิ่งพิมพ์เป็นอักษรเบรลล์ หรืออักษรเบรลล์เป็นสื่อสิ่งพิมพ์
2. โปรแกรมสำหรับแปลภาพเป็นอักษรและมีเสียงสังเคราะห์ฯ
3. โปรแกรมสำหรับขยายหน้าจอ
4. โปรแกรมสำหรับอ่านหนังสือ
5. โปรแกรมสำหรับช่วยในการพิมพ์
6. โปรแกรมพจนานุกรมสำหรับคนพิการ
7. โปรแกรมสำหรับมือถือเพื่ออำนวยความสะดวกในการสื่อสาร
8. เครื่องมือหรืออุปกรณ์ที่ช่วยในการใช้คอมพิวเตอร์
9. ชุดอุปกรณ์สำหรับการใช้แป้นพิมพ์

<u>รายการอุปกรณ์สำหรับการให้ยืมแบบที่ต้องทำสัญญายืมโดยมีระยะเวลาการยืม 1 ปี ได้แก่</u>

1. โทรศัพท์เคลื่อนที่
2. เครื่องช่วยสื่อสารพร้อมอุปกรณ์ต่อพ่วง
3. เครื่องพิมพ์อักษรเบรลล์
4. เครื่องสแกนเนอร์
5. เครื่องแสดงผลอักษรเบรลล์ชนิด 20 เซลล์และชนิด Mini Seika 16 เซลล์
6. อุปกรณ์ควบคุมตัวชี้ตำแหน่ง

คำถามที่พบบ่อยเกี่ยวกับเกณฑ์ราคากลางครุภัณฑ์คอมพิวเตอร์

๑. ถาม : ราคากลางใหม่จะเริ่มใช้งานเมื่อไหร่
ตอบ: โดยปกติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จะดำเนินการประกาศเกณฑ์ราคากลางใหม่ในช่วง มี.ค.– เม.ย. ของทุกปี ทั้งนี้ อาจเลื่อนตามความเหมาะสม

๒. ถาม : หน่วยงานสามารถเพิ่ม - ลด คุณลักษณะตามที่ระบุไว้ในเกณฑ์ราคากลางได้หรือไม่
ตอบ: ไม่สามารถลดคุณลักษณะได้ แต่สามารถเพิ่มคุณลักษณะได้ ถ้าไม่กระทบต่อราคา แต่หากเพิ่มคุณลักษณะแล้วทำให้ราคาเพิ่มขึ้น หน่วยงานต้องใช้วิธีสอบราคาตลาด เนื่องจากเกณฑ์ราคากลาง เป็นคุณลักษณะเบื้องต้นเท่านั้น ซึ่งหน่วยงานต้องกำหนดคุณลักษณะอื่นๆ ให้ตรงตามความต้องการของหน่วยงาน

๓. ถาม : ราคาในเกณฑ์ราคากลาง รวมภาษีมูลค่าเพิ่ม (VAT) แล้วหรือไม่
ตอบ: รวมภาษีมูลค่าเพิ่ม ๗ % แล้ว

คำถามที่พบบ่อยเกี่ยวกับเกณฑ์ราคากลางระบบกล้องโทรทัศน์วงจรปิด

๑. ถาม : ราคาอุปกรณ์ต่างๆ ที่กำหนดในเกณฑ์ราคากลางของระบบกล้องโทรทัศน์วงจรปิดรวมค่าติดตั้งหรือไม่
ตอบ : อุปกรณ์ที่กำหนดในเกณฑ์ราคากลางไม่รวมค่าติดตั้งและค่าสายสัญญาณใดๆ ทั้งสิ้น

๒. ถาม : ราคาอุปกรณ์ต่างๆ ที่กำหนดในราคากลางระบบกล้องโทรทัศน์วงจรปิดรวมค่าภาษีมูลค่าเพิ่ม (VAT) หรือไม่
ตอบ : อุปกรณ์ที่กำหนดในเกณฑ์ราคากลาง รวมค่าภาษีมูลค่าเพิ่ม ๗ % แล้ว

๓. ถาม : อุปกรณ์บันทึกภาพผ่านเครือข่าย (NVR) ราคาที่กำหนดรวมหน่วยจัดเก็บข้อมูลหรือไม่
ตอบ: อุปกรณ์บันทึกภาพผ่านเครือข่าย (NVR) ราคารวมหน่วยจัดเก็บตามที่ได้กำหนดในคุณลักษณะพื้นฐานแล้ว

คำถามที่พบบ่อยเว็บไซต์การรับฟังความคิดเห็นด้านกฎหมายไทย

1. **คำถาม :** หน่วยงานจะนำร่างกฎหมายขึ้นเผยแพร่บนเว็บไซต์ lawamendment.go.th ต้องดำเนินการอย่างไร
คำตอบ : สามารถติดต่อขอลงทะเบียนผ่านทาง e-mail: lawamendment@mdes.go.th หรือทางหมายเลขโทรศัพท์ 0 2141 6916

2. **คำถาม :** การจัดทำร่างกฎหมายจะต้องนำขึ้นเผยแพร่บนเว็บไซต์ lawamendment.go.th หรือไม่
คำตอบ : แนวทางการจัดทำและการเสนอร่างกฎหมายตามบทบัญญัติมาตรา ๗๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ได้ระบุไว้ในส่วนที่ ๒ ข้อ ๑.๑ ให้หน่วยงานของรัฐจัดให้มีการรับฟังความคิดเห็นเพื่อประกอบการจัดทำร่างกฎหมายในระดับพระราชบัญญัติ โดยในการรับฟังความคิดเห็นอย่างน้อยต้องรับฟังผ่านระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐนั้น หรือผ่านเว็บไซต์ lawamendment.go.th หรือจะใช้วิธีอื่นใดด้วยก็ได้ ทั้งนี้ ระยะเวลาในการรับฟังความคิดเห็นต้องไม่น้อยกว่า 15 วัน

คำถามที่พบบ่อยเกี่ยวกับคณะกรรมการจัดหาระบบคอมพิวเตอร์ของรัฐ

คำถาม : หากจะนำโครงการเข้าสู่กระบวนการพิจารณาของคณะกรรมการจัดหาระบบคอมพิวเตอร์ของรัฐต้องดำเนินการอย่างไรบ้าง
คำตอบ : โครงการดังกล่าวต้องมีวงเงินตั้งแต่ 100 ล้าน ขึ้นไป โดยสามารถศึกษารายละเอียดได้ที่เว็บไซต์คณะกรรมการจัดหาระบบคอมพิเตอร์ของรัฐ www.100m.mdes.go.th

<u>คำถามที่พบบ่อยเกี่ยวกับการกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ฯ</u>

1. คำถาม : "อาชญากรรมทางคอมพิวเตอร์" คืออะไร ยกตัวอย่างเช่น และส่งผลกระทบต่อประชาชนอย่างไร

<u>คำตอบ</u> : อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่างๆ เป็นต้น ระบบคอมพิวเตอร์ในที่นี้ หมายรวมถึงระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าวด้วย สำหรับอาชญากรรมในระบบเครือข่ายคอมพิวเตอร์ (เช่น อินเทอร์เน็ต) อาจเรียกได้อีกอย่างหนึ่ง คือ อาชญากรรมไซเบอร์ (Cybercrime) อาชญากรที่ก่ออาชญากรรมประเภทนี้ มักถูกเรียกว่า แครกเกอร์ (Cracker)

อาชญากรรมทางคอมพิวเตอร์ คือ

1. การกระทำการใด ๆ เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และผู้กระทำได้รับผลประโยชน์ตอบแทน

2. การกระทำผิดกฎหมายใด ๆ ซึ่งใช้เทคโนโลยี คอมพิวเตอร์เป็นเครื่องมือและในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีเช่นเดียวกัน การประกอบอาชญากรรมทางคอมพิวเตอร์ได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล อาชญากรรมทางคอมพิวเตอร์ จึงจัดเป็นอาชญากรรมทางเศรษฐกิจ หรือ อาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ

2. คำถาม : โดยส่วนมากการเกิดอาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบกับประชาชนจะเกิดจากสาเหตุใด

<u>คำตอบ</u> : ประเทศไทยมีจำนวนผู้ใช้ Facebook มากที่สุดเป็นอันดับหนึ่ง อันดับรองลงมาคือ Youtube, Line และ Instagram ตามลำดับ จากการตรวจสอบข้อมูลเกี่ยวกับการกระทำความผิดทางเทคโนโลยีสารสนเทศพบว่า จำนวนผู้เสียหายจากการกระทำความผิดในเครือข่ายสังคมออนไลน์พบได้มากที่สุดใน Facebook รองลงมาคือ Line, Instagram, Twitter, และ Youtube ตามลำดับ สำหรับ Skype, WhatsApp, WeChat และ BeeTalk พบได้บ้างแต่ยังน้อย

เมื่อพิจารณาถึงปัจจัยที่ทำให้เกิดการกระทำความผิดจำนวนมากหรือน้อย สาเหตุหนึ่งคาดว่ามาจากระดับความนิยมและจำนวนผู้ใช้งาน ยิ่งได้รับความนิยมมากและจำนวนผู้ใช้งานยิ่งมาก โอกาสที่จะเกิดการกระทำความผิดก็มากขึ้นตามไปด้วย อีกปัจจัยหนึ่งก็คือ รูปแบบ วัตถุประสงค์การให้บริการโซเชียลมีเดียของผู้ให้บริการแต่ละราย อย่างใน Youtube กลับพบการกระทำความผิดได้น้อยกว่า Line, Instagram และ Twitter ทั้งที่มีจำนวนผู้ใช้ใกล้เคียงกับ Facebook สาเหตุอาจเนื่องมาจาก Youtube นั้นให้บริการเกี่ยวกับการสร้างและรับชมวีดีโอเป็นหลัก แม้จะให้มีการแสดงความคิดเห็นได้ แต่ปฏิสัมพันธ์ระหว่างผู้ใช้ยังไม่สะดวกมากนัก และรูปแบบของสื่อที่ให้บริการก็ไม่หลากหลายเท่ากับ Facebook, Line, Instagram และ Twitter ส่วนโซเชียลมีเดียที่ให้บริการในลักษณะเฉพาะ อย่าง LinkedIn หรือ Pinterest จะพบการกระทำความผิดน้อยมาก

ในโซเชียลมีเดียอื่นๆ เช่น Line, Instagram, และ Twitter ก็มีลักษณะการกระทำความผิดที่คล้ายคลึงกันแต่จำนวนจะแตกต่างกัน เช่น Line จะมีทั้งปลอมแปลงแอบอ้างบุคคล ฉ้อโกง หมิ่นประมาท ส่งภาพลามกอนาจาร ลักษณะใกล้เคียงกับ Facebook ส่วนใน Instagram หรือ Twitter จะพบมากในเรื่องปลอมแปลงแอบอ้างและหมิ่นประมาท

3. คำถาม : ยกตัวอย่างอาชญากรรมคอมพิวเตอร์ที่เป็นปัญหาในปัจจุบัน

<u>คำตอบ</u> : ปัจจุบันโซเชียลมีเดีย ทำให้การมีปฏิสัมพันธ์กันระหว่างผู้ใช้ได้อย่างง่ายดาย สะดวกรวดเร็ว สามารถใช้สื่อได้หลายรูปแบบ และมีฟังก์ชันการใช้งานที่หลากหลาย ทำให้มีการกระทำความผิด และภัยคุกคามหลายรูปแบบมากด้วย เช่น ฉ้อโกงในการซื้อขายสินค้า การหลอกลวงเหยื่อให้แสดงออกทางเพศผ่านวีดีโอคอล (Video Call) ส่งต่อรูปภาพลามกอนาจารในกลุ่มการสนทนา (Group Chat) ถ่ายทอดสดการแสดงลามกอนาจาร (Live Video) การสนทนาข่มขู่ด้วยข้อความ (Messenger) เป็นต้น ซึ่งบางกรณีนั้นเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม ตัวอย่างการกระทำความผิดทางสื่อสังคมออนไลน์ที่พบบ่อย มีดังนี้

Facebook

- **ถูกฉ้อโกงหลอกลวงในการซื้อขายสินค้า**

การซื้อขายสินค้าใน Facebook เป็นที่นิยมอย่างมาก เนื่องจากสะดวกในการค้นหาสินค้า ผู้ซื้ออาจหาสินค้าได้ง่ายๆ ด้วยการเข้าร่วมกลุ่มหรือเพจที่เป็นแหล่งสินค้าที่ต้องการโดยเฉพาะ ผู้ขายใช้บัญชีส่วนตัว เพจ กลุ่ม หรือบริการ Market Place ของ Facebook ในการประกาศขายสินค้า ไม่ว่าจะเป็นสินค้าใหม่หรือสินค้ามือสอง มีความสะดวกในการติดต่อระหว่างผู้ซื้อกับผู้ขายมาก สะดวกในการเจรจาต่อรองราคา แต่มีผู้เสียหายจำนวนมากที่ซื้อสินค้าผ่าน Facebook แล้วถูกฉ้อโกงหลอกลวง ชำระเงินแล้วไม่ได้รับสินค้า หรือสินค้าที่ได้รับไม่ตรงตามที่ตกลง ซึ่งพบว่าการกระทำความผิดมักมีพฤติการณ์ดังต่อไปนี้

▶ ประกาศขายของที่มีราคาถูกกว่าราคาปกติในท้องตลาดเพื่อดึงดูดความสนใจของเหยื่อ

▶ ไม่แจ้งที่อยู่หรือหมายเลขโทรศัพท์ หรือแจ้งไว้แต่ก็ไม่สามารถติดต่อได้ เช่น โทรไม่ติด ไม่รับสาย หรือเป็นหมายเลขโทรศัพท์ของบุคคลอื่น แต่จะให้ติดต่อสนทนาทาง Facebook Messenger หรือ Line แทน

▶ โปรไฟล์ (Profile) Facebook ของผู้ขายใช้ชื่อปลอมและไม่ใช้รูปถ่ายตัวจริง บางครั้งใช้รูปการ์ตูน สิ่งของ สินค้า วิวทิวทัศน์ รูปดาราหรือบุคคลอื่น และไม่มีการโพสต์เนื้อหาในไทม์ไลน์ (Timeline) ที่เกี่ยวกับตนเอง

▶ ตั้งเงื่อนไขให้ผู้ซื้อโอนเงินก่อนเสมอไม่ว่าจะโอนเต็มจำนวนหรือมัดจำบางส่วน หรือบางครั้งขอส่งเป็นพัสดุเก็บเงินปลายทางโดยมีเจตนาจะส่งสินค้าที่ไม่ตรงกับที่ตกลงซื้อขาย

▶ ไม่ยินยอมที่จะนัดพบเพื่อขอดูสินค้าหรือรับของ พยายามบ่ายเบี่ยง เช่น อ้างว่าผู้ขายอยู่ไกลไม่สะดวกในการนัดพบ หากโอนเงินมาเลยจะลดราคาให้อีก เป็นต้น

▶ พฤติการณ์ที่พบว่าผิดปกติอย่างมาก คือ ไม่ให้ผู้ซื้อโอนเงินผ่านบัญชีธนาคาร แต่จะให้ผู้ซื้อซื้อบัตรเติมเงินให้กับผู้ขาย หรือให้โอนเงินผ่านบริการทางการเงินระหว่างประเทศ เช่น Western Union หรือ MoneyGram เป็นต้น

▶ หลังจากเหยื่อที่หลงเชื่อโอนเงินไปให้ผู้ขายแล้วก็จะไม่สามารถติดต่อกับผู้ขายได้อีกเลย หรือผู้ขายนิ่งเฉยไม่ตอบการสนทนา หรือปิดบัญชีและเพจหลบหนีไป

- **ถูกเข้าถึงบัญชีผู้ใช้งานโดยมิชอบหรือแฮก (Hack)**

การถูกแฮกบัญชี Facebook มีอยู่เป็นประจำ คาดว่าน่าจะมีผู้เสียหายอย่างน้อย ๕ รายในแต่ละวัน สาเหตุอันดับแรกที่ทำให้บัญชีถูกแฮก คือ ผู้เสียหายมักใช้หมายเลขโทรศัพท์ส่วนตัวเป็นรหัสผ่าน ซึ่งถือว่าเป็นรหัสผ่านที่ไม่ปลอดภัยอย่างมากเนื่องจากง่ายต่อการคาดเดา หลายรายไม่ทราบวิธีการตั้งรหัสผ่านที่ปลอดภัย และไม่เข้าใจวิธีการใช้งาน Facebook หรือใช้งานอีเมล มักให้ผู้อื่นโดยเฉพาะร้านจำหน่ายโทรศัพท์มือถือตั้งรหัสผ่านให้ คนร้ายมีพฤติการณ์และวัตถุประสงค์แตกต่างกันไป ที่พบเห็นได้เป็นประจำ คือ

▶ แฮกเพื่อนำบัญชี Facebook ไปสนทนาหลอกลวงเอาเงินจากเพื่อนใน Facebook ของผู้เสียหาย คนร้ายในลักษณะนี้มีอยู่ทั่วไปและไม่เคยรู้จักกับผู้เสียหายมาก่อน แฮกเข้าใช้บัญชีง่าย ๆ ด้วยการเดารหัสผ่านจากหมายเลขโทรศัพท์ หรือแฮกอีเมลที่ใช้ร่วมกับบัญชี Facebook แล้วทำการเปลี่ยนรหัสผ่าน เมื่อเข้าบัญชีได้แล้วคนร้ายจะเข้าไปอ่านข้อความที่ผู้เสียหายเคยสนทนากับเพื่อนๆ แล้วเลียนแบบลักษณะการพูดคุยและคำพูดที่ใช้ของผู้เสียหาย ทำให้ไม่มีผู้ใดสงสัยว่าเป็นคนร้าย หลอกลวงอ้างขอยืมเงิน เช่น อ้างว่าตกรถโดยสารไม่มีเงิน ลูกไม่สบายอยู่โรงพยาบาลต้องใช้เงินด่วน เอาเงินไปซื้อของก่อนแล้วจะคืนให้ เป็นต้น หากเป็นบัญชีหรือเพจที่ใช้ขายสินค้าหรือเป็นร้านค้า ก็จะนำไปสนทนากับลูกค้าที่เคยติดต่อซื้อสินค้า แล้วหลอกให้ลูกค้าโอนเงินให้ผ่านระบบเติมเงินทรูมันนี่ หรือบัญชีธนาคารที่เตรียมไว้ หลังจากที่ได้เงินไปแล้วคนร้ายจะยังไม่หยุดการแฮกเพียงเท่านี้ แต่จะนำบัญชีของผู้เสียหายไปเข้าดูหมายเลขโทรศัพท์ของบัญชี Facebook อื่น ๆ ที่เป็นเพื่อนกับผู้เสียหาย หากมีบัญชีใดใช้หมายเลขโทรศัพท์เป็นรหัสผ่านอีกก็จะถูกแฮกเป็นบัญชีต่อไป จากนั้นคนร้ายจะทำการหลอกลวงเพื่อนและทำการแฮกบัญชีอื่นต่อไปเรื่อย ๆ

▶ แฮกเพื่อเอาเพจของผู้เสียหายไปเป็นของตนเอง เพจที่เป็นเป้าหมายของคนร้าย เป็นเพจที่มีผู้กดถูกใจหรือติดตามจำนวนมากเป็นหลักหนึ่งหมื่นหรือหนึ่งแสนคนขึ้นไป มีทั้งแบบเดารหัสผ่าน แฮกอีเมล ฟิชชิ่ง (Phishing) เช่น ส่งข้อความแจ้งเตือนผู้เสียหายว่าบัญชี Facebook กำลังจะถูกปิด ต้องทำการยืนยันข้อมูลโดยให้ผู้เสียหายกรอกข้อมูลและรหัสผ่านที่หน้าเว็บเพจที่ทำปลอมขึ้นมา เมื่อผู้เสียหายหลงเชื่อคนร้ายก็จะได้ข้อมูลและรหัสผ่านผู้เสียหายไป เมื่อคนร้ายได้เพจไปแล้วก็จะเอาไปหลอกขายต่อให้บุคคลอื่น

▶ แฮกเพื่อเอาบัญชีผู้โฆษณาของผู้เสียหายไปโฆษณาให้เพจของตน ให้ผู้เสียหายเป็นฝ่ายชำระเงินค่าโฆษณาแทน มีทั้งแบบเดารหัสผ่าน แฮกอีเมล ฟิชชิ่ง (Phishing) ลักษณะเดียวกับการแฮกเพื่อเอาเพจ

▶ แฮกเพื่อนำไปใช้ส่งข้อความด่าทอ ประจาน หมิ่นประมาทบุคคลอื่น หรือผู้เสียหายเอง ผู้กระทำความผิดมักเป็นบุคคลที่มีความรู้จักคุ้นเคยกับผู้เสียหายเอง หรือมีปัญหาทะเลาะเบาะแว้งกันมาก่อน มีทั้งเข้าโดยเดารหัสผ่าน แฮกอีเมล

▶ แฮกเพื่อนำไปใช้ส่งข้อความรูปภาพที่ลามกอนาจาร เป็นหมายมักเป็นผู้หญิง มักไม่ต้องการครอบครองบัญชีและไม่มีการเปลี่ยนแปลงรหัสผ่าน ส่งรูปภาพลามกไปให้ผู้เสียหาย หรือขอมีเพศสัมพันธ์โดยใช้ข้อความที่ไม่เหมาะสม

4. คำถาม : วิธีตรวจสอบ ป้องกันและแก้ไขปัญหา

<u>คำตอบ</u>

- **การป้องกันสำหรับถูกฉ้อโกงหลอกลวงในการซื้อขายสินค้า**

▶ ควรอ่านประกาศด้วยความรอบคอบ ตรวจสอบราคาสินค้าจากแหล่งอื่นด้วยว่าราคาใกล้เคียงกันหรือไม่ ให้ระมัดระวังหรือไม่เลือกซื้อสินค้าที่ถูกกว่าราคาท้องตลาดมากเกินไป หากราคาถูกมากควรขอข้อมูลเพิ่มเติมเกี่ยวกับสินค้า สภาพสินค้าเป็นอย่างไร เหตุผลในการขายในราคาถูกคืออะไร และขอรูปถ่ายเพิ่มเติมจากผู้ขาย

▶ ไม่ซื้อสินค้ากับผู้ขายที่ปกปิดข้อมูลตนเองในโปรไฟล์หรือไทม์ไลน์ Facebook

▶ ตรวจสอบประวัติของผู้ขายก่อนซื้อ ข้อมูลของผู้ขาย เช่น ชื่อจริง ชื่อผู้ใช้ อีเมลแอดเดรส Line ID เลขที่บัญชีธนาคาร สินค้าที่เคยขาย สามารถค้นหาได้ง่าย ๆ ด้วย Google Search หากเป็นผู้ขายที่ประวัติไม่ดีอาจพบว่ามีผู้เสียหายรายอื่นเคยถูกฉ้อโกงหลอกลวงมาก่อนประกาศไว้ตามเว็บไซต์ต่าง ๆ

▶ ขอหมายเลขโทรศัพท์ของผู้ขายและติดต่อไปเพื่อตรวจสอบให้แน่ใจว่ามีหมายเลขโทรศัพท์อยู่จริงและติดต่อทางโทรศัพท์ให้มาก ไม่ควรติดต่อเพียงทาง Facebook Messenger, Line หรือสื่อสังคมออนไลน์เท่านั้น หากผู้ขายปฏิเสธการให้หมายเลขโทรศัพท์มีความเป็นได้สูงว่าจะเป็นมิจฉาชีพ

▶ ไม่ควรโอนเงินผ่านบัญชีธนาคารก่อนได้รับสินค้า หากจำเป็นต้องโอนเงินผ่านบัญชีธนาคาร ให้ตรวจสอบชื่อบัญชีธนาคารที่รับโอนด้วย ซึ่งควรเป็นชื่อเดียวกันกับชื่อของผู้ขาย

▶ ระมัดระวังโอนเงินด้วยบริการประเภทอื่น เช่น บัตรเติมเงิน Western Union MoneyGram

▶ หากเป็นไปได้ควรขอที่อยู่ของผู้ขาย หรือสถานที่เพื่อไปรับสินค้าด้วยตนเองและชำระค่าสินค้าเมื่อได้รับของแล้ว

▶ เก็บข้อมูลประกาศขายสินค้า ข้อมูลผู้ขาย ข้อมูลโปรไฟล์ Facebook การสนทนา ข้อมูลการติดต่อ และการโอนเงินไว้เป็นหลักฐาน

▶ ซื้อสินค้าจากเพจที่ได้การรับรองจาก Facebook

- **การแก้ไขปัญหาและการหาพยานหลักฐานสำหรับถูกฉ้อโกงหลอกลวงในการซื้อขายสินค้า**

▶ หากทราบว่าถูกฉ้อโกงหลอกลวงแล้ว ให้เก็บรวบรวมหลักฐานต่าง ๆ ได้แก่ข้อมูลประกาศขายสินค้า ข้อมูลผู้ขาย โปรไฟล์ และ URL ของ Facebook ข้อมูลการติดต่อและการสนทนา Line ID หมายเลขโทรศัพท์ และหลักฐานการโอนเงิน โดยรวบรวมหลักฐานอย่างละเอียดให้ได้มากที่สุด

▶ รวบรวมข้อมูลกิจกรรมบนไทม์ไลน์ Facebook ของผู้ขายทั้งก่อนเกิดเหตุจนถึงปัจจุบัน ได้แก่ การลงข้อความ รูปถ่ายหรือวีดีโอส่วนตัว สถานที่เช็คอินหรือที่เดินทางไป รายชื่อเพื่อน ผู้มาแสดงความคิดเห็น โดยเฉพาะผู้ที่น่าจะรู้จักกับผู้ขายเป็นอย่างดี เช่น การเอ่ยชื่อเล่น การกล่าวถึงกิจกรรมที่ทำร่วมกัน เป็นต้น เพื่อเป็นหลักฐานเกี่ยวกับบุคคลที่อาจเป็นพยานหรือการสืบสวนสอบสวนได้

▶ หากทราบหมายเลขโทรศัพท์อาจนำไปค้นหาใน Facebook หรือ Google Search เพื่อหาข้อมูลบัญชีและข้อมูลการประกาศสินค้าอย่างอื่น เป็นการหาหลักฐานเพิ่มเติม ซึ่งบางครั้งผู้กระทำความผิดอาจมีการลงหมายเลขโทรศัพท์ไว้ที่เว็บไซต์อื่นและอาจสามารถนำไปใช้ในการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ได้ด้วย

▶ นำหลักฐานที่รวบรวมเข้าแจ้งความร้องทุกข์มอบคดีต่อพนักงานสอบสวนหรือหน่วยงานสำนักงานตำรวจแห่งชาติที่มีอำนาจหน้าที่ เช่น สถานีตำรวจท้องที่ที่เกิดเหตุ กองบังคับการปราบปราม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี เป็นต้น เพื่อให้ดำเนินการสืบสวนสอบสวนหาตัวผู้กระทำความผิดมาดำเนินคดีตามกฎหมาย

▶ พนักงานสอบสวนอาจทำหนังสือร้องขอไปยังธนาคารเจ้าของบัญชีที่รับโอน เพื่อขออายัดบัญชีธนาคารไว้สำหรับการสืบสวนสอบสวนและระงับการโอนย้ายเงินในบัญชี หรือตรวจสอบเส้นทางการเงินว่ามีการถอนหรือโอนอย่างไร ปลายทางของการโอนไปที่ไหน เพื่อหาตัวผู้กระทำความผิด หรือเพื่อการเจรจากับเจ้าของบัญชีในการคืนเงินให้กับผู้เสียหาย

- **การป้องกัน สำหรับถูกเข้าถึงบัญชีผู้ใช้งานโดยมิชอบหรือแฮก (Hack)**

ที่สำคัญลำดับแรก คือ การตั้งรหัสผ่าน ควรเป็นรหัสผ่านที่มีความปลอดภัย ไม่สามารถคาดเดาได้ง่าย ไม่ใช้หมายเลขโทรศัพท์หรือข้อมูลส่วนตัวเป็นรหัสผ่าน หลักการตั้งรหัสผ่านที่ดี ควรมีความยาวอย่างน้อย ๘ ตัวอักษรหรือมากกว่านั้น (แต่ไม่ควรยาวเกินไปเพราะอาจทำให้จำยากและมีโอกาสป้อนผิดได้บ่อย) โดยประกอบด้วยอักขระดังต่อไปนี้ ตัวอักษร (a-z, A-Z) ตัวเลข (๐-๙) เครื่องหมายหรืออักขระพิเศษบวก ลบ คูณ หาร หรือ อื่นๆ เช่น (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./) และควรตั้งรหัสผ่านด้วยตนเอง ไม่ควรให้บุคคลอื่นหรือร้านจำหน่ายโทรศัพท์มือถือตั้งรหัสผ่านให้รักษาความปลอดภัยอีเมลให้ดี เพราะหากถูกแฮกอีเมล Facebook ที่เชื่อมอยู่กับอีเมลก็จะถูกแฮกด้วย รหัสผ่านที่ใช้ก็สำคัญเช่นเดียวกัน และไม่ควรใช้รหัสผ่านเดียวกันกับ Facebook หากเป็นรหัสผ่านเดียวกันอาจถูกแฮกทั้งหมด แต่หากคนร้ายแฮกอีเมลไม่ได้ก็ยังมีโอกาสกู้คืนบัญชี Facebook กลับมาด้วยอีเมล

▶ ไม่ควรบอกรหัสผ่านให้ผู้อื่นทราบ

▶ ไม่เปิดเผยอีเมลและหมายเลขโทรศัพท์ใน Facebook ควรตั้งค่าให้เห็นได้เฉพาะตนเอง หากคนร้ายทราบอีเมลหรือหมายเลขโทรศัพท์ คนร้ายก็ทราบเป้าหมายในการแฮก

▶ อย่าคลิกลิงก์หรือเปิดไฟล์แนบที่บุคคลที่ไม่รู้จักหรือไม่น่าไว้ใจส่งมาให้ อาจเป็นเครื่องมือที่คนร้ายใช้แฮกบัญชีหรือดักเอารหัสผ่านไป

▶ ระมัดระวังการกรอกรหัสผ่านควรดู URL ของหน้าที่ใช้งานว่าเป็นโดเมนเนม facebook.com หรือไม่ อาจมีการทำปลอมขึ้นมาเลียนแบบให้เหยื่อหลงเชื่อ เช่น fakebook.com facekook.com fakeb00k.com เป็นต้น เมื่อกรอกรหัสผ่านคนร้ายก็จะได้รหัสผ่านไป

▶ โดยปกติ Facebook จะให้กรอกรหัสผ่านเมื่อล็อกอิน หรือตั้งค่าบัญชีบางอย่างเท่านั้น หากมีการส่งข้อความมาให้ใส่รหัสผ่านให้คิดไว้ก่อนว่าอาจเป็นการกระทำของคนร้าย

▶ อีเมลที่ได้รับจาก Facebook สังเกตที่โดเมนเนมของอีเมลแอดเดรสให้ดีว่าเป็น @facebook.com หรือ @facebookmail.com ถ้าเป็นอย่างอื่นอาจเป็นอีเมลหลอกลวง

▶ ควรตั้งค่าความปลอดภัยโดยให้ Facebook แจ้งเตือนมาที่อีเมล หรือ SMS เมื่อมีผู้เข้าสู่ระบบด้วยอุปกรณ์อื่น หรือมีการเปลี่ยนแปลงข้อมูล เปลี่ยนรหัสผ่าน

▶ ใน Facebook มีการตั้งค่าความปลอดภัยอีกมาก ที่ผู้ใช้งานควรศึกษา ทั้งตั้งค่าความปลอดภัยแบบสองชั้นโดยส่ง SMS เป็น OTP หรือการตั้งค่าความช่วยหรือจากเพื่อน การอนุมัติเข้าสู่ระบบด้วยอุปกรณ์ และอื่น ๆ หากตั้งค่าต่าง ๆ อย่างดีจะมีความปลอดภัยสูงมาก

- **การแก้ไขปัญหาสำหรับถูกเข้าถึงบัญชีผู้ใช้งานโดยมิชอบหรือแฮก (Hack)**

<u>การแก้ไขปัญหาและการรวบรวมพยานหลักฐาน</u>

▶ แจ้งความที่สถานีตำรวจท้องที่ไว้เป็นหลักฐานว่าถูกแฮกบัญชี เนื่องจากคนร้ายอาจนำบัญชีไปใช้ในทางผิดกฎหมาย

▶ กรณีที่ถูกแฮกบัญชี Facebook ผู้ใช้ควรรีบดำเนินการกู้คืนบัญชีกลับคืนมา การกู้คืนอาจทำได้โดยปฏิบัติตามคำแนะนำในอีเมลที่ Facebook ส่งมาแจ้งเตือน หรือทำการกู้คืนโดยใช้คอมพิวเตอร์โทรศัพท์มือถือที่เคยใช้งานบัญชีก็สามารถทำได้ หากกู้คืนและสามารถเข้าใช้งานได้แล้ว ผู้ใช้สามารถดูข้อมูลจราจรทางคอมพิวเตอร์ได้ ว่ามีการเข้าใช้งานหรือเปลี่ยนแปลงข้อมูลด้วยไอพีแอเดรสอะไร วันที่และเวลาใด ซึ่งสามารถนำไปแจ้งความพนักงานสอบสวนเพื่อหาตัวคนร้ายได้

▶ เมื่อถูกแฮกบัญชีแล้วมีการเปลี่ยนแปลงรหัสผ่าน ทาง Facebook จะแจ้งเตือนมาที่อีเมลที่ใช้งานร่วมกับ Facebook ซึ่งอาจปรากฏข้อมูลไอพีแอดเดรสของคนร้าย ก็นำหลักฐานนี้ไปแจ้งความต่อพนักงานสอบสวนได้ด้วย

- กรณีความเสียหายอื่น ๆ เช่น

▶ ถูกปลอมแปลงแอบอ้างตัวบุคคลหรือองค์กร กรณีนี้ผู้เสียหายสามารถแจ้งปิดบัญชีปลอมได้ด้วยตนเองตามช่องทางที่ Facebook มีให้

▶ ถูกหมิ่นประมาท (ไม่เข้าข่าย พรบ.คอมพิวเตอร์)

▶ ถูกกลั่นแกล้ง (CyberBullying) เช่น ลงข้อความ รูปภาพ หรือวีดีโอ ทำให้ได้รับความอับอาย

▶ ถูกข่มขู่เพื่อเรียกเงิน (Black Mail) ขู่ว่าจะเผยแพร่ภาพหรือวีดีโอส่วนตัวของผู้เสียหายหากไม่โอนเงินให้

▶ ถูกละเมิดทรัพย์สินทางปัญญา

กรณีที่ถูกแฮกบัญชีโซเชียลมีเดีย อีเมล หากผู้ใช้สามารถกู้คืนบัญชีได้ และเข้าสามารถใช้งานได้อยู่ ทางผู้ให้บริการส่วนมาก อย่างเช่น Facebook, Twitter หรืออีเมลต่าง ๆ มีบริการที่ให้ผู้ใช้สามารถดูข้อมูลจราจรทางคอมพิวเตอร์ได้ ว่ามีการเข้าใช้งานหรือเปลี่ยนแปลงข้อมูลด้วยไอพีแอเดรสอะไร ซึ่งสามารถนำไปแจ้งความพนักงานสอบสวนเพื่อหาตัวคนร้ายได้

5. คำถาม : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีการดำเนินการอย่างไรในการช่วยเหลือผู้ที่ถูกคุกคามทางไซเบอร์

คำตอบ : ปัจจุบันกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในฐานะผู้กำกับดูแลการใช้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยรัฐมนตรีว่าการกระทรวงฯ เป็นผู้รักษาการตามกฎหมาย ได้มีการแต่งตั้งพนักงานเจ้าหน้าที่เพื่อปฏิบัติงานในการดำเนินการเฝ้าระวัง รับเรื่องราวร้องทุกข์ ติดตามและการดำเนินการร่วมกับเจ้าหน้าที่ตำรวจในการจับกุมผู้กระทำความผิดที่เข้าข่ายตาม พ.ร.บ. รวมทั้งมีศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center: CSOC) ดำเนินการเฝ้าระวังเกี่ยวกับเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม รองรับภัยคุกคามด้านสารสนเทศในระดับประเทศตลอด 24 ชั่วโมง และหมายเลขสายด่วน 1212 ให้ประชาชนแจ้งข้อมูล เบาะแส นอกจากนี้ยังมีกลุ่มงานวิเคราะห์และพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensic) และฝ่ายกฎหมายที่ร่วมกับพนักงานสอบสวนในการออกหมายจับ หมายค้น ร่วมดำเนินการจับกุมกับเจ้าหน้าที่ตำรวจ ในกรณีพบเบาะแสหรือมีเหตุควรสงสัย หรือมีหลักฐานตามสมควรที่จะสามารถเอาผิดกับผู้ต้องสงสัยได้ ตลอดจนมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ ThaiCERT (Thai Computer Emergency Response Team) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หน่วยงานในกำกับของกระทรวงฯ

สายด่วนทันภัยไซเบอร์

- กด 1212 ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- กด 1111 ศูนย์บริการภาครัฐและประชาชน
- กด 1166 สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
- กด 1599 สำนักงานตำรวจแห่งชาติ
- กด 1200 สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)
- กด 0 2860 1358 มูลนิธิอินเตอร์เน็ตร่วมพัฒนาไทย (ไทยฮอตไลน์)
- กด 0 2143 8448 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

6. คำถาม : ทางกระทรวงได้มีการประชาสัมพันธ์ ให้ข้อมูลเกี่ยวกับอาชญากรรมคอมพิวเตอร์อย่างไร

คำตอบ : มีการประชาสัมพันธ์ผ่านช่องทาง YouTube, Twitter, Instagram, Facebook และ Line@ ในหัวข้อ “รอบรู้ ทันภัย CYBER”

7. คำถาม : แนะนำวิธีการใช้เทคโนโลยี และโซเชียลมีเดียให้ปลอดภัย

คำตอบ :

- คิดให้รอบคอบก่อนโพสต์ข้อมูลใดๆ เพราะอย่าลืมว่าข้อมูลเหล่านี้จะเปิดเผยให้ทุกคนสามารถเข้าถึงได้ง่าย โดยเฉพาะอย่างยิ่งการโพสต์ข้อมูลที่สุ่มเสี่ยงก็อาจจะส่งผลร้ายต่อตัวเราเองก็เป็นได้

▶ ใช้ความระมัดระวังในการคลิกลิงก์ต่างๆ ที่มากับการแชร์หรือข้อความ หลีกเลี่ยงลิงก์แปลกปลอม หรือมาจากคนที่ไม่รู้จัก หรือแม้แต่เพื่อนซึ่งใช้ภาษาในการสื่อสารที่ดูแปลกไปจากปกติ เพราะอาจเป็นลิงก์ที่นำไปสู่ไวรัสหรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์

▶ พิมพ์ที่อยู่ URL ของเว็บไซต์โซเชียลเน็ตเวิร์กนั้นๆ โดยตรง โดยบนเบราว์เซอร์ให้หลีกเลี่ยงการเข้าเครือข่ายทางสังคมผ่านทางคลิกลิงก์จากผลแสดงการค้นหา หรือจากอีเมล เพราะอาจเป็น URL ปลอมที่นำเราไปยังเว็บไซต์ปลอม เพื่อหลอกเอาบัญชีผู้ใช้และ Password ได้ เช่น www.facebook.com อาจมี URL หลอกเป็น www.faeebook.com เป็นต้น

▶ คัดกรองคนที่ขอเป็นเพื่อน หรือขอเชื่อมโยงกับเครือข่ายสังคมออนไลน์ของเรา หลีกเลี่ยงการตอบรับคนที่ไม่รู้จักกันมาก่อน เพราะผู้ไม่หวังดีอาจแฝงมากับคนที่ขอเข้ามาเป็นเพื่อนเรา และหากพบคนที่เป็นเพื่อนซึ่งเราไม่รู้จักและน่าสงสัยก็ควรลบออกไป

▶ ตั้งค่าความเป็นส่วนตัว ผู้ให้บริการแต่ละรายจะกำหนดการตั้งค่าส่วนตัวไว้เพื่อไม่ให้ข้อมูลหรือสิ่งที่เราทำ หลุดออกไปยังคนที่ไม่พึงประสงค์ ดังนั้น เราควรตั้งค่าให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเรา และหลีกเลี่ยงการตั้งค่าสิ่งที่เราทำให้เป็นสาธารณะ หรือคนทั่วไปเห็นได้

▶ ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น บัตรประจำตัวประชาชน บัตรเครดิตลงในโซเชียลเน็ตเวิร์ก ไม่ว่าจะอยู่ในรูปแบบข้อความ หรือรูปภาพ เพราะแฮกเกอร์และผู้ไม่หวังดีสามารถแฝงตัวมากับกลุ่มเพื่อนที่เราอนุญาตให้เข้าชมได้

▶ เปิดใช้งาน Do Not Track เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ ซึ่งอาจรวมไปถึงผู้ไม่หวังดีที่ลักลอบเข้ามาขโมยข้อมูลด้วย ซึ่งปัจจุบันมีเว็บเบราว์เซอร์ที่เปิดใช้งาน Do Not Track ได้แล้ว เช่น Internet Explorer 10

▶ ใช้วิจารณญาณในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที รวมทั้งการกล่าวอ้างถึงแหล่งที่มาของข้อมูลนั้นๆ เพราะอาจมีการสวมรอย หรือสมอ้างจากผู้ไม่หวังดีเพื่อสร้างข่าว หรือสร้างความเสื่อมเสียต่อแหล่งที่มานั้นได้

▶ ดูแลและควบคุมการใช้งานของบุตรหลานอย่างใกล้ชิด สอนให้เด็กรู้จักวิเคราะห์ข้อมูล และรู้จักเล่นอย่างถูกวิธี เพราะความรู้ในโซเชียลเน็ตเวิร์กก็มีอยู่มากมาย และปัจจุบันครูอาจารย์ก็ทันสมัยจนมีการสื่อสารแจ้งเรื่องต่างๆ แก่ลูกศิษย์ผ่านโซเชียลเน็ตเวิร์ก เช่น Facebook หรือ Twitter กันแล้ว นอกจากนี้ อาจหาเครื่องมือในการควบคุมการใช้งานของบุตรหลายได้ เช่น โปรแกรม Windows Live Family Safety ซึ่งเป็นโปรแกรมที่ไมโครซอฟต์เปิดให้ใช้งานได้ฟรีๆ นอกจากจะใช้ควบคุมการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมได้แล้ว ยังสามารถกำหนดช่วงเวลาในการใช้คอมพิวเตอร์ และป้องกันการใช้โปรแกรม หรือเล่นเกมที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตได้อีกด้วย

▶ ตระหนักว่ามันเป็นสังคมเสรี แม้ว่าทุกคนจะมีสิทธิ์ในการแสดงความคิดเห็น แต่ทุกคำพูดและการกระทำที่ไม่เหมาะสมก็สามารถเป็นเหตุในการฟ้องร้องได้ และศาลก็อาจจะรับฟังคำร้องด้วย

ที่มา: https://www.etda.or.th/content/social-network-security.html