บทเรียนที่ 7

การหลีกเลี่ยงการถูกหลอกลวง

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | We Think Digital

มาตรฐานชุมชน Facebook ที่เกี่ยวข้อง

- สินค้าควบคุม (Regulated Goods)
- การฉ้อโกงและการหลอกลวง (Fraud and Deception)
- ความปลอดภัยทางไซเบอร์ (Cybersecurity)

สามารถเรียนรู้เพิ่มเติมเกี่ยวกับมาตรฐานชุมชน Facebook ได้ที่

สินค้าควบคุม (REGULATED GOODS)
facebook.com/communitystandards/regulated_goods

การฉ้อโกงและการหลอกลวง
facebook.com/communitystandards/fraud_deception

ความปลอดภัยทางไซเบอร์ (CYBERSECURITY)
facebook.com/communitystandards/cybersecurity

Lesson 1

การสังเกตการหลอกลวงต่าง ๆ (Scams)

การหลอกลวงคืออะไร ?

การหลอกลวง คือ การกระทำฉ้อโกงที่สามารถทำได้ในรูปแบบโกงเงินผู้อื่นหรือในรูปแบบขโมยข้อมูลที่เป็นความลับ

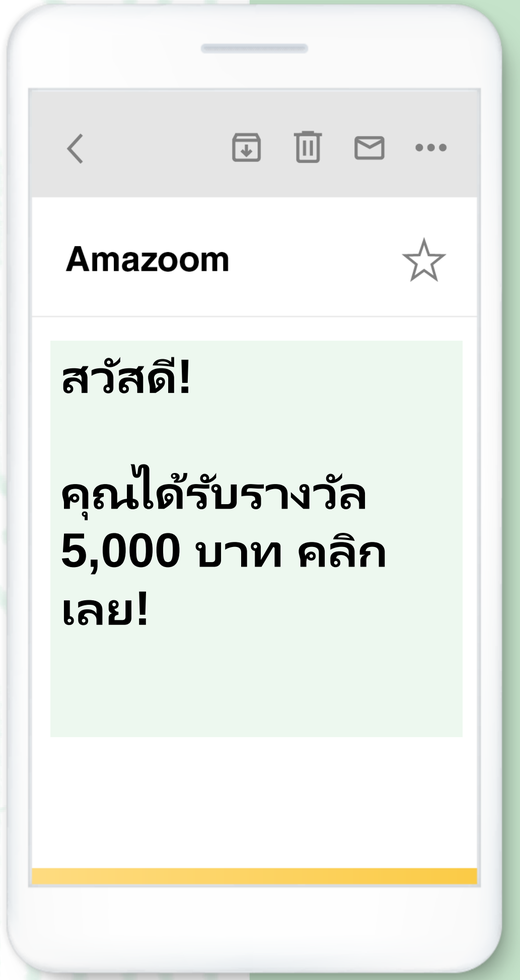
การหลอกลวงสามารถเกิดขึ้นได้หลากหลายวิธี ไม่ว่าจะเป็น แอปพลิเคชันหาคู่ออนไลน์ อีเมล เว็บไซต โซเชียลมีเดีย การติดต่อทางโทรศัพท์ หรือแม้แต่ข้อความ

การหลอกลวงที่พบได้บ่อย

- การหลอกลวงด้านการเงิน รวมถึงการกุศล การเสี่ยงโชค
- การหลอกลวงจากงาน และการหลอกลวงในเรื่องการชำระเงินรูปแบบอื่น ๆ
- การขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางการแพทย์
- การหลอกลวงด้านความสัมพันธ์คู่รัก ไม่ว่าจะเป็น การแอบอ้างเป็นคนอื่น และการหลอกลวงจากการหาคู่ออนไลน์
- การหลอกลวงด้านเทคนิค รวมถึงการขโมยรหัสแบบสุ่มสำหรับใช้ในการล็อกอินแอปพลิเคชัน

มาเรียนรู้เกี่ยวกับการฉ้อโกงที่พบเห็นได้ทั่วไปในรูปแบบออนไลน์และดูตัวอย่างนักหลอกลวง ในวิดีโอต่อไปนี้

การฟิชชิงคืออะไร?



- **การฟิชชิงคือการหลอกลวงประเภทหนึ่งที่หลอกให้คนแชร์การล็อกอินหรือข้อมูลส่วนบุคคลของพวกเขา**
- การฟิชชิงสามารถเจอได้ในรูปแบบอีเมล ข้อความ การติดต่อทางโทรศัพท์ และโพสต์จากโซเชียลมีเดีย
- ข้อความหรืออีเมลอาจดูเหมือนส่งมาจากบริษัทที่เรารู้จักและน่าเชื่อถือ เช่น ธนาคาร ร้านค้าออนไลน์ หรือเว็บไซต์

ลักษณะของข้อความฟิชชิง

ข้อความฟิชชิงอาจจะใช้กลยุทธ์ต่อไปนี้เพื่อล่อลวงให้ผู้คนคลิกลิงก์ เปิดเอกสารแนบ หรือแชร์การล็อกอินหรือข้อมูลส่วนบุคคล

- สอบถามข้อมูลส่วนบุคคลเพื่อใช้ในการยืนยัน
- อ้างว่าบัญชีผู้ใช้งานหรือข้อมูลด้านการชำระเงินของเรามีปัญหา
- แนบใบเสร็จหรือใบเสนอราคาปลอม หรือแนบลิงก์เพื่อให้จ่ายหรือดูการชำระเงิน
- เสนอบัตรกำนัลได้รับของฟรีที่ดูเกินจริง
- ส่งการแจ้งเตือนเกี่ยวกับการกระทำที่น่าสงสัยหรือการพยายามที่จะล็อกอินเข้าบัญชีผู้ใช้งานของเรา
- แจ้งว่าเราได้รับสิทธิ์ในการชำระเงินหรือได้รับเงินคืน

การแอบอ้างเป็นคนอื่นคืออะไร?

การแอบอ้างเป็นคนอื่นคือเมื่อนักต้มตุ๋นสร้างบัญชีผู้ใช้งานปลอมหรือสร้างตัวตนปลอมขึ้นมาเพื่อหลอกให้คนหลงเชื่อว่ากำลังพูดคุยกับคนจริง ๆ

วิธีป้องกันการฟิชชิง

สัญญาณที่อาจบอกได้ว่าข้อความอาจเป็นการหลอกลวงฟิชชิง

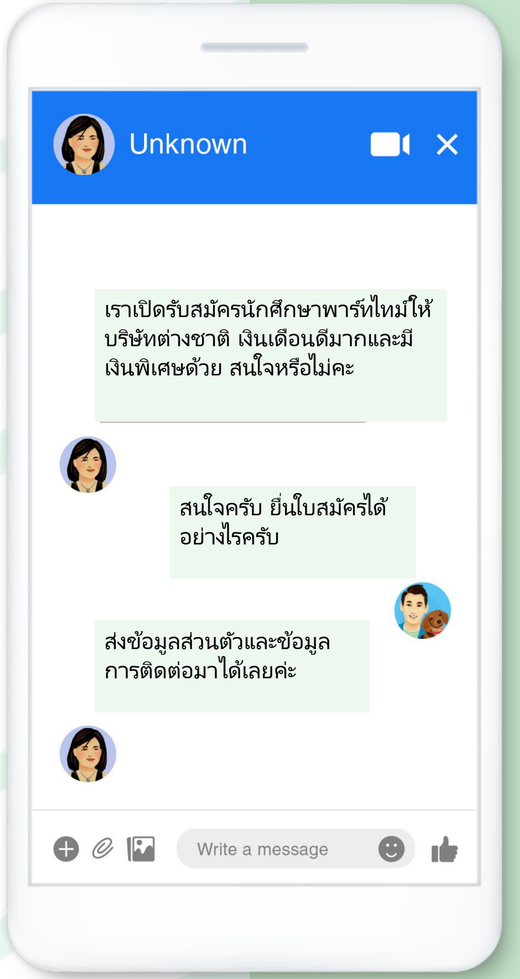
- ใครก็ตามที่ขอให้เราชำระเงินค่าสมัครงาน
- ข้อความหรือโพสต์ที่สะกดผิดและมีข้อผิดพลาดทางไวยากรณ์
- คนที่ร้องขอเงินจากเราโดยที่ไม่รู้จักเป็นการส่วนตัว
- คนที่ขอให้เราเปลี่ยนช่องทางการสนทนาจาก Facebook เป็นช่องทางที่เป็นสาธารณะน้องลงหรือไม่ค่อยมีความปลอดภัย เช่น การใช้อีเมลอื่นๆ นอกเหนือจากที่ระบุไว้ในที่สาธารณะ

วิธีป้องกันการฟิชชิง

สัญญาณที่อาจบอกได้ว่าข้อความอาจเป็นการหลอกลวงฟิชชิง

- คนที่ขอให้เราส่งเงินหรือบัตรกำนัล เพื่อที่จะรับเงิน รางวัล หรืออื่น ๆ
- คนที่อ้างว่าเป็นเพื่อนหรือญาติเรา
- คนหรือบัญชีผู้ใช้งานที่ให้เราเข้าไปในเว็บเพจอื่นที่ต่างไปจากเดิมเพื่อรับรางวัล
- คนที่บิดเบือนสถานที่ที่พวกเขาอยู่

การหลอกลวงด้านการเงิน

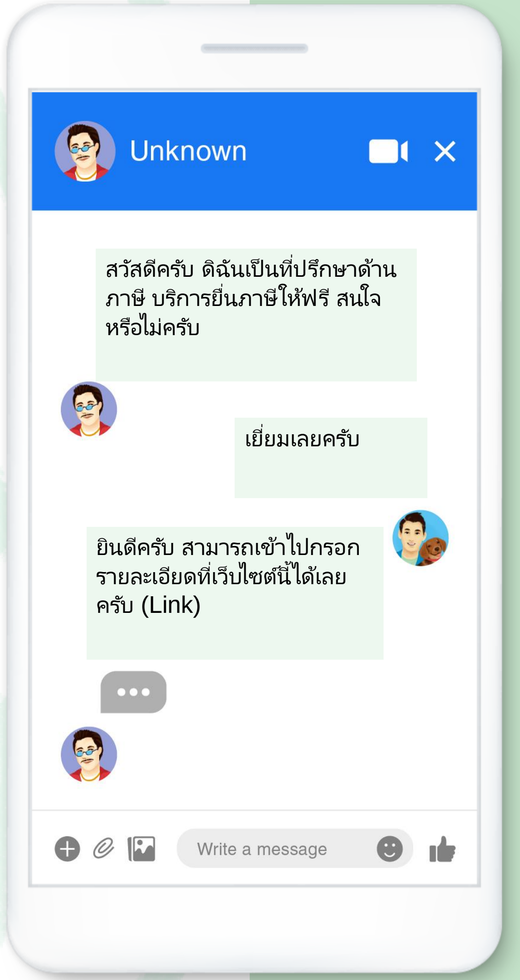


- การหลอกลวงประเภทแรกคือ การหลอกลวงทางการเงิน รวมถึงภาษี การกุศล การรับมรดก การเสี่ยงโชค การบริจาค การกู้ยืม การพาณิชย์อิเล็กทรอนิกส์ และการหลอกลวงการชำระเงินอื่น ๆ

- ในบรรดาการหลอกลวงทั้งหมด อาจมีคนอ้างว่ามาจากสถาบันทางการเงินหรือองค์กรรัฐบาลจะติดต่อเรามาทางโทรศัพท์ ข้อความหรืออีเมล หรือทิ้งข้อความว่าเรายังไม่ได้ชำระภาษีหรือเงิน

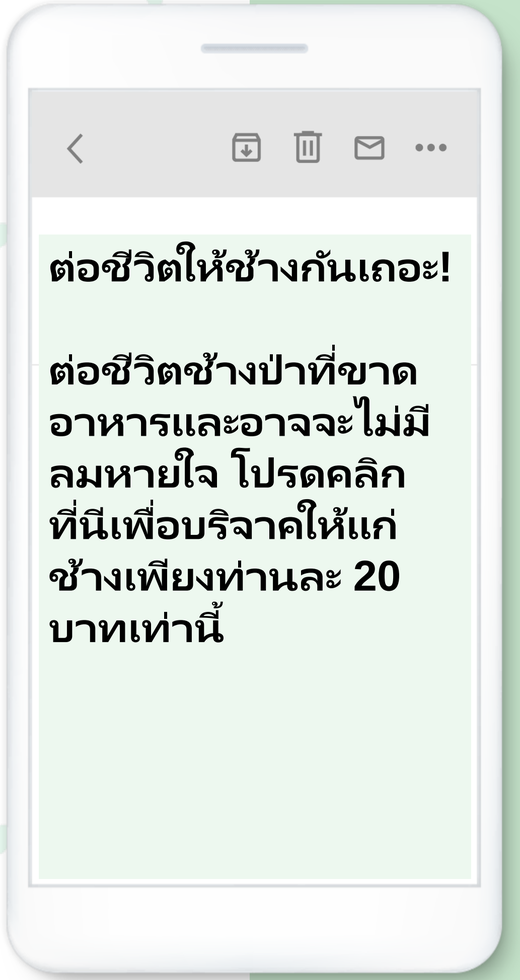
- พวกเขาอาจบอกว่าหากเราไม่ชำระเงินในทันที จะดำเนินการทางกฎหมายกับเรา

การหลอกลวงด้านภาษี



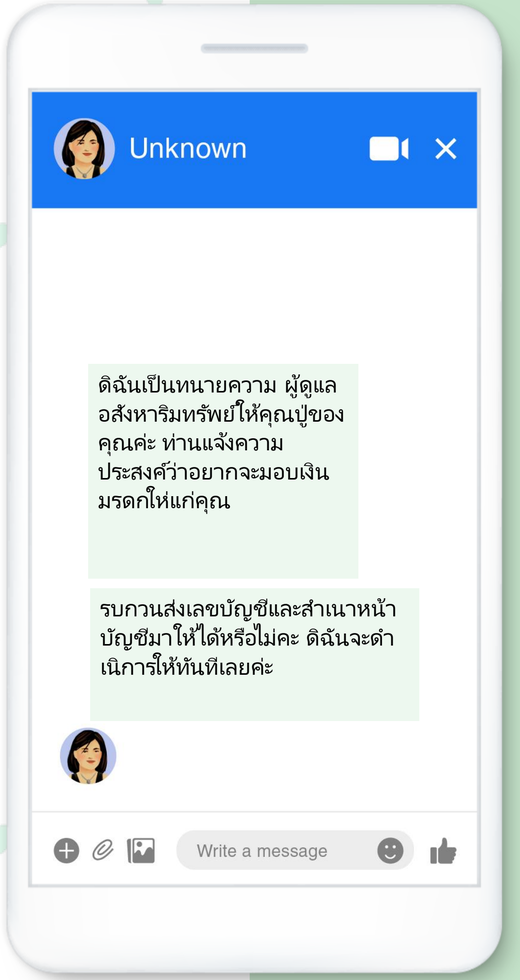
- ให้สงสัยข้อความที่อ้างว่าเป็นผู้เชี่ยวชาญด้านภาษี
- ให้ใช้ซอร์ฟแวร์ที่ถูกกฎหมายหรือเว็บไซต์เพื่อยื่นภาษีเท่านั้น

การหลอกลวงด้านการกุศล



- ระวัง! หากได้รับอีเมลไม่พึงประสงค์จากองค์กรการกุศลเพื่อให้บริจาคผ่านช่องทางออนไลน์
- หากเราไม่คุ้นเคยกับองค์กรการกุศลหรือไม่มั่นใจว่าองค์กรนั้นถูกกฎหมายหรือไม่
  - ตรวจสอบข้อมูลองค์กรได้ที่ CharityNavigator.org.
  - ให้มั่นใจว่าได้บริจาคผ่านเว็บไซต์องค์กรที่เป็นทางการ

การหลอกลวงด้านมรดก



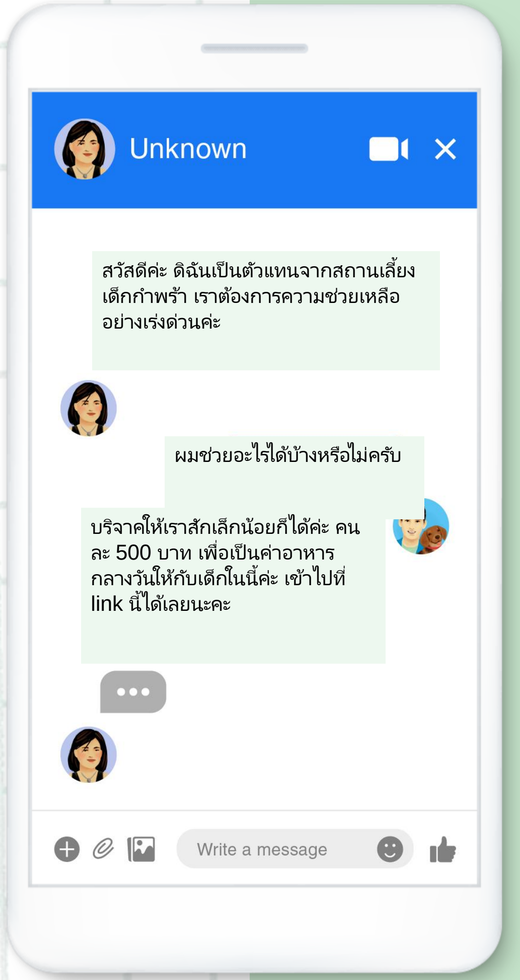
- นักต้มตุ๋นอาจจะอ้างเป็นทนายความ เพื่อนสนิท หรือญาติ เพื่อพูดคุยเกี่ยวกับทรัพย์สินของบุคคลที่เสียชีวิตไปแล้ว
- พวกเขาอาจอ้างว่าเรามีสิทธิ์ในมรดกนั้น
- นักต้มตุ๋นอาจให้เราบอกข้อมูลส่วนบุคคล เช่น ที่อยู่หรือรายละเอียดของธนาคาร

การหลอกลวงด้านการเสี่ยงโชค

- การหลอกลวงด้านการเสี่ยงโชคมักจะสำเร็จได้จากการที่ใช้บัญชีผู้ใช้งานปลอมเป็นคนที่เรารู้จักหรือสร้างโปรไฟล์ปลอมเพื่อแสร้งเป็นองค์กรนั้น ๆ

- ตัวข้อความอาจอ้างว่าเราได้รับรางวัลจากการเสี่ยงโชคและสามารถรับเงินได้ฟรี นักต้มตุ๋นอาจขอให้เราบอกข้อมูลส่วนบุคคล เช่น ที่อยู่หรือรายละเอียดธนาคาร

การหลอกลวงด้านการบริจาค



- การหลอกลวงประเภทนี้สามารถทำได้โดยการปลอมบัญชีผู้ใช้งานเป็นผู้ที่มีชื่อเสียงทางด้านศาสนาหรือปลอมเป็นบัญชีผู้ใช้งานที่มาจากองค์กรการกุศลหรือสถานรับเลี้ยงเด็กกำพร้า

- นักต้มตุ๋นอาจขอให้เราบริจาคให้

การหลอกลวงด้านการกู้ยืม

- นักต้มตุ๋นการกู้ยืมจะส่งข้อความหรือโพสต์และคอมเมนท์บนเพจและในกลุ่ม หรืออ้างว่ารู้จักใครบางคนที่ให้ยืมได้ สามารถยืมได้ทันทีในอัตราดอกเบี้ยที่ต่ำ

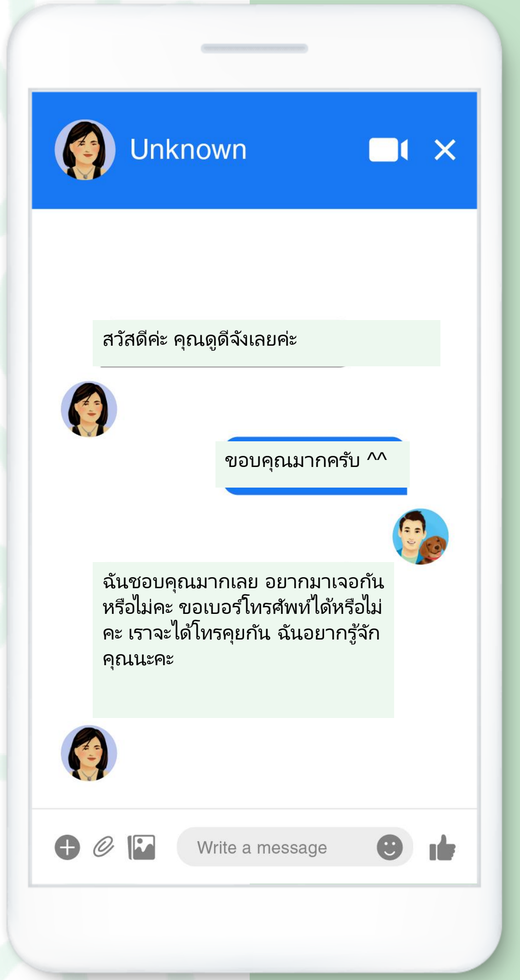
การหลอกลวงผ่านร้านค้าบน Facebook

- ระมัดระวังเมื่อต้องมีทำธุรกรรมระหว่างบุคคลเพื่อที่จะซื้อสินค้าในรูปแบบการพาณิชย์อิเล็กทรอนิกส์ โดยเฉพาะอย่างยิ่งหากสินค้าชิ้นนั้นต้องจัดส่งจากพื้นที่ระยะไกล

เคล็ดลับสำหรับการซื้อขายสินค้าออนไลน์

- ระมัดระวังการหลอกลวงในรูปแบบบัตรกำนัล
- การติดต่อสื่อสารบน Facebook
- พิจารณาตัวเลือกในการจัดส่ง
- อย่าซื้อหรือขายสินค้าที่ถูกเรียกคืนรายการ
- ศึกษาว่าสินค้าตัวไหนที่ไม่สามารถซื้อขายได้บน Facebook
- พบเจอกับผู้ซื้อหรือผู้ขายโดยตรง
- ปกป้องความเป็นส่วนตัวของเรา
- ใช้ช่องทางการชำระเงินออนไลน์
- ตรวจสอบสินค้า
- ระวังสินค้าปลอม

การหาคู่ออนไลน์หรือการหลอกลวงในด้านความสัมพันธ์คู่รัก



- หากเราเลือกใช้งานการหาคู่ออนไลน์ผ่านแอปพลิเคชันหรือเว็บไซต์ อยากให้จำไว้ว่า อาจมีใครบางคนในโลกออนไลน์อ้างเป็นใครบางคนก็ได้
- เราอาจต้องระวังคนที่เราพบเจอในโลกออนไลน์ให้มากขึ้น หากพวกเขาแสดงปฏิกิริยาต่อไปนี้:
  - รูปภาพของพวกเขาดูเป็นรูปทางการ
  - พวกเขาอาจทำให้คุณรู้สึกไม่สะดวกใจโดยการใช้ถ้อยคำรุนแรงในการสารภาพรักทันที
  - พวกเขาทำให้เราไม่สบายใจโดยการชักชวนไปเดทในสถานที่จริงและให้ติดต่อกับพวกเขาผ่านทางอีเมลหรือข้อความ

อยู่ให้ปลอดภัยขณะหาคู่ออนไลน์

เมื่อต้องพบเจอกับใครในโลกออนไลน์:

- ระมัดระวังให้ดี
- เก็บข้อมูลส่วนบุคคลไว้เป็นส่วนตัว
- รายงานและปิดกั้นใครก็ตามที่ขอให้เราแชร์ข้อมูลส่วนบุคคล ข้อมูลที่อาจเป็นภัยต่อความเป็นส่วนตัวของเรา ความปลอดภัย และความมั่นคง หรือใครก็ตามที่เรารู้สึกว่าน่าสงสัย

การหาคู่ออนไลน์: สัญญาณเตือนที่พบได้บ่อย

เหล่านี้คือ สัญญาณเตือนที่พบเห็นได้บ่อยเมื่อเราเจอนักต้มตุ๋น:

- ต้องการออกจากแอปพลิเคชันหาคู่ทันทีและใช้อีเมลส่วนตัวหรือส่งข้อความผ่านกล่องข้อความ
- อ้างว่าตกหลุมรักเราอย่างรวดเร็ว เพื่อที่จะโน้มน้าวให้เราคุยกับพวกเขา
- วางแผนที่จะพบเจอกัน แต่อ้างว่ามีเหตุร้ายที่ทำให้เจอไม่ได้และต้องยกเลิกการนัดไป
- ขอให้เราส่งเงินหรือของขวัญหรือบัตรกำนัลให้

จำไว้ว่าความรักทางโลกออนไลน์ที่ขอเงินจากเราอาจเป็นการหลอกลวงจากนักต้มตุ๋น

ข้อแนะนำในการอยู่ให้ปลอดภัยเมื่อต้องพบเจอ

- บอกใครบางคนเกี่ยวกับแผนนัดหมายของเรา
- แชร์สถานที่ที่เราอยู่
- พบเจอกันในพื้นที่สาธารณะ
- ทำตัวให้คุ้นชินกับสถานที่ที่นัดเจอกัน
- ตรวจสอบการบริโภคแอลกอฮอล์หรือสารเสพย์ติด
- มั่นใจว่าโทรศัพท์มีแบตเตอร์รี่เพียงพอ
- จัดการการเดินทางของเราเอง
- แชร์ข้อมูลส่วนบุคคลอย่างระมัดระวัง

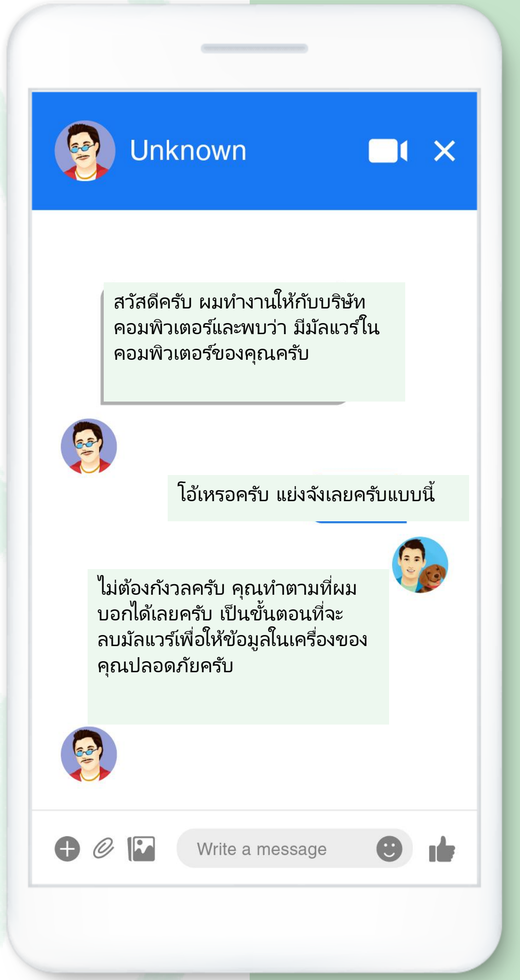
หากเรารู้สึกไม่สะดวกใจหรือไม่ปลอดภัย

- หากเราหรือคนที่เรารู้จักเป็นเหยื่อของอาชญากรรมหรือตกอยู่ในอันตราย ให้ติดต่อสถานที่บังคับใช้กฎหมายในท้องถิ่นเพื่อขอความช่วยเหลือ

- หากเรารู้สึกกดดันหรือไม่สะดวกใจ เราสามารถ:

  - จบการเดทและกลับบ้านด้วยตัวเอง
  - ปิดกั้นใครก็ตามที่ทำให้เรารู้สึกไม่สะดวกใจ
  - รายงานใครก็ตามที่เราคิดว่าน่าสงสัย

คอมพิวเตอร์โดนแฮกหรือการหลอกลวงด้านเทคนิค



- การหลอกลวงประเภทนี้เกิดจากการสายเรียกเข้าที่ไม่พึงประสงค์ - อาจมาจากหมายเลขที่ไม่รู้จักหรือไม่ได้ลงทะเบียน อีเมล หรือข้อความ ใครบางคนอ้างเป็นฝ่ายเทคนิคจากบริษัทและแจ้งว่าคอมพิวเตอร์ของเราได้รับไวรัส

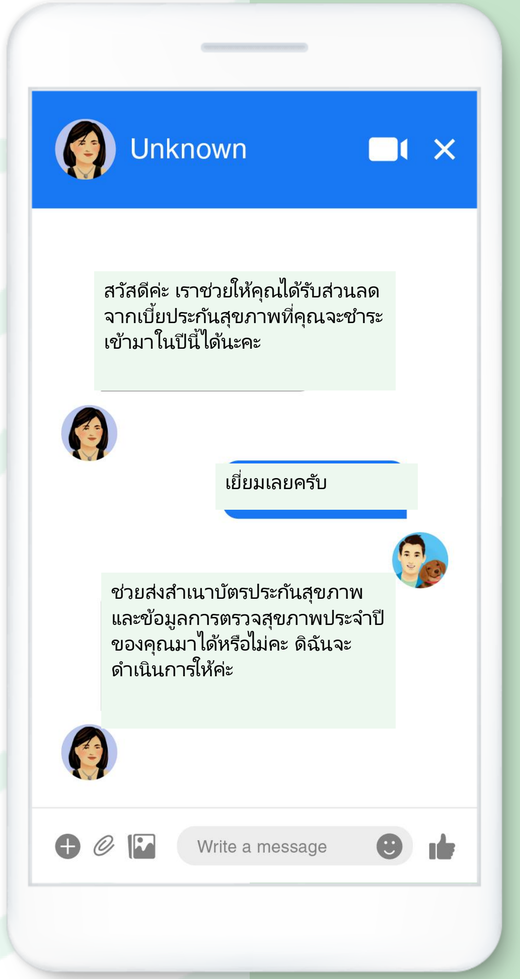
- จากนั้นพวกเขาจะให้เราทำตามคำสั่งเพื่อรักษาข้อมูลของเราไว้ ซึ่งทำให้พวกเขาสามารถติดตั้งมัลแวร์ในคอมพิวเตอร์ของเราได้หรือขโมยข้อมูลส่วนบุคคล ในบางกรณีพวกเขาอาจสอบถามข้อมูลทางการเงินหรือต้องการให้เราซื้อบัตรกำนัลเพื่อกู้คืนการเข้าถึงคอมพิวเตอร์ของเรา

- เพื่อหลีกเลี่ยงการหลอกลวงนี้ วางสายหรือเพิกเฉยข้อความ จากนั้นถ้าเรามีคำถามหรือข้อกังวลให้ติดต่อโดยตรงไปยังบริษัท

- อย่าตอบกลับข้อความที่ไม่ถึงประสงค์

การขโมยข้อมูลระบุตัวตนด้านการแพทย์

นักต้มตุ๋นอาจใช้ข้อมูลส่วนตัวของคุณเพื่อขอรับยาอันตรายหรือยาต้องห้าม หรือแม้กระทั่งการขอรับบริการด้านการรักษาอื่น ๆ



ข้อแนะนำต่อไปเพื่อหลีกเลี่ยงการขโมยข้อมูลระบุตัวตนทางการแพทย์:

- ระมัดระวังเกี่ยวกับการให้ข้อมูลประกันสุขภาพ ข้อมูลโครงการประกันสุขภาพของรัฐบาล หรือข้อมูลประกันสังคมกับบริษัทหรือคนที่เราไม่รู้จัก
- ในขณะที่บริษัทประกันอาจขอเก็บสำเนาบัตรประกันสุขภาพ พยายามหลีกเลี่ยงให้คนอื่นเก็บสำเนาบัตรประกันสุขภาพของเราหรือลงชื่อในการอ้างประกันอื่น ๆ
- ตรวจสอบสถานะและการอธิบายผลประโยชน์ของประกัน
- โปรดระวังเมื่อเราสั่งยาหรือซื้อยาผ่านช่องทางออนไลน์ หากราคาถูกจนเกินไปอาจเป็นการหลอกลวงได้

ใครคือกลุ่มเป้าหมายของการหลอกลวง?

- ใครก็ตามสามารถเป็นกลุ่มเป้าหมายของการหลอกลวงได้
- หากเรามักจะคลิกลิงก์ เอกสารแนบ และรูปภาพภายในอีเมลจากแหล่งที่มาที่ไม่รู้จัก เราอาจอยู่ในกลุ่มเสี่ยงและอาจทำให้นักต้มตุ๋นรู้ว่าเราสามารถหลอกได้ง่ายจากข้อความเหล่านั้น

มาเรียนรู้ข้อแนะนำในการอยู่ในโลกออนไลน์ให้ปลอดภัย

กลยุทธ์เพิ่มเติมในการหลีกเลี่ยงการถูกหลอกลวง

- หากข้อเสนอนั้นดูดีจนเกินไป อาจเป็นไปได้ว่านั่นคือการหลอกลวง
- หากการแข่งขัน งาน หรือทุน ขอให้เราจ่ายเงินล่วงหน้า อย่าทำตาม
- ระวังการให้ข้อมูลส่วนบุคคลกับบุคคลหรือองค์กรที่ไม่รู้จักและไม่น่าไว้ใจ
- ติดต่อบุคคล องค์กร หรือองค์กรการกุศลโดยตรง ด้วยการไปพบ เพื่อตรวจสอบข้อเท็จจริง

การหลอกลวงที่พบได้บ่อยบน Facebook

การหลอกลวงด้านความสัมพันธ์คู่รัก

การหลอกลวงด้านการเสี่ยงโชค

การหลอกลวงด้านการกู้ยืม

การขโมยการเข้าถึงรหัส

การหลอกลวงจากการหางาน

เรียนรู้เกี่ยวกับวิธีหลีกเลี่ยงการหลอกลวงบน Facebook ได้ที่: facebook.com/help

สิ่งที่ควรระวังเมื่อซื้อสินค้าออนไลน์

- คนที่มาขอเงินโดยที่เราไม่รู้จักเขาเป็นการส่วนตัว
- คนที่ขอให้เราส่งเงินหรือบัตรกำนัลที่สามารถรับเงินยืม รางวัล หรืออื่น ๆ ได้
- ใครก็ตามที่ขอให้จ่ายเงินเพื่อสมัครงาน
- เพจที่อ้างว่ามาจากบริษัทใหญ่ องค์กร หรือบุคคลสาธารณะที่ไม่ได้รับการตรวจสอบ
- คนที่ขอให้เราเปลี่ยนช่องทางสนทนาไปแพลต์ฟอร์มอื่น
- คนที่อ้างว่าเป็นเพื่อนหรือญาติในกรณีฉุกเฉิน
- คนทีบิดเบือนสถานที่ที่พวกเขาอยู่
- ข้อความหรือโพสที่สะกดคำผิดหรือมีข้อผิดพลาดทางไวยากรณ์
- คนหรือบัญชีผู้ใช้งานที่ให้ไปรับรางวัลที่หน้าเพจ

วิธีรายงานนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัยในข้อความ Facebook

หากเราประสบกับนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัย เมื่อส่งหรือรับเงินในข้อความ เราสามารถรายงานบัญชีผู้ใช้งานนั้นเพื่อตรวจสอบได้

สามารถดูวิธีรายงานนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัยในข้อความFacebookได้ที่: facebook.com/help

วิธีรายงานโพสต์หรือโปรไฟล์บนอินสตาแกรม

รายงานโพสต์ผ่านหน้าฟีด

1. กด ••• (ไอโฟน) หรือ ⋮ (แอนดรอยด์) ด้านบนโพสต์
2. กดรายงาน
3. ปฏิบัติตามคำสั่งบนหน้าจอ

รายงานคนผ่านหน้าโปรไฟล์

1. กดชื่อผู้ใช้งานจากหน้าฟีดหรือสตอรี่ หรือกดค้นหาชื่อผู้ใช้เพื่อไปหน้าโปรไฟล์ และ
2. กด ••• (ไอโฟน) หรือ ⋮ (แอนดรอยด์) บนมุมขวาด้านบนของโปรไฟล์
3. กดรายงาน
4. ปฏิบัติตามคำสั่งบนหน้าจอ

รายงานคนผ่านข้อความ

จำกัดคนผ่านข้อความ:

1. กด หรือ บนมุมขวาด้านบนของหน้าฟีด
2. กดกล่องข้อความของคนที่เราอยากรายงาน
3. กดชื่อบุคคลนั้นด้านบนข้อความ
4. กดรายงาน จากนั้นปฏิบัติตามคำสั่งบนหน้าจอ

เราสามารถเรียนรู้วิธีรายงานโปรไฟล์บนอินสตาแกรมได้ที่:
help.instagram.com/192435014247952

เราสามารถเรียนรู้วิธีรายงานข้อความได้ที่:
help.instagram.com/198034803689028

เราสามารถเรียนรู้วิธีรายงานข้อความได้ที่: help.instagram.com/568100683269916

พูดคุยและพิจารณาตนเอง

- ที่ผ่านมาคุณเคยพบเจอกับการหลอกลวงบนโลกออนไลน์หรือไม่?
- คุณทำอย่างไร?
- แล้วตอนนี้คุณจะทำอย่างไร?

กิจกรรม: แชร์ข้อมูลส่วนบุคคล

แทรกรูปภาพตรงนี้

www.url.com

แทรกรูปภาพตรงนี้

www.url.com

กิจกรรม: ไปฟิชชิงกัน - สังเกตการหลอกลวง

www.url.com

www.url.com

กิจกรรม: ไปฟิชชิงกัน - สังเกตการหลอกลวง

www.url.com

www.url.com

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

_____ คือประเภทของการหลอกลวงที่หลอกให้คนแชร์ข้อมูลการเข้าสู่ระบบหรือข้อมูลส่วนบุคคล

- การสแปม
- การทำฟาร์ม
- การฟิชชิง
- การก่อกวน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

_____ คือประเภทของการหลอกลวงที่หลอกให้คนแชร์ข้อมูลการเข้าสู่ระบบหรือข้อมูลส่วนบุคคล

- การสแปม
- การทำฟาร์ม
- การฟิชชิง
- การก่อกวน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

_____ คือเมื่อนักต้มตุ๋นสร้างบัญชีผู้ใช้งานปลอมหรือตัวตนปลอมเพื่อหลอกให้คนหลงเชื่อว่ากำลังคุยกับบุคคลนั้นจริง ๆ

- การแอบอ้างเป็นคนอื่น
- การทำฟาร์ม
- การสแปม
- การก่อกวน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

_____ คือเมื่อนักต้มตุ๋นสร้างบัญชีผู้ใช้งานปลอมหรือตัวตนปลอมเพื่อหลอกให้คนหลงเชื่อว่ากำลังคุยกับบุคคลนั้นจริง ๆ

- การแอบอ้างเป็นคนอื่น
- การทำฟาร์ม
- การสแปม
- การก่อกวน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

คุณควรตรวจสอบข้อเท็จจริงของสายเรียกเข้าหรืออีเมลจากบริการของรัฐบาลหรือหน่วยงาน โดยการติดต่อผ่านช่องทางทางการที่ให้ไว้ในเว็บไซต์หรือไม่

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

คุณควรตรวจสอบข้อเท็จจริงของสายเรียกเข้าหรืออีเมลจากบริการของรัฐบาลหรือหน่วยงาน โดยการติดต่อผ่านช่องทางทางการที่ให้ไว้ในเว็บไซต์หรือไม่

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 4

กลยุทธ์หนึ่งที่ใช้เพื่อหลีกเลี่ยงการหลอกลวงออนไลน์คือการแชร์ข้อมูลส่วนบุคคลให้กับคนหรือองค์กรที่คุณรู้จักหรือเชื่อใจ

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 4

กลยุทธ์หนึ่งที่ใช้เพื่อหลีกเลี่ยงการหลอกลวงออนไลน์คือการแชร์ข้อมูลส่วนบุคคลให้กับคนหรือองค์กรที่คุณรู้จักหรือเชื่อใจ

ถูก

ผิด

Lesson 2

การซื้อสินค้าออนไลน์อย่างปลอดภัย

การเข้ารหัสจริง ๆ แล้วคืออะไร

- เมื่อเว็บไซต์ถูกเข้ารหัส นั่นหมายความว่าตัวเลขและข้อมูลบนเว็บไซต์ได้รับการป้องกันจากการมองเห็นของบุคคลที่สาม

- เมื่อเราแชร์และรับข้อมูลจากเว็บไซต์เข้ารหัส การส่งต่อข้อมูลนั้นมีความปลอดภัยและสามารถเข้าถึงได้แค่เราและเว็บไซต์นั้น

วิธีสังเกตเว็บไซต์ที่ไม่ถูกเข้ารหัส

- เว็บไซต์ที่ไม่ถูกเข้ารหัสจะไม่ใช้การเชื่อมต่อส่วนตัว
- เราสามารถระบุเว็บไซต์ที่ไม่ถูกเข้ารหัสได้ถ้า:

  ใช้ “http://” แทนการใช้ “https://” ในช่องที่อยู่

  – อินเทอร์เน็ตเบราว์เซอร์บางอันอาจปักธงว่าเป็นเว็บไซต์ที่อันตราย

ข้อมูลเพิ่มเติมเกี่ยวกับวิธีที่เว็บเบราว์เซอร์ตรวจสอบความปลอดภัยจากเว็บไซต์ส่วนบุคคล สามารถดูได้จากที่มานี้:

- Check if a site's connection is secure (Google Chrome Help).
- If Safari says it can't establish a secure connection, or the website is using weak encryption (Apple Support).

พูดคุยและทบทวนตนเอง

- ที่ผ่านมาคุณเคยใช้งานเว็บไซต์ที่ไม่เข้ารหัสหรือไม่?
- คุณใช้มันทำอะไร?
- ปัจจุบันคุณยังใช้เว็บไซต์เหล่านั้นอยู่หรือไม่?
- ทำไม หรือ ทำไมไม่ใช้?

ทำไมการใช้เว็บไซต์ที่เข้ารหัสถึงสำคัญ?

การซื้อของออนไลน์อย่างปลอดภัย

- นอกจากการใช้เว็บไซต์ที่เข้ารหัสแล้ว มีกลยุทธ์หนึ่งที่เราสามารถใช้เพื่อความปลอดภัยในขณะซื้อสินค้าออนไลน์:
- ซื้อสินค้าจากร้านออนไลน์ที่น่าเชื่อถือเท่านั้น
- หยุดคิดก่อนจะซื้อ
- มีการตอบสนองเชิงรุก

แพลตฟอร์มสำหรับซื้อขายบนโลกออนไลน์

- อินเทอร์เน็ตเป็นช่องทางที่ดีในการเชื่อมต่อคนที่ซื้อและขายสินค้าของตัวเอง

- โซเชียลมีเดียหลาย ๆ สื่อรวมถึงแพลตฟอร์มสำหรับการซื้อขายบนโลกออนไลน์ อนุญาตให้ซื้อและขายสินค้าของตัวเองได้

ข้อแนะนำในการซื้อสินค้าอย่างปลอดภัยบนแพลตฟอร์มสำหรับซื้อขายบนโลกออนไลน์

- ให้มั่นใจว่าได้ตรวจสอบข้อแนะนำสินค้าที่เฉพาะเจาะจงว่าอะไรอนุญาตให้ขายบนแพลตฟอร์ม
- ปกป้องความเป็นส่วนตัวและระวังการแชร์รายละเอียดและข้อมูลส่วนบุคคล
- ระวังบัตรกำนัลและการซื้อขายที่ดูดีเกินจริง
- เป็นผู้บริโภคที่มีวิจารณญาณ
- ระวังสินค้าปลอมหรือสินค้าที่ถูกเรียนคืนและเปรียบเทียบราคาสินค้าก่อนการซื้อ
- เช็คเงินสดสามารถปลอมแปลงได้ ดังนั้นให้ใช้การชำระเงินในรูปแบบออนไลน์ เช่น PayPal

ข้อแนะนำในการอยู่อย่างปลอดภัยเมื่อต้องพบเจอบุคคลซื้อ/ขาย

- อย่าแชร์ข้อมูลส่วนบุคคล เช่น ที่อยู่อาศัย แต่ให้ไปเจอในที่สาธารณะแทน สถานที่ที่มีแสงสว่างเพียงพอระหว่างวัน
- วางแผนการพบเจอและแชร์ให้กับเพื่อนที่เราไว้ใจหรือสมาชิกในครอบครัว
- ขอให้ใครบางคนไปด้วยเมื่อเราต้องแลกเปลี่ยนสินค้า
- นำโทรศัพท์ที่ชาร์ตเต็มแล้วติดตัวไปด้วยเผื่อในกรณีที่ต้องติดต่อขอความช่วยเหลือจากใคร

นโยบายการค้าของ Facebook

- นโยบายการค้าของ Facebook ออกกฎว่าสินค้าหรือบริการประเภทไหนที่สามารถขายบน Facebook อินสตาแกรม และวอตส์แอปป์ได้
- ผู้ซื้อและผู้ขายก็ต้องทำตามกฎหมายและข้อกำหนดที่บังคับใช้
- การไม่ทำตามนโยบายอาจส่งผลดังนี้ ถอดรายการขายและเนื้อหาอื่น ๆ ออก ปฏิเสธการแท็กสินค้า การระงับหรือการยุติการเข้าถึงฟีเจอร์การค้าบน Facebook อินสตาแกรมหรือวอตส์แอปป์ทั้งหมด

เรียนรู้เพิ่มเติมเกี่ยวกับนโยบายการค้าของ Facebook เข้าดูได้ที่: facebook.com/policies_center/commerce

ขั้นตอนที่ต้องทำหากเรา ไม่ได้รับอนุมัติ

หากรายการสินค้าถูกปฏิเสธเนื่องจากละเมิดนโยบายการค้าของ Facebook และเรารู้ว่าเป็นข้อผิดพลาด เราสามารถส่งคำร้องขอตรวจสอบโดยปฏิบัติตามขั้นตอนนี้:

- **แพลตฟอร์มสำหรับการซื้อขายบนโลกออนไลน์ของ Facebook:** facebook.com/help/2193854224216494
- **อินสตาแกรม:** help.instagram.com/494867298080532

การรายงานร้านค้าหรือสินค้าบนอินสตาแกรม

รายงานผู้ขาย:

1. ไปที่หน้าโปรไฟล์ของผู้ขายที่ต้องการรายงาน
2. กด (ไอโฟน) หรือ (แอนดรอยด์) มุมขวาด้านบน
3. กดรายงานและทำตามคำสั่งบนหน้าจอ

รายงานสินค้า:

1. ไปที่หน้าเพจสินค้าที่เราต้องการรายงาน
2. กด (ไอโฟน) หรือ (แอนดรอยด์) มุมขวาด้านบน
3. กดรายงานและทำตามคำสั่งบนหน้าจอ

รายงานโพสต์ที่มีการแท็กสินค้า:

1. ไปที่โพสต์ที่มีการแท็กสินค้า
2. กด (ไอโฟน) หรือ (แอนดรอยด์) มุมขวาด้านบน
3. กดรายงานและทำตามคำสั่งบนหน้าจอ

เรียนรู้วิธีรายงานผู้ขายหรือสินค้าบนอินสตาแกรม เข้าดูได้ที่: help.instagram.com/396314741132037

เรียนรู้ว่าเราควรทำอะไรหากเห็นโฆษณาที่เราไม่ชอบบนอินสตาแกรม เข้าดูได้ที่: facebook.com/help/instagram/615366948510230

พูดคุยและทบทวนตนเอง

- คุณเคยซื้อสินค้าจากร้านค้าออนไลน์หรือไม่? มันเป็นไปอย่างไร? หลังจากเรียนเนื้อหาในบทเรียนนี้ คุณจะทำอะไรที่แตกต่างไปจากเดิมหรือไม่? ทำไม หรือ ทำไมไม่ทำ?

- คุณเคยซื้อหรือขายสินค้าในแพลตฟอร์มการซื้อขายสินค้าบนโลกออนไลน์หรือไม่? เป็นอย่างไร? หลังจากเรียนเนื้อหาในบทเรียนนี้ คุณจะทำอะไรที่แตกต่างไปจากเดิมหรือไม่? ทำไม หรือ ทำไมทำไม่?

กิจกรรม: ตรวจสอบแพลตฟอร์มสำหรับซื้อขายของบนโลกออนไลน์

www.url.com

www.url.com

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

เว็บไซต์ที่เข้ารหัสหมายความว่าเราสามารถเชื่อถือองค์กรที่เป็นเจ้าของเว็บไซต์ได้

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

เว็บไซต์ที่เข้ารหัสหมายความว่าเราสามารถเชื่อถือองค์กรที่เป็นเจ้าของเว็บไซต์ได้

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

สัญญาณของเว็บไซต์ที่เข้ารหัสคืออะไร?

เลือกทั้งหมดที่สามารถใช้ได

- **สัญลักษณ์รูปกุญแจ**
- หน้าต่างป๊อปอัพเมื่อเราเข้าเว็บไซต์ที่บอกว่า "ปลอดภัย" ครั้งแรก
- https:// ขึ้นต้น URL
- คะแนน 5 ดาวบนกูเกิ้ล

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

สัญญาณของเว็บไซต์ที่เข้ารหัสคืออะไร?

เลือกทั้งหมดที่สามารถใช้ได

- **สัญลักษณ์รูปกุญแจ**
- หน้าต่างป๊อปอัพเมื่อเราเข้าเว็บไซต์ที่บอกว่า "ปลอดภัย" ครั้งแรก
- https:// ขึ้นต้น URL
- คะแนน 5 ดาวบนกูเกิ้ล

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

การโพสต์บนแพลตฟอร์มการซื้อขายสินค้าบนโลกออนไลน์มักจะเปิดเป็นสาธารณะบนเว็บไซต์

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

การโพสต์บนแพลตฟอร์มการซื้อขายสินค้าบนโลกออนไลน์มักจะเปิดเป็นสาธารณะบนเว็บไซต์

ถูก

ผิด

Lesson 3

การรายงานอาชญากรรมไซเบอร์และการหลอกลวง

การต่อสู้กับการฉ้อโกง: ปกป้องอุปกรณ์ของเรา

- ติดตั้งซอร์ฟแวร์กำจัดมัลแวร์และไวรัส และกดสแกนตามปกติ
- ติดตั้งและอัพเดทแอปพลิเคชัน โปรแกรมเสริม และซอร์ฟแวร์
- ตั้งค่าการตรวจสอบสิทธิ์แบบหลายปัจจัยหรือสองปัจจัยสำหรับบัญชีผู้ใช้งานส่วนบุคคล
- สำรองไฟล์สำคัญและข้อมูลส่วนบุคคลโดยการใช้วิธีที่ปลอดภัย

สังเกตสัญญาณเตือน

- ข้อความที่มีข้อผิดพลาดทางไวยากณ์และการสะกด
- ข้อความที่ต้องตัดสินใจอย่างเร่งด่วน
- ข้อเสนอหรือข้อตกลงที่ดูดีเกินจริง
- ใครบางคนปลอมเป็นบุคคลหรือองค์กรจริง ๆ
- เราถูกขอให้กดลิงก์ เปิดเอกสารแนบ หรือใส่ข้อมูลส่วนบุคคลในเว็บไซต์ภายนอกที่เราไม่รู้จักและไม่น่าเชื่อถือ

เกิดอะไรขึ้นถ้าเราคิดว่าคอมพิวเตอร์เรามีไวรัส?

- ติดตั้งระบบสแกนโดยใช้ซอร์ฟแวร์กำจัดมัลแวร์และไวรัสที่น่าเชื่อถือ
- หากซอร์ฟแวร์ของเราแนะนำให้ดำเนินการ ให้ทำตามคำแนะนำนั้น

ข้อมูลเพิ่มเติมเกี่ยวกับจะเกิดอะไรขึ้นถ้าคอมพิวเตอร์เราได้รับไวรัส เข้าไปดูได้ที่แหล่งที่มาจาก GCFGlobal: Internet Safety: What To Do if Your Computer Gets a Virus.

จะเกิดอะไรขึ้นหากเราเจอการหลอกลวง?

- หากเราให้นักต้มตุ๋นลงชื่อเข้าใช้งานข้อมูลเรา ให้เปลี่ยนรหัสผ่านในทันที
- หากเราใช้รหัสผ่านเดิมสำหรับหลายบัญชีผู้ใช้งานหรือเว็บไซต์ ให้เปลี่ยนรหัสผ่านให้หมด
- สร้างรหัสผ่านใหม่ที่รัดกุมและแตกต่าง
- หากเราจ่ายเงินให้นักต้มตุ๋นผ่านบัตรเครดิตหรือเดบิต ให้ติดต่อธนาคารหรือบริษัทบัตรเครดิตทันที รายงานการหลอกลวงและสอบถามวิธีการที่เราสามารถขอเงินคืน

กิจกรรม: วิธีรายงานการหลอกลวง

www.url.com

www.url.com

การหลอกลวงที่พบได้บ่อยบน Facebook

เรียนรู้เกี่ยวกับวิธีหลีกเลี่ยงการหลอกลวงบนFacebookได้ที่: facebook.com/help/1674717642789671

สิ่งที่ควรระวังเมื่อซื้อสินค้าออนไลน์

- คนที่มาขอเงินโดยที่เราไม่รู้จักเขาเป็นการส่วนตัว
- คนที่ขอให้เราส่งเงินหรือบัตรกำนัลที่สามารถรับเงินยืม รางวัล หรืออื่น ๆ ได้
- ใครก็ตามที่ขอให้จ่ายเงินเพื่อสมัครงาน
- เพจที่อ้างว่ามาจากบริษัทใหญ่ องค์กร หรือบุคคลสาธารณะที่ไม่ได้รับการตรวจสอบ
- คนที่ขอให้เราเปลี่ยนช่องทางสนทนาไปแพลต์ฟอร์มอื่น
- คนที่อ้างว่าเป็นเพื่อนหรือญาติในกรณีฉุกเฉิน
- คนที่บิดเบือนสถานที่ที่พวกเขาอยู่
- ข้อความหรือโพสท์ที่สะกดคำผิดหรือมีข้อผิดพลาดทางไวยากรณ์
- คนหรือบัญชีผู้ใช้งานที่ให้ไปรับรางวัลที่หน้าเพจ

วิธีรายงานนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัยในข้อความ Facebook

หากเราประสบกับนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัยเมื่อส่งหรือรับเงินในข้อความ เราสามารถรายงานบัญชีผู้ใช้งานนั้นเพื่อตรวจสอบได้

สามารถดูวิธีรายงานนักต้มตุ๋นหรือกิจกรรมที่น่าสงสัยในข้อความFacebookได้ที่: facebook.com/help

วิธีรายงานโพสต์หรือโปรไฟล์บนอินสตาแกรม

รายงานโพสต์ผ่านหน้าฟีด

1. กด (ไอโฟน) หรือ (แอนดรอยด์) ด้านบนโพสต์
2. กดรายงาน
3. ปฏิบัติตามคำสั่งบนหน้าจอ

รายงานคนผ่านหน้าโปร์ไฟล์

1. กดชื่อผู้ใช่งานจากหน้าฟีดหรือสตอรี่ หรือกด และค้นหาชื่อผู้ใช้ เพื่อไปหน้าโปรไฟล์
2. กด (ไอโฟน) หรือ (แอนดรอยด์) บนมุมขวาด้านบนของโปรไฟล์
3. กดรายงาน
4. ปฏิบัติตามคำสั่งบนหน้าจอ

รายงานคนผ่านข้อความ

จำกัดคนผ่านข้อความ:

1. กด หรือ บนมุมขวาด้านบนของหน้าฟีด
2. กดกล่องข้อความของคนที่เราอยากรายงาน
3. กดชื่อบุคคลนั้นด้านบนข้อความ
4. กดรายงาน จากนั้นปฏิบัติตามคำสั่งบนหน้าจอ

เราสามารถเรียนรู้วิธีรายงานโปรไฟล์บนอินสตาแกรมได้ที่:
help.instagram.com/192435014247952

เราสามารถเรียนรู้วิธีรายงานข้อความได้ที่:
help.instagram.com/198034803689028

เราสามารถเรียนรู้วิธีรายงานข้อความได้ที่: help.instagram.com/568100683269916

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

อันไหนต่อไปนี้คือวิธีการตอบสนองเชิงรุกในการป้องกันการหลอกลวง?

เลือกตอบทั้งหมดที่เป็นไปได

- ติดตั้งซอร์ฟแวร์กำจัดมัลแวร์และไวรัสในคอมพิวเตอร์
- อัปเดตแอปและซอร์ฟแวร์ในอุปกรณ์ส่วนตัวทั้งหมดเป็นประจำ
- ใช้การตรวจสอบสิทธิ์แบบหลายปัจจัยเมื่อเป็นไปได้
- ใช้อุปกรณ์สาธารณะหรือ Wi-Fi โดยปราศจากการป้องกัน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 1

อันไหนต่อไปนี้คือวิธีการตอบสนองเชิงรุกในการป้องกันการหลอกลวง?

เลือกตอบทั้งหมดที่เป็นไปได

- ติดตั้งซอร์ฟแวร์กำจัดมัลแวร์และไวรัสในคอมพิวเตอร์
- อัปเดตแอปและซอร์ฟแวร์ในอุปกรณ์ส่วนตัวทั้งหมดเป็นประจำ
- ใช้การตรวจสอบสิทธิ์แบบหลายปัจจัยเมื่อเป็นไปได้
- ใช้อุปกรณ์สาธารณะหรือ Wi-Fi โดยปราศจากการป้องกัน

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

การอัปเดตแอปและซอร์ฟแวร์ไม่สำคัญในการรักษาความปลอดภัยของอุปกรณ์ของเรา

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 2

การอัปเดตแอปและซอร์ฟแวร์ไม่สำคัญในการรักษาความปลอดภัยของอุปกรณ์ของเรา

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

_____คือวิธีที่จะป้องกันบัญชีผู้ใช้งานออนไลน์ โดยต้องการข้อมูลเพิ่มเติมในการลงชื่อเข้าใช้บัญชี

ซอร์ฟแวร์กำจัดไวรัส

การตรวจสอบสิทธิ์แบบหลายปัจจัย

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 3

_____คือวิธีที่จะป้องกันบัญชีผู้ใช้งานออนไลน์ โดยต้องการข้อมูลเพิ่มเติมในการลงชื่อเข้าใช้บัญชี

ซอร์ฟแวร์กำจัดไวรัส

การตรวจสอบสิทธิ์แบบหลายปัจจัย

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 4

หากนักต้มตุ๋นฉ้อโกงการซื้อของผ่านบัตรเครดิต แล้วเราไม่เคยได้รับเงินคืนเลย

ถูก

ผิด

กิจกรรม: ตรวจสอบความเข้าใจ

คำถามที่ 4

หากนักต้มตุ๋นฉ้อโกงการซื้อของผ่านบัตรเครดิต แล้วเราไม่เคยได้รับเงินคืนเลย

ถูก

ผิด

LEARNING MODULE

การหลีกเลี่ยง การถูกหลอกลวง

This module was reviewed by Get Safe Online.
To learn more about this partner, visit getsafeonline.org

Meta | We Think Digital