**ข้อสรุปที่ได้จากการถอดประสบการณ์และแลกเปลี่ยนเรียนรู้**

**เรื่อง *สังคมออนไลน์***

***PHISHINGหรือเว็บหลอกลวง***

**Phishing** คือ คำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมล์ หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น ในบทความนี้จะเน้นในเรื่องของ **Phishing** ที่มีจุดมุ่งหมายเพื่อหลอกลวงทางการเงิน เนื่องจากจะทำให้ผู้อ่านมองเห็นผลกระทบได้ง่าย

**FACEBOOK ปลอมสังเกตจาก URL**

****

***รูปแบบการหลอกลวง***

-2-

**1. การประมูลสินค้าทางอินเทอร์เน็ตโดยหลอกลวง (Internet Auction Fraud)**

 การโฆษณาขายสินค้าทางอินเทอร์เน็ตด้วยวิธีการประมูลสินค้า ผู้ซื้อที่สนใจจะเข้าร่วมการ

ประมูลมักต้องลงทะเบียนเป็น สมาชิกของเว็บไซต์นั้นๆ ซึ่งโดยทั่วไปจะไม่เสียค่าใช้จ่ายใดๆ หลังจากนั้นจะได้รับหมายเลขสมาชิกและรหัสผ่าน (password) ผู้ซื้อจะต้องเสนอราคาซื้อแข่งขันกับผู้ซื้อรายอื่น เมื่อเสร็จสิ้นการประมูลถือว่ามีการทำสัญญาซื้อขายระหว่างผู้ประมูลและผู้ เสนอขาย โดยจะมีการส่งข้อความทางอีเมล์ (e-mail) แจ้งให้ผู้ซื้อและผู้ขายทราบผลการประมูล และแจ้งรายละเอียดที่จะติด ต่อกันได้ เพื่อให้ทั้งฝ่ายผู้ซื้อขและผู้ขายติดต่อกันในเรื่องการชำระเงินและการส่งมอบสินค้า

**ลักษณะการหลอกลวง :**

 การประมูลสินค้าทางอินเทอร์เน็ต เป็นวิธีการซื้อขายสินค้าที่ได้รับความนิยม และเป็นช่อง

ทางการติดต่อซื้อขายสินค้าที่ สะดวกรวดเร็ว ในรายงานสำรวจที่กล่าวมาแล้วของบางประเทศพบว่า เป็นวิธีการหลอกลวงที่พบมากที่สุดเช่นกัน การหลอกลวง มีหลายรูปแบบ เช่น ผู้ขายไม่ส่งมอบสินค้าที่ผู้ซื้อประมูลได้ เพราะไม่มีสินค้าอยู่จริง, การหลอกลวงโดยการปั่นราคาซื้อขาย ผู้ขายหรือบุคคลที่เกี่ยวข้องกับผู้ขายจะเข้าเสนอราคาเพื่อประมูลสินค้าของตน เพื่อให้สินค้ามีราคาสูงขึ้น ทำให้ผู้ซื้อต้องซื้อ สินค้าในราคาที่สูงเกินจริง เป็นต้น

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ซื้อได้ชำระค่าสินค้าให้แก่ผู้ขายแล้ว แต่ยังไม่ได้รับสินค้า หรือได้รับสินค้าที่ชำรุดเสียหาย

หรือเป็นสินค้าที่มีลักษณะ ไม่ตรงกับที่มีการเสนอขายแต่แรก ด้านผู้ให้บริการประมูลทางอินเทอร์เน็ตเองก็อาจได้รับความเสียหาย เพราะผู้ใช้บริการ (ผู้ซื้อและผู้ขาย) ไม่ให้ความไว้วางใจและไม่ใช้บริการ

**วิธีการป้องกัน :**

 ผู้ซื้อควรตรวจสอบว่าเว็บไซต์ที่ทำหน้าที่เป็นผู้ให้บริการด้านการประมูลทางอินเทอร์เน็ต

(คนกลาง) มีวิธีการระบุตัวบุคคลที่ เป็นผู้ขาย (หรือผู้ซื้อ) ดีพอหรือไม่ กล่าวคือมีการเก็บประวัติ รายละเอียดของผู้ขาย ที่สามารถติดต่อได้ หรือพิจารณาว่าผู้ให้ บริการด้านการประมูลทางอินเทอร์เน็ต (คนกลาง) มีนโยบายการประกันความเสียหายที่อาจเกิดขึ้นหรือไม่ โดยเฉพาะอย่างยิ่ง สำหรับสินค้าที่มีมูลค่าค่อนข้างสูง

**2. การให้บริการอินเทอร์เน็ตโดยหลอกลวง (Internet Service Provider Scams)**

 ผู้หลอกลวงจะส่งเช็คจำนวนหนึ่ง (เช่นราว 3.5 ดอลลาร์สหรัฐฯ) ให้แก่ผู้ใช้บริการ เมื่อมีการ

เบิกเงินตามเช็คแล้ว ก็ถือว่าผู้ บริโภคตกลงที่จะใช้บริการของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider - ISP) ที่ได้รับแจ้ง ในการนี้อาจจะไม่มีการ แจ้งค่าธรรมเนียมหรือค่าใช้จ่ายใดๆ และมักเป็นการทำ

-3-

สัญญาให้บริการอินเทอร์เน็ตที่มีระยะเวลานาน ผู้หลอกลวงจงใจให้ผู้ บริโภคหรือผู้ใช้บริการเกิดความสับสนและเข้าใจผิดในสาระสำคัญเกี่ยวกับการบริการนั้น กล่าวคือเมื่อผู้บริโภคเข้าทำสัญญา ดังกล่าวแล้วจะถือว่ายินยอมตามเงื่อนไขทุกประการที่ระบุไว้ การหลอกลวงดังกล่าวนี้มักพบในประเทศที่มีผู้ให้บริการ อินเทอร์เน็ตหลายรายและมีบริการที่หลากหลาย

**ลักษณะการหลอกลวง :**

 ผู้บริโภคถูกเรียกเก็บเงินค่าบริการต่างๆ จากผู้ให้บริการอินเทอร์เน็ต นอกจากนี้ ยังอาจจะมี

คำขู่ที่กล่าวว่าถ้าหากผู้ใช้บริการ ต้องการเลิกสัญญาก่อนครบกำหนดสัญญา จะถูกปรับเป็นจำนวนเงินที่สูง

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้บริโภคถูกเรียกเก็บเงินค่าบริการต่างๆ จากผู้ให้บริการอินเทอร์เน็ต นอกจากนี้ ยังอาจจะมี

คำขู่ที่กล่าวว่าถ้าหากผู้ใช้บริการ ต้องการเลิกสัญญาก่อนครบกำหนดสัญญา จะถูกปรับเป็นจำนวนเงินที่สูง

**วิธีการป้องกัน :**

 เมื่อผู้บริโภคได้รับเช็คโดยไม่ทราบสาเหตุที่ชัดเจนแล้ว ไม่ควรทำข้อตกลงใดๆ กับบุคคลอื่น

 แต่ควรศึกษารายละเอียด ของเอกสารหรือข้อตกลงที่ส่งมาโดยถี่ถ้วน ตรวจสอบค่าใช้จ่ายต่างๆ ที่จะถูกเรียกเก็บให้ครบถ้วน และควรติดต่อผู้ให้ บริการอินเทอร์เน็ตโดยตรง

**3. การใช้บัตรเครดิตโดยไม่ได้รับอนุญาต (Credit Card Fraud)**

 การชำระค่าสินค้า ค่าบริการทางอินเทอร์เน็ตที่ได้รับความนิยมที่สุดวิธีหนึ่งคือ การชำระเงิน

ด้วยบัตรเครดิต เนื่องจากมี ความสะดวกแก่ทั้งผู้ซื้อและผู้ขาย ผู้ซื้อสามารถชำระเงินโดยการให้ข้อมูลบัตรเครดิตคือ หมายเลขบัตรเครดิต ชื่อ-สกุลของ ผู้ถือบัตร และวันหมดอายุแก่ร้านค้า ร้านค้าสามารถตรวจสอบได้เพียงว่า บัตรดังกล่าวเป็นบัตรที่ออกโดยผู้ออกบัตรจริง แต่ไม่สามารถตรวจสอบตัวบุคคลผู้ใช้บัตรได้ว่าเป็นบุคคลใด

**ลักษณะการหลอกลวง :**

 วิธีการหลอกลวงเกี่ยวกับการชำระเงินด้วยบัตรเครดิตทางอินเทอร์เน็ตมีหลายวิธี ตัวอย่างเช่น

การให้บริการดูภาพลามก อนาจารโดยไม่เสียค่าใช้จ่ายใดๆ สำหรับผู้ที่มีอายุตั้งแต่ 18 ปีขึ้นไป (ตามกฎหมายสหรัฐอเมริกา) แต่ผู้บริโภคต้องแจ้ง ข้อมูลบัตรเครดิตให้ผู้ให้บริการทราบ เพื่อตรวจสอบความถูกต้องของข้อมูล แล้วผู้หลอกลวงจะใช้ข้อมูลนี้ไปกระทำผิดในที่อื่น

-4-

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ถือบัตรที่เป็นผู้บริโภคถูกเรียกเก็บเงินค่าสินค้าหรือบริการจากบริษัทหรือธนาคารผู้ออก

บัตร ทั้งที่ผู้ถือบัตรไม่ได้ใช้บัตร เครดิตชำระรายการนั้นๆ เลย ซึ่งกฎหมายบางประเทศจะให้ความคุ้มครองผู้ถือบัตรในกรณีนี้ หรือผู้ถือบัตรรับผิดไม่เกิน จำนวนเงินที่กำหนดไว้ในข้อตกลงระหว่างผู้ออกบัตรและผู้ถือบัตร

**วิธีการป้องกัน :**

 ผู้ถือบัตรเครดิตไม่ควรแจ้งข้อมูลบัตรเครดิตให้บุคคลอื่นทราบ แต่หากต้องมีการชำระเงิน

ด้วยบัตรเครดิตทางอินเทอร์เน็ต ก็ควรเลือกร้านค้าที่มีความน่าเชื่อถือ หรือมีหลักแหล่งที่แน่นอนสามารถติดต่อได้ หรือผู้บริโภคอาจเลือกใช้บัตรที่มีวิธีการ ตรวจสอบตัวบุคคลผู้ใช้บัตรว่าเป็นผู้ถือบัตร เช่น การใช้รหัสประจำตัว (PIN) หรือรหัสใดๆ ที่ไม่ปรากฎอยู่บนบัตร แต่ถือ เป็นข้อมูลส่วนตัวของผู้ถือบัตรที่ไม่เปิดเผยให้บุคคลอื่นทราบ นอกจากนี้ ผู้ถือบัตรควรตรวจดูข้อตกลงที่ทำไว้กับผู้ออกบัตร ด้วยว่ามีเงื่อนไขความรับผิดชอบอย่างไร

**4. การเข้าควบคุมการใช้โมเดมของบุคคลอื่น (International Modem Dialing/ Modem Hijacking)**

**ลักษณะการหลอกลวง :**

 การโฆษณาการให้บริการสื่อลามกอนาจารโดยไม่เสียค่าใช้จ่ายใดๆ ผู้ใช้บริการจะต้องติดตั้ง

โปรแกรมคอมพิวเตอร์เพื่อดู ภาพดังกล่าวหรือเรียกว่า ‘viewer’ หรือ ‘dialer’ ของผู้ให้บริการ เมื่อผู้ใช้บริการเปิดดูภาพด้วยโปรแกรมข้างต้นแล้ว การทำงาน ของโปรแกรมดังกล่าวจะเริ่มเมื่อมีการใช้เครื่องโมเดม (modem) ในขณะเดียวกันโปรแกรมฯ จะควบคุมการทำงานของโมเดม และสั่งให้หยุดการทำงานโดยที่ผู้ใช้บริการไม่รู้ตัว แล้วจะสั่งให้มีการต่อเชื่อมผ่านโมเดมอีกครั้งหนึ่ง โดยเป็นการใช้โทรศัพท์ ทางไกลจากที่ใดที่หนึ่ง แล้วมีการใช้อินเทอร์เน็ตอีกครั้งจากที่นั้น เพื่อให้ผู้ใช้บริการสามารถดูเว็บไซต์

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ใช้บริการจะถูกเรียกเก็บเงินค่าโทรศัพท์ทางไกลจำนวนมาก ทั้งที่ผู้ใช้บริการอาจไม่รับรู้ ซึ่ง

เป็นเพราะมีบุคคลอื่น ลักลอบใช้โทรศัพท์โดยอาศัยโปรแกรมคอมพิวเตอร์ดังกล่าว

**วิธีการป้องกัน :**

-5-

 ผู้ใช้บริการหรือผู้บริโภคควรหลีกเลี่ยงไม่ติดตั้งโปรแกรมคอมพิวเตอร์ สำหรับการให้บริการ

ใดๆ โดยไม่เสียค่าใช้จ่าย โดยเฉพาะอย่างยิ่งการดูเว็บไซต์ที่มีข้อมูลภาพลามกอนาจาร และควรตรวจสอบเงื่อนไขและค่าใช้จ่ายต่างๆ ถ้าพบสิ่งผิดปกติ ต้องแจ้งระงับการใช้งานกับผู้ให้บริการทันที นอกจากนั้น ผู้ใช้บริการควรตรวจสอบใบแจ้งหนี้ค่าบริการโทรศัพท์อย่างสม่ำเสมอ

**5. การหลอกลวงให้ใช้บริการเกี่ยวกับเว็บไซต์ (Web Cramming)**

**ลักษณะการหลอกลวง :**

 การหลอกลวงว่ามีการให้บริการเปิดเว็บเพจ (web page) โดยไม่เสียค่าใช้จ่ายใดๆ เช่นการ

เปิดเว็บเพจเป็นเวลา 30 วัน และไม่มีข้อผูกพันใดๆ ถ้าไม่ใช้บริการต่อไป

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 เมื่อมีการตกลงใช้บริการดังกล่าวแล้ว ผู้ใช้บริการจะถูกเรียกเก็บเงินค่าใช้บริการโทรศัพท์

หรือค่าใช้บริการในการมี เว็บเพจ (ค่าธรรมเนียมการใช้พื้นที่) เป็นจำนวนมาก ทั้งๆ ที่ตนไม่เคยใช้บริการหรือไม่ได้สมัครแต่อย่างใด ผู้ใช้บริการยังไม่ สามารถแจ้งให้ผู้ให้บริการยกเลิกได้ทันทีอีกด้วย

**วิธีการป้องกัน :**

 ผู้บริโภคควรตรวจสอบข้อมูลเกี่ยวกับผู้ให้บริการ และเลือกใช้บริการที่มีความน่าเชื่อถือ

เท่านั้น (กรณีนี้มักพบใน ประเทศที่มีผู้ให้บริการโทรศัพท์จำนวนมากเช่นในประเทศสหรัฐอเมริกา เป็นต้น)

**6. การหลอกลวงโดยใช้การตลาดหรือการขายแบบตรง (Multilevel Marketing Plans/ Pyramids)**

**ลักษณะการหลอกลวง :**

 การหลอกลวงในลักษณะนี้คล้ายคลึงกับการนำสื่อโฆษณาในการทำตลาดหรือการขายตรง

 โดยมีการชักชวนให้บุคคลทั่วไปเข้าร่วมเป็นสมาชิกในเครือข่ายธุรกิจ โดยการกล่าวอ้างว่าผู้ขายจะได้รับสิทธิในการจำหน่ายสินค้าหลายชนิด และได้รับผลประโยชน์จากการขายสินค้าหรือชักชวนบุคคลอื่นเข้ามาเป็นตัวแทนขายตรง เป็นทอดๆ ทำให้ผู้ที่ได้รับประโยชน์จริงมีจำนวนน้อยราย

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้บริโภคที่เข้าร่วมเครือข่ายจะต้องชำระค่าสมาชิกจำนวนหนึ่ง แต่จะไม่มีรายได้ประจำแต่

อย่างใด รายได้ของผู้บริโภคจึงไม่แน่นอนและมักจะไม่ได้รับผลประโยชน์ตามที่ผู้หลอกลวงกล่าวอ้าง เพราะไม่สามารถขายสินค้าได้ตามเป้าหมาย

**วิธีการป้องกัน :**

-6-

 ผู้บริโภคควรระมัดระวังในการสมัครเป็นสมาชิกหรือตัวแทนจำหน่ายสินค้า ที่ต้องหาสมาชิก

รายอื่นเพิ่มขึ้นหรือต้อง จำหน่ายสินค้าที่มีราคาค่อนข้างสูงให้ได้ตามยอดจำหน่ายที่กำหนด เพราะอาจถูกหลอกลวงได้

**7. การหลอกลวงโดยเสนอให้เงินจากประเทศไนจีเรีย (Nigerian Money Offers)**

**ลักษณะการหลอกลวง :**

 ผู้ใช้อินเทอร์เน็ตจะได้รับข้อความจากจดหมายหรืออีเมล์ (e-mail) จากบุคคลที่กล่าวอ้างว่ามี

ความสำคัญในประเทศไนจีเรีย เพื่อขอช่วยเหลือในการโอนเงินจำนวนมากไปยังต่างประเทศ โดยผู้บริโภคจะได้รับเงินส่วนแบ่งจำนวนนับล้านเหรียญ ดอลลาร์สหรัฐฯ ข้อความในจดหมายหรืออีเมล์มีเนื้อหาทำนองว่า ประชาชนในประเทศไนจีเรียไม่สามารถเปิดบัญชีเงินฝากในต่างประเทศ หรือโอนเงินออกนอกประเทศที่มีมูลค่าราว 10 ล้านดอลลาร์สหรัฐฯ ได้ หรือรัฐบาลไนจีเรียต้องการทำธุรกิจกับชาวต่างชาติ จึงต้องการความช่วยเหลือจากชาวต่างชาติในการเปิดบัญชีเงินฝากประเภทกระแสรายวันที่เบิกด้วยเช็ค ซึ่งท่านจะได้รับค่า ตอบแทนหรือค่านายหน้า ผู้บริโภคเพียงแต่แจ้งรายละเอียดของบัญชีเงินฝากของตน และกรอกเอกสารพร้อมทั้งลงลายมือชื่อ ของเจ้าของบัญชีเท่านั้น

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 เมื่อมีการแจ้งข้อมูลบัญชีเงินฝากแล้ว ผู้บริโภคจะถูกเรียกเก็บค่าธรรมเนียมหรือค่าใช้จ่ายใน

การดำเนินการตลอดเวลา โดยให้ผู้บริโภคโอนเงินเข้าบัญชีที่แจ้งไว้ ผู้ที่หลอกลวงจึงสามารถเบิกเงินจากบัญชีดังกล่าวได้โดยอ้างเอกสารมอบอำนาจของเจ้า ของบัญชี แต่การโอนเงินลักษณะนี้อาจทำไม่ได้ในประเทศไทย เว้นแต่จะเป็นการโอนเงินระหว่างบัญชีของธนาคารเดียวกัน ทางอินเทอร์เน็ต

**วิธีการป้องกัน :**

 ผู้บริโภคไม่ควรหลงเชื่อบุคคลอื่นที่อ้างตัวและเสนอจะให้ผลประโยชน์จำนวนมหาศาลโดย

ไม่มีความเสี่ยงเช่นนี้ และ ไม่ควรเปิดเผยข้อมูลบัญชีธนาคารของตนแก่ผู้อื่นด้วย

**8. การหลอกลวงให้ประกอบธุรกิจที่บ้าน (Work-at-Home)**

**ลักษณะการหลอกลวง :**

 บริษัทที่หลอกลวงจะเชิญชวนให้ผู้ต้องการประกอบธุรกิจทางอินเทอร์เน็ตหรือธุรกิจด้าน

พาณิชย์อิเล็กทรอนิกส์ สมัครเป็นสมาชิกเพื่อทำธุรกิจ โดยผู้บริโภคมีเพียงเครื่องคอมพิวเตอร์และสามารถใช้อินเทอร์เน็ตจากที่บ้านได้ และมักอ้าง ว่าธุรกิจประเภทนี้เป็นธุรกิจที่เติบโตอย่างรวดเร็ว ในขณะที่ผู้บริโภค

-7-

จะไม่ได้รับคำแนะนำในการทำธุรกิจ ไม่มีข้อมูลธุรกิจ ที่ชัดเจนหรือไม่ทราบว่าตนอาจไม่ได้รับค่าตอบแทนใดๆ เลย ผู้ถูกหลอกลวงจะถูกเรียกเก็บเงินค่าสมาชิกหรือซื้ออุปกรณ์ที่ จำเป็นเพื่อเริ่มทำธุรกิจ

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ลงทุนจะไม่ได้รับเงินค่าตอบแทนตามที่มีการกล่าวอ้าง และอาจต้องสูญเสียเงินจากการ

ลงทุนอีกด้วย

**วิธีการป้องกัน :**

 ผู้ที่ต้องการลงทุนหรือต้องการเป็นเจ้าของกิจการ ควรศึกษาหรือสอบถามรายละเอียดของ

ประเภทธุรกิจที่จะลงทุนการจ่าย เงินค่าตอบแทนที่ผู้บริโภคจะได้รับ ที่มีกำหนดเวลาที่แน่นอนรวมถึงค่าใช้จ่ายทั้งหมดที่จะต้องจ่ายในการเริ่มต้นทำธุรกิจ และผู้บริโภคควรระวังไม่หลงเชื่อคำเชิญชวนของผู้ที่อ้างว่าเป็นธุรกิจที่สร้างรายได้จำนวนมากภายในระยะเวลาสั้นๆ

**9. การหลอกลวงให้จดทะเบียนโดเมนเนม (Domain name registration scams)**

**ลักษณะการหลอกลวง :**

 ผู้ที่ต้องการทำธุรกิจทางอินเทอร์เน็ตที่ต้องการมีเว็บไซต์และโดเมนเนมของตนเอง จะได้รับ

การเสนอแนะว่า ท่านสามารถได้รับสิทธิในการจดทะเบียนโดเมนเนมในระดับบนที่เรียกว่า “Generic Top-Level Domain’ หรือ gTLD ได้แก่ .com, .org, .net, .int, .edu, .gov, .mil, .aero, .biz, .coop, .info, .museum, .name, and .pro เป็นต้น ก่อนบุคคลอื่น และถูกเรียกเก็บค่าธรรมเนียมในการจองโดเมนเนมที่ต้องการ ซึ่งในความเป็นจริงไม่มีการให้บริการในลักษณะดังกล่าว

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ที่หลงเชื่ออาจได้รับความเสียหายเพราะได้ชำระเงินให้แก่ผู้ที่หลอกลวง โดยไม่ได้รับสิทธิ

หรือประโยชน์ตามที่กล่าวอ้าง

**วิธีการป้องกัน :**

 หลีกเลี่ยงการใช้บริการการขอจดทะเบียนโดเมนเนมล่วงหน้า ที่ให้การรับรองว่าจะได้รับ

สิทธิ ในการเลือกโดเมนเนมประเภทนี้ (gTLD) ก่อนบุคคลอื่น และไม่ควรหลงเชื่อคำโฆษณา ควรติดตามข่าวสารเกี่ยวกับการยื่นขอจดทะเบียนจากผู้รับจดทะเบียนที่ได้รับสิทธิภายใน ประเทศหรือเว็บไซต์ของ [ICANN](http://www.icann.org/) (Internet Corporation for Assigned Names and Numbers) (www.icann.org) ควรใช้บริการจดทะเบียนโดเมนเนมกับหน่วยงานที่น่าเชื่อถือ เช่น ผู้ให้บริการอินเทอร์เน็ต, บริษัทที่ประกอบธุรกิจเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ หรือใช้บริการของ “ศูนย์สารสนเทศเครือข่ายแห่งประเทศไทย” (Thailand Network Information Center – THNIC) (www.thnic.net)

-8-

**10. การหลอกลวงโฆษณาหรือขายยามหัศจรรย์ (Miracle products)**

**ลักษณะการหลอกลวง :**

 การโฆษณาหรือขายยาทางอินเทอร์เน็ตที่อ้างสรรพคุณว่าสามารถรักษาโรคหรืออาการ

เจ็บป่วยด้วยโรคร้ายแรง เช่น โรคมะเร็ง, โรคภูมิคุ้มกันบกพร่อง (HIV/AIDS), โรคความดันโลหิตสูง ฯลฯ หรือสามารถบรรเทาความเจ็บป่วยได้ภายในระยะเวลาอันสั้น และมักอ้างว่ายาเหล่านี้ได้รับการรับรองหรือการพิสูจน์ทางวิทยาศาสตร์แล้ว

**ความเสียหายที่อาจเกิดขึ้นได้ :**

 ผู้ป่วยที่ซื้อยาดังกล่าวโดยเชื่อว่าสามารถรักษาความเจ็บป่วยได้ อาจต้องสูญเสียเงินหรือ

โอกาสในการได้รับการรักษาอย่างถูกต้อง นอกจากนั้น ยังอาจได้รับอันตรายจากการใช้ยาเหล่านั้นด้วย

**วิธีการป้องกัน :**

 การใช้ยารักษาโรคควรได้รับคำแนะนำจากแพทย์หรือเภสัชกรเท่านั้น

***PHISHING ฟิสชิ่งระวังได้***

1. ไม่เปิดลิงก์ที่แนบมาในอีเมล์ดีที่สุด
2. พึงระวังอีเมล์ที่ขอให้กรอกข้อมูลส่วนบุคคล
3. สังเกตให้แน่ใจว่าเว็บไซต์ที่ใช้งานเป็น **https://** ก่อนให้ข้อมูลส่วนบุคคลที่สำคัญ
4. ลบอีเมล์น่าสังสัยออกไป เพื่อไม่ให้พลั้งเผลอกดเปิดครั้งถัดไป......สุดท้ายคือ ระมัดระวังอยู่

เสมอทุกครั้งที่เข้า **Internet** อย่าไว้ใจอะไรง่ายจนเกินไป เพราะอย่าลืมว่า มิจฉาชีพจ้องดูอยู่เสมอ

***ข้อควรระวังก่อนซื้อของออนไลน์***

1. ตรวจสอบเว็บไซต์ที่ทำการสั่งซื้อของออนไลน์ว่ามีความน่าเชื่อถือหรือไม่
2. การเพิ่มความระมัดระวังในการเลือกซื้อสินค้าผ่านระบบออนไลน์
3. หากมีการสั่งซื้อ ควรเก็บหลักฐานต่าง ๆ ไว้ให้ได้มากที่สุด
4. กรณีที่ถูกหลอกลวง ควรแจ้งเจ้าหน้าที่ตำรวจ
5. ดูรีวิวสินค้าหรือบริการก่อนเสมอ ๆ
6. ติดต่อขอที่อยู่ผู้ขายทุกครั้ง
7. สังเกตในเรื่องของการทำธุรกรรม

-9-

***ข้อควรระวังในการใช้ Social Network***

1. ไม่ควรระบุ ข้อมูลส่วนตัวให้แสดงเกินความจำเป็น เช่น ว/ด/ป สถานที่เกิด
2. วางแผนจะเดินทางไปท่องเที่ยวที่ไหน อย่างไร เมื่อไร ไม่จำเป็นต้องบอกหรือแสดงเอาไว้ใน Wall

หรือ New Feed

1. ที่อยู่ บ้านที่ทำงาน ต่าง ๆ ไม่ควรนำมาแสดงไว้โดยไม่จำเป็น
2. นำเรื่องขององค์กร บริษัท หรือข้อมูลทางการเงินไปโพสไว้ในสังคมออนไลน์
3. ไม่ระบุชื่อบุตรหลาน ระบุภาพหรือติด tag ในรูปภาพมากเกินไป อาจทำให้เกิดอันตรายจากคนที่ไม่

หวังดี

1. การตั้งความเป็นส่วนตัว และการปล่อยให้ Face book ค้นหาพบคุณได้จำกัดลงบ้าง

***เหตุผลที่ห้ามเด็กอายุต่ำกว่า 13 ปี เล่น Instagram***

**1. ป้องกันการเข้าถึงข้อมูลส่วนตัวของ “เด็ก”**

เนื่องจาก Social Media เหล่านี้คอยเก็บข้อมูลของเราตลอดเวลา เช่น ข้อมูลส่วนตัว พฤติกรรมเพื่อนำไปทำการตลาดหาลู่ทางในการโฆษณา

**2. เสี่ยงต่อการสื่อสารที่ผิดพลาด**

สมองในการตัดสินใจและกระบวนการคิดของเด็กยังไม่สมบูรณ์ เพราะสมองยังพัฒนาไม่เต็มที่ เสี่ยงต่อการติดต่อสื่อสารที่ผิดพลาดเกิดผลเสียต่อตนเองและผู้อื่นได้

**3. ป้องกันการเข้าถึงของมิจฉาชีพ**

 การโพสตำแหน่งปัจจุบันของเด็ก รูปภาพ วีดีโอหรือคลิปเสียง ก็สามารถระบุลักษณะเฉพาะของเด็กเสี่ยงต่อการทำให้มิจฉาชีพเข้าถึงตัวเด็กได้ง่าย

**4. ป้องกันการเสียเงินฟรี**

 อุปกรณ์จำพวก Smartphone หรือ Tablet อาจทำให้คุณเสียเงินไปฟรี ๆ กับการโหลดข้อมูล app โดยความไม่รู้เรื่องรู้ราวของเด็ก (แม้ว่า apps นั้นจะฟรีก็ตาม)

**5. จุดเริ่มต้นของการโกหก**

-10-

ถึง Social media อย่าง instagram จะป้องกันในขั้นตอนการสมัคร โดยการไม่มีอายุต่ำกว่า 13 ให้เลือกอาจทำให้เด็กโกงอายุของตัวเองได้ ถึงจะเป็นเรื่องเล็กน้อยแต่ก็เป็นจุดเริ่มต้นของการฝึก “ละเมิดกฎ”

***กฎหมายคอมพิวเตอร์น่ารู้***

1. ขโมย ID และ PASSWORD

 การนำไอดีและพาสเวิร์ดของผู้อื่นไปใช้งานโดยที่เจ้าของไม่อนุญาต

***ผิดกฎหมาย สามารถฟ้องร้องเรียกค่าเสียหาย 100,000 บาท***

2. โพสต์ข้อความด่า

 การโพสต์ข้อความด่า หรือจงใจกล่าวหา ใส่ร้ายผู้อื่น

 ***จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 100,000 บาท***

3. การนำข้อมูลของผู้อื่นไปเผยแพร่ แก้ไข หรือดัดแปลงเนื้อหา โดยที่เจ้าของไม่อนุญาต และสร้างความ

 เสียหายให้บุคคลนั้น

***จำคุกไม่เกิน 1-5 ปี ปรับไม่เกิน 100,000 ถึง 200,000 บาท หรือทั้งจำทั้งปรับ***

4. แชร์สื่อลามก การแชร์ข้อมูลที่ลามก หรือสื่อให้เห็นถึงเนื้อหนัง ใต้ร่มผ้า

 ***จำคุกไม่เกิน ปี ปรับไม่เกิน 100,000 บาท***

5. เอารูปของผู้อื่นไปแชร์

 การนำรูปของผู้อื่นไปแชร์ หรือไปดัดแปลงทำให้ผู้อื่นเสียหาย เกิดการอับอาย

 ***จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 100,000 บาท***

6. ส่งอีเมล์ลูกโซ่

 การส่งอีเมล์ลูกโซ่ หรือการส่งข้อความไปรบกวนผู้อื่น โดยปกปิดที่มา

 ***ปรับไม่เกิน 100,000 บาท***

**คณะผู้จัดทำ KM**

1. รองศาสตราจารย์สุนี โชติดิลก

2. อาจารย์โสภณา จิรวงศ์นุสรณ์

3. อาจารย์พวงผกา ภูยาดาว

4.อาจารย์มงคล เจริญโต

5. อาจารย์สันติเลิศ เพ็ชรอาภรณ์

6. อาจารย์นวินครุธวีร์

7.อาจารย์ศุภกาญน์ วิชานาติ

8.อาจารย์พัฒนพงษ์ จันทร์ควง