

## เผยโฉม 10 กลโกงทางอินเทอร์เน็ต (Internet Fraud)

อินเทอร์เน็ตเป็นสื่อที่ทำให้คนทั่วโลกสามารถติดต่อถึงกันได้แบบปฏิสัมพันธ์ กล่าวคือ ผู้รับและผู้ส่งข้อมูลสามารถสื่อสารและโต้ตอบข้อความกันได้ทันที ในรูปแบบมัลติมีเดีย อีกทั้งยังลดข้อจำกัดเรื่องระยะเวลาและสถานที่ในการแลกเปลี่ยนข้อมูลและการทำธุรกิจ ผู้ซื้อและผู้ขายได้รับความสะดวกในการซื้อขายและการโฆษณาสินค้าหรือบริการ อินเทอร์เน็ตทำให้การประกอบธุรกิจผ่านสื่ออิเล็กทรอนิกส์หรือ "พาณิชย์อิเล็กทรอนิกส์" มีประสิทธิภาพและได้รับความนิยมในปัจจุบันมากขึ้น

อย่างไรก็ดี การใช้อินเทอร์เน็ตอาจจะถูกนำไปใช้ในแง่ลบเพื่อหลอกลวงบุคคล เช่นเดียวกันกับการซื้อขายตามปกติ เนื่องด้วยผู้ใช้อินเทอร์เน็ตในการทำธุรกรรม อาจไม่ทราบตัวบุคคลของผู้ที่ติดต่อว่าเป็นบุคคลใด โดยเฉพาะอย่างยิ่งเมื่อไม่เคยพบเห็นกันมาก่อน

### ข้อมูล สถิติ

จากการศึกษาข้อมูล สถิติเรื่องการใช้อินเทอร์เน็ตเมื่อกลางปี พ.ศ. 2544 (อ้างอิงจาก Nua Internet Survey, สิงหาคม 2544) มีการประมาณการว่าจำนวนผู้ใช้อินเทอร์เน็ตทั่วโลกสูงถึง 513 ล้านคน หรือคิดเป็นร้อยละ 8.46 ของประชากรทั่วโลก สำหรับภูมิภาคเอเชีย-แปซิฟิก มีจำนวนกว่า 144 ล้านคน สำหรับข้อมูลจำนวนผู้ใช้อินเทอร์เน็ตในประเทศไทยระหว่างเดือนมกราคมถึงมีนาคม 2544 สืบค้นโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ร่วมกับสำนักงานสถิติแห่งชาติ พบว่ามีจำนวน 3.5 ล้านคน (<http://ntl.nectec.or.th/internet>) นอกจากนี้ รายงานสำรวจเรื่อง "การหลอกลวงทางอินเทอร์เน็ต" เมื่อปี พ.ศ. 2543 ของหน่วยงานของสหรัฐอเมริกาที่ชื่อว่า "National Fraud Information Center" ซึ่งมีหน้าที่รับเรื่องร้องเรียนจากประชาชนเกี่ยวกับการซื้อขายสินค้าและบริการทางอินเทอร์เน็ต พบว่าในช่วงครึ่งหลังของปีเดียวกัน มีการร้องเรียนเป็นจำนวนทั้งสิ้น 20,014 เรื่อง และเมื่อรวมมูลค่าความเสียหายตลอดทั้งปีคิดเป็นเงิน 3,387,530 ดอลลาร์สหรัฐฯ หรือความเสียหายเฉลี่ยต่อบุคคลคิดเป็นจำนวนเงิน 427 ดอลลาร์สหรัฐฯ เรื่องที่ได้รับการร้องเรียนมากที่สุด 5 ลำดับแรกคือ การประมูลสินค้าทางอินเทอร์เน็ต (Internet Auctions) (78%), การซื้อสินค้าทั่วไป (10%), การให้บริการอินเทอร์เน็ต (Internet Access Services) (3%), การประกอบธุรกิจที่บ้าน (Work-At-Home) (3%) และการให้สินเชื่อล่วงหน้า (Advance Fee Loans) (2%) ตามลำดับ และจากการสำรวจในปี 2544 ที่ผ่านมามีพบว่าผู้บริโภคได้รับความเสียหายเพิ่มขึ้นเป็นจำนวนเงิน 4,371,724 ดอลลาร์สหรัฐฯ การใช้อินเทอร์เน็ตเป็นเครื่องมือในการหลอกลวงมีหลายวิธีการ ตั้งแต่วิธีการดั้งเดิมที่อาจพบโดยทั่วไปไปจนถึงวิธีการที่สลับซับซ้อน ผู้หลอกลวงใช้ความรู้ทางเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด หรือก่อให้เกิดความเสียหายแก่สาธารณชน แม้ว่าผู้บริโภคจะมีความรู้ทางเทคโนโลยี แต่ก็อาจไม่รู้เท่าทันหรือไม่ทราบถึงวิธีการหลอกลวงดังกล่าว จึงอาจได้รับความเสียหายได้ ดังนั้นการทำความเข้าใจถึงรูปแบบของการหลอกลวงที่ใช้อินเทอร์เน็ตเป็นเครื่องมือและเสนอแนะวิธีป้องกันจะเป็นประโยชน์แก่ผู้บริโภคทำให้สามารถป้องกันปัญหาที่อาจเกิดขึ้น อีกทั้งจะช่วยสร้างความเชื่อมั่นให้กับทั้งผู้บริโภคและผู้ประกอบธุรกิจเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ให้ดียิ่งขึ้นด้วย

**รูปแบบของการหลอกลวงทางอินเทอร์เน็ต มีลักษณะและวิธีการป้องกันโดยสรุป ดังนี้**

**1. การประมูลสินค้าทางอินเทอร์เน็ตโดยหลอกลวง (Internet Auction Fraud)** การโฆษณาขายสินค้าทางอินเทอร์เน็ตด้วยวิธีการประมูลสินค้า ผู้ซื้อที่สนใจจะเข้าร่วมการประมูลมักต้องลงทะเบียนเป็นสมาชิกของเว็บไซต์นั้นๆ ซึ่งโดยทั่วไปจะไม่เสียค่าใช้จ่ายใดๆ หลังจากนั้นจะได้รับหมายเลขสมาชิกและรหัสผ่าน (password) ผู้ซื้อจะต้องเสนอราคาซื้อแข่งขันกับผู้ซื้อรายอื่น เมื่อเสร็จสิ้นการประมูลถือว่ามี การทำสัญญาซื้อขายระหว่างผู้ประมูลและผู้เสนอขาย โดยจะมีการส่งข้อความทางอีเมล (e-mail) แจ้งให้ผู้ซื้อและผู้ขายทราบผลการประมูล และแจ้งรายละเอียดที่จะติดต่อกันได้ เพื่อให้ทั้งฝ่ายผู้ซื้อและผู้ขายติดต่อกันในเรื่องการชำระเงินและการส่งมอบสินค้า

**ลักษณะการหลอกลวง:**

การประมูลสินค้าทางอินเทอร์เน็ต เป็นวิธีการซื้อขายสินค้าที่ได้รับความนิยมและเป็นช่องทางการติดต่อซื้อขายสินค้าที่สะดวกรวดเร็ว ในรายงานสำรวจที่กล่าวมาแล้วของบางประเทศพบว่า เป็นวิธีการหลอกลวงที่พบมากที่สุดเช่นกัน การหลอกลวงมีหลายรูปแบบ เช่น ผู้ขายไม่ส่งมอบสินค้าที่ผู้ซื้อประมูลได้ เพราะไม่มีสินค้าอยู่จริง, การหลอกลวงโดยการปั่นราคาซื้อขาย ผู้ขายหรือบุคคลที่เกี่ยวข้องกับผู้ขายจะเข้าเสนอราคาเพื่อประมูลสินค้าของตน เพื่อให้สินค้ามีราคาสูงขึ้น ทำให้ผู้ซื้อต้องซื้อสินค้าในราคาที่สูงเกินจริง เป็นต้น ความเสียหายที่อาจเกิดขึ้นได้:

ผู้ซื้อได้ชำระค่าสินค้าให้แก่ผู้ขายแล้ว แต่ยังไม่ได้รับสินค้า หรือได้รับสินค้าที่ชำรุดเสียหาย หรือเป็นสินค้าที่มีลักษณะไม่ตรงกับที่มีการเสนอขายแต่แรก ด้านผู้ให้บริการประมูลทางอินเทอร์เน็ตเองก็อาจได้รับความเสียหาย เพราะผู้ใช้บริการ (ผู้ซื้อและผู้ขาย) ไม่ให้ความไว้วางใจและไม่ใช้บริการ

**วิธีการป้องกัน:**

ผู้ซื้อควรตรวจสอบว่าเว็บไซต์ที่ทำหน้าที่เป็นผู้ให้บริการด้านการประมูลทางอินเทอร์เน็ต (คนกลาง) มีวิธีการระบุตัวบุคคลที่เป็นผู้ขาย (หรือผู้ซื้อ) ดีพอหรือไม่ กล่าวคือมีการเก็บประวัติ รายละเอียดของผู้ขาย ที่สามารถติดต่อได้ หรือพิจารณาว่าผู้ให้บริการด้านการประมูลทางอินเทอร์เน็ต (คนกลาง) มีนโยบายการประกันความเสียหายที่อาจเกิดขึ้นหรือไม่ โดยเฉพาะอย่างยิ่งสำหรับสินค้าที่มีมูลค่าค่อนข้างสูง

**2. การให้บริการอินเทอร์เน็ตโดยหลอกลวง (Internet Service Provider Scams)** ผู้หลอกลวงจะส่งเช็คจำนวนหนึ่ง (เช่นราว 3.5 ดอลลาร์สหรัฐฯ) ให้แก่ผู้ใช้บริการ เมื่อมีการเบิกเงินตามเช็คแล้ว ก็ถือว่าผู้บริโภครอดกลางที่จะใช้บริการของผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider - ISP) ที่ได้รับแจ้ง ในการนี้อาจจะไม่มีการแจ้งค่าธรรมเนียมหรือค่าใช้จ่ายใดๆ และมักเป็นการทำสัญญาให้บริการอินเทอร์เน็ตที่มีระยะเวลาสั้น ผู้หลอกลวงจงใจให้ผู้บริโภคหรือผู้ใช้บริการเกิดความสับสนและเข้าใจผิดในสาระสำคัญเกี่ยวกับการบริการนั้น กล่าวคือเมื่อผู้บริโภคเข้าทำสัญญา ดังกล่าวแล้วจะถือว่ายินยอมตามเงื่อนไขทุกประการที่ระบุไว้ การหลอกลวงดังกล่าวนี้มักพบในประเทศที่มีผู้ให้บริการอินเทอร์เน็ตหลายรายและมีบริการที่หลากหลาย

### **ลักษณะการหลอกลวง:**

ผู้บริโภคถูกเรียกเก็บเงินค่าบริการต่างๆ จากผู้ให้บริการอินเทอร์เน็ต นอก  
จากนี้ ยังอาจจะมีคำขู่ที่กล่าวว่าถ้าหากผู้ใช้บริการต้องการเลิกสัญญาก่อน  
ครบกำหนดสัญญา จะถูกปรับเป็นจำนวนเงินที่สูง

**ความเสียหายที่อาจเกิดขึ้นได้:**

ผู้บริโภคถูกเรียกเก็บเงินค่าบริการต่างๆ จากผู้ให้บริการอินเทอร์เน็ต นอก  
จากนี้ ยังอาจจะมีคำขู่ที่กล่าวว่าถ้าหากผู้ใช้บริการต้องการเลิกสัญญาก่อน  
ครบกำหนดสัญญา จะถูกปรับเป็นจำนวนเงินที่สูง

**วิธีการป้องกัน:**

เมื่อผู้บริโภคได้รับเช็คโดยไม่ทราบสาเหตุที่ชัดเจนแล้ว ไม่ควรทำข้อตกลง  
ใดๆ กับบุคคลอื่น แต่ควรศึกษารายละเอียด

ของเอกสารหรือข้อตกลงที่ส่งมาโดยถี่ถ้วน ตรวจสอบค่าใช้จ่ายต่างๆ ที่จะถูก  
เรียกเก็บให้ครบถ้วน และควรติดต่อผู้ให้บริการอินเทอร์เน็ตโดยตรง

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

การชำระค่าสินค้า ค่าบริการทางอินเทอร์เน็ตที่ได้รับความนิยมที่สุดวิธีหนึ่งคือ  
การชำระเงินด้วยบัตรเครดิต เนื่องจากมีความสะดวกแก่ทั้งผู้ซื้อและผู้ขาย ผู้  
ซื้อสามารถชำระเงินโดยการให้ข้อมูลบัตรเครดิตคือ หมายเลขบัตรเครดิต  
ชื่อ-สกุลของ ผู้ถือบัตร และวันหมดอายุแก่ร้านค้า ร้านค้าสามารถตรวจสอบ  
ได้เพียงว่า บัตรดังกล่าวเป็นบัตรที่ออกโดยผู้ออกบัตรจริงแต่ไม่สามารถตรวจ  
สอบตัวบุคคลผู้ใช้บัตรได้ว่าเป็นบุคคลใด

**ลักษณะการหลอกลวง:**

วิธีการหลอกลวงเกี่ยวกับการชำระเงินด้วยบัตรเครดิตทางอินเทอร์เน็ตมีหลาย  
วิธี ตัวอย่างเช่น การให้บริการดูภาพลามก

อนาจารโดยไม่เสียค่าใช้จ่ายใดๆ สำหรับผู้ที่มีอายุตั้งแต่ 18 ปีขึ้นไป (ตาม  
กฎหมายสหรัฐอเมริกา) แต่ผู้บริโภคต้องแจ้งข้อมูลบัตรเครดิตให้ผู้ให้บริการ  
ทราบ เพื่อตรวจสอบความถูกต้องของข้อมูล แล้วผู้หลอกลวงจะใช้ข้อมูลนี้ไป  
กระทำผิดในที่อื่น

**ความเสียหายที่อาจเกิดขึ้นได้:**

ผู้ถือบัตรที่เป็นผู้บริโภครู้ถูกเรียกเก็บเงินค่าสินค้าหรือบริการจากบริษัทหรือ  
ธนาคารผู้ออกบัตร ทั้งที่ผู้ถือบัตรไม่ได้ใช้บัตรเครดิตชำระรายการนั้นๆ เลย  
ซึ่งกฎหมายบางประเทศจะให้ความคุ้มครองผู้ถือบัตรในกรณีนี้ หรือผู้ถือบัตร  
รับผิดชอบไม่เกินจำนวนเงินที่กำหนดไว้ในข้อตกลงระหว่างผู้ออกบัตรและผู้ถือ  
บัตร

**วิธีการป้องกัน:**

ผู้ถือบัตรเครดิตไม่ควรแจ้งข้อมูลบัตรเครดิตให้บุคคลอื่นทราบ แต่หากต้องม  
ีการชำระเงินด้วยบัตรเครดิตทางอินเทอร์เน็ตก็ควรเลือกร้านค้าที่มีความน่า  
เชื่อถือ หรือมีหลักแหล่งที่แน่นอนสามารถติดต่อได้ หรือผู้บริโภครู้ อาจเลือกใช้  
บัตรที่มีวิธีการตรวจสอบตัวบุคคลผู้ใช้บัตรว่าเป็นผู้ถือบัตร เช่น การใช้รหัส  
ประจำตัว (PIN) หรือรหัสใดๆ ที่ไม่ปรากฏอยู่บนบัตร แต่ถือเป็นข้อมูลส่วนตัว  
ของผู้ถือบัตรที่ไม่เปิดเผยให้บุคคลอื่นทราบ นอกจากนี้ ผู้ถือบัตรควรตรวจดู  
ข้อตกลงที่ทำไว้กับผู้ออกบัตรด้วยว่ามีเงื่อนไขความรับผิดชอบอย่างไร

#### **4. การเข้าควบคุมการใช้โมเด็มของบุคคลอื่น (International Modem Dialing/ Modem Hijacking)**

**ลักษณะการหลอกลวง:**

การโฆษณาการให้บริการสื่อลามกอนาจารโดยไม่เสียค่าใช้จ่ายใดๆ ผู้ใช้บริการจะต้องติดตั้งโปรแกรมคอมพิวเตอร์เพื่อดูภาพดังกล่าวหรือเรียกว่า 'viewer' หรือ 'dialer' ของผู้ให้บริการ เมื่อผู้ให้บริการเปิดดูภาพด้วยโปรแกรมข้างต้นแล้ว การทำงานของโปรแกรดังกล่าวจะเริ่มเมื่อมีการใช้เครื่องโมเด็ม (modem) ในขณะเดียวกันโปรแกรมฯ จะควบคุมการทำงานของโมเด็มและสั่งให้หยุดการทำงานโดยที่ผู้ให้บริการไม่รู้ตัว แล้วจะสั่งให้มีการต่อเชื่อมผ่านโมเด็มอีกครั้งหนึ่ง โดยเป็นการใช้โทรศัพท์ทางไกลจากที่ใดที่หนึ่ง แล้วมีการใช้อินเทอร์เน็ตอีกครั้งจากที่นั้น เพื่อให้ผู้ให้บริการสามารถดูเว็บไซต์

**ความเสียหายที่อาจเกิดขึ้นได้:**

ผู้ให้บริการจะถูกเรียกเก็บเงินค่าโทรศัพท์ทางไกลจำนวนมาก ทั้งที่ผู้ให้บริการอาจไม่รู้ ซึ่งเป็นเพราะมีบุคคลอื่นลักลอบใช้โทรศัพท์โดยอาศัยโปรแกรมคอมพิวเตอร์ดังกล่าว

**วิธีการป้องกัน:**

ผู้ให้บริการหรือผู้บริโภคควรหลีกเลี่ยงไม่ติดตั้งโปรแกรมคอมพิวเตอร์ สำหรับการให้บริการใดๆ โดยไม่เสียค่าใช้จ่าย โดยเฉพาะอย่างยิ่งการดูเว็บไซต์ที่มีข้อมูลภาพลามกอนาจาร และควรตรวจสอบเงื่อนไขและค่าใช้จ่ายต่างๆ ถ้าพบสิ่งผิดปกติต้องแจ้งระงับการใช้งานกับผู้ให้บริการทันที นอกจากนี้ ผู้ใช้บริการควรตรวจสอบใบแจ้งหนี้ค่าบริการโทรศัพท์อย่างสม่ำเสมอ

#### **5. การหลอกลวงให้ใช้บริการเกี่ยวกับเว็บไซต์ (Web Cramming)**

**ลักษณะการหลอกลวง:**

การหลอกลวงว่ามีการให้บริการเปิดเว็บเพจ (web page) โดยไม่เสียค่าใช้จ่ายใดๆ เช่นการเปิดเว็บเพจเป็นเวลา 30 วัน และไม่มีข้อผูกพันใดๆ ถ้าไม่ใช้บริการต่อไป

**ความเสียหายที่อาจเกิดขึ้นได้:**

เมื่อมีการตกลงใช้บริการดังกล่าวแล้ว ผู้ใช้บริการจะถูกเรียกเก็บเงินค่าบริการโทรศัพท์ หรือค่าบริการในการมีเว็บเพจ (ค่าธรรมเนียมการใช้พื้นที่) เป็นจำนวนมาก ทั้งๆ ที่ตนไม่เคยใช้บริการหรือไม่ได้สมัครแต่อย่างใด ผู้ใช้บริการยังไม่สามารถแจ้งให้ผู้ให้บริการยกเลิกได้ทันทีอีกด้วย

**วิธีการป้องกัน:**

ผู้บริโภคควรตรวจสอบข้อมูลเกี่ยวกับผู้ให้บริการ และเลือกใช้บริการที่มีความน่าเชื่อถือเท่านั้น (กรณีนี้มักพบในประเทศที่มีผู้ให้บริการโทรศัพท์จำนวนมาก เช่นในประเทศสหรัฐอเมริกา เป็นต้น)

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

**ลักษณะการหลอกลวง:**

การหลอกลวงในลักษณะนี้คล้ายคลึงกับการนำเสนอโฆษณาในการทำตลาดหรือการขายตรง โดยมีชักชวนให้บุคคลทั่วไปเข้าร่วมเป็นสมาชิกในเครือข่ายธุรกิจ โดยการกล่าวอ้างว่าผู้ขายจะได้รับสิทธิในการจำหน่ายสินค้าหลาย

ชนิด และได้รับผลประโยชน์จากการขายสินค้าหรือชักชวนบุคคลอื่นเข้ามาเป็นตัวแทนขายตรง เป็นทอดๆ ทำให้ผู้ที่ได้รับประโยชน์จริงมีจำนวนน้อยราย ความเสียหายที่อาจเกิดขึ้นได้:

ผู้บริโภคที่เข้าร่วมเครือข่ายจะต้องชำระค่าสมาชิกจำนวนหนึ่ง แต่จะไม่มีรายได้ประจำแต่อย่างใด รายได้ของผู้บริโภคจึงไม่แน่นอนและมักจะไม่ได้รับผลประโยชน์ตามที่ผู้หลอกลวงกล่าวอ้าง เพราะไม่สามารถขายสินค้าได้ตามเป้าหมาย

**วิธีการป้องกัน:**

ผู้บริโภคควรระมัดระวังในการสมัครเป็นสมาชิกหรือตัวแทนจำหน่ายสินค้า ที่ต้องหาสมาชิกรายอื่นเพิ่มขึ้นหรือต้องจำหน่ายสินค้าที่มีราคาค่อนข้างสูงให้ได้ตามยอดจำหน่ายที่กำหนด เพราะอาจถูกหลอกลวงได้

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

**ลักษณะการหลอกลวง:**

ผู้ใช้อินเทอร์เน็ตจะได้รับข้อความจากจดหมายหรืออีเมล (e-mail) จากบุคคลที่กล่าวอ้างว่ามีความสำคัญในประเทศไนจีเรียเพื่อขอช่วยเหลือในการโอนเงินจำนวนมากไปยังต่างประเทศ โดยผู้บริโภคจะได้รับเงินส่วนแบ่งจำนวนนับล้านเหรียญดอลลาร์สหรัฐฯ ข้อความในจดหมายหรืออีเมลมีเนื้อหาทำนองว่า ประชาชนในประเทศไนจีเรียไม่สามารถเปิดบัญชีเงินฝากในต่างประเทศหรือโอนเงินออกนอกประเทศที่มีมูลค่าราว 10 ล้านดอลลาร์สหรัฐฯ ได้ หรือรัฐบาลไนจีเรียต้องการทำธุรกิจกับชาวต่างชาติจึงต้องการความช่วยเหลือจากชาวต่างชาติในการเปิดบัญชีเงินฝากประเภทกระแสรายวันที่เบิกด้วยเช็ค ซึ่งท่านจะได้รับคำตอบแทนหรือค่านายหน้า ผู้บริโภคเพียงแต่แจ้งรายละเอียดของบัญชีเงินฝากของตน และกรอกเอกสารพร้อมทั้งลงลายมือชื่อของเจ้าของบัญชีเท่านั้น

ความเสียหายที่อาจเกิดขึ้นได้:

เมื่อมีการแจ้งข้อมูลบัญชีเงินฝากแล้ว ผู้บริโภคจะถูกเรียกเก็บค่าธรรมเนียมหรือค่าใช้จ่ายในการดำเนินการตลอดเวลาโดยให้ผู้บริโภคโอนเงินเข้าบัญชีที่แจ้งไว้ ผู้ที่หลอกลวงจึงสามารถเบิกเงินจากบัญชีดังกล่าวได้โดยอ้างเอกสารมอบอำนาจของเจ้าของบัญชี แต่การโอนเงินลักษณะนี้อาจทำไม่ได้ในประเทศไทย เว้นแต่จะเป็นการโอนเงินระหว่างบัญชีของธนาคารเดียวกันทางอินเทอร์เน็ต

**วิธีการป้องกัน:**

ผู้บริโภคไม่ควรหลงเชื่อบุคคลอื่นที่อ้างตัวและเสนอจะให้ผลประโยชน์จำนวนมหาศาลโดยไม่มีความเสี่ยงเช่นนี้ และไม่ควรเปิดเผยข้อมูลบัญชีธนาคารของตนแก่ผู้อื่นด้วย

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

**ลักษณะการหลอกลวง:**

บริษัทที่หลอกลวงจะเชิญชวนให้ผู้ต้องการประกอบธุรกิจทางอินเทอร์เน็ตหรือธุรกิจด้านพาณิชย์อิเล็กทรอนิกส์ สมัครเป็นสมาชิกเพื่อทำธุรกิจ โดยผู้บริโภคมีเพียงเครื่องคอมพิวเตอร์และสามารถใช้อินเทอร์เน็ตจากที่บ้านได้ และมักอ้างว่าธุรกิจประเภทนี้เป็นธุรกิจที่เติบโตอย่างรวดเร็ว ในขณะที่ผู้บริโภคจะไม่ได้รับคำแนะนำในการทำธุรกิจ ไม่มีข้อมูลธุรกิจ ที่ชัดเจนหรือไม่

ทราบว่าตนอาจไม่ได้รับค่าตอบแทนใดๆ เลย ผู้ถูกหลอกลวงจะถูกเรียกเก็บเงินค่าสมาชิกหรือซื้ออุปกรณ์ที่จำเป็นเพื่อเริ่มทำธุรกิจ

ความเสียหายที่อาจเกิดขึ้นได้:

ผู้ลงทุนจะไม่ได้รับเงินค่าตอบแทนตามที่มีการกล่าวอ้าง และอาจต้องสูญเสียเงินจากการลงทุนอีกด้วย

วิธีการป้องกัน:

ผู้ที่ต้องการลงทุนหรือต้องการเป็นเจ้าของกิจการ ควรศึกษาหรือสอบถามรายละเอียดของประเภทธุรกิจที่จะลงทุนการจ่ายเงินค่าตอบแทนที่ผู้บริโภครจะได้รับ ที่มีกำหนดเวลาที่แน่นอนรวมถึงค่าใช้จ่ายทั้งหมดที่จะต้องจ่ายในการเริ่มต้นทำธุรกิจและผู้บริโภครอระวังไม่หลงเชื่อคำเชิญชวนของผู้ที่อ้างว่าเป็นธุรกิจที่สร้างรายได้จำนวนมากภายในระยะเวลาสั้นๆ

## 9. การหลอกลวงให้จดทะเบียนโดเมนเนม (domain name registration scams)

ลักษณะการหลอกลวง:

ผู้ที่ต้องการทำธุรกิจทางอินเทอร์เน็ตที่ต้องการมีเว็บไซต์และโดเมนเนมของตนเอง จะได้รับการเสนอแนะว่า 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:

ผู้ที่หลงเชื่ออาจได้รับความเสียหายเพราะได้ชำระเงินให้แก่ผู้ที่หลอกลวงโดยไม่ได้รับสิทธิหรือประโยชน์ตามที่กล่าวอ้าง

วิธีการป้องกัน:

1. หลีกเลี่ยงการใช้บริการการขอจดทะเบียนโดเมนเนมล่วงหน้า ที่ให้การรับรองว่าจะได้รับสิทธิ ในการเลือกโดเมนเนมประเภทนี้ (gTLD) ก่อนบุคคลอื่น และไม่ควรถูกหลอกลวงข้อเสนอ
2. ควรติดตามข่าวสารเกี่ยวกับการยื่นขอจดทะเบียนจากผู้รับจดทะเบียนที่ได้รับสิทธิภายใน ประเทศหรือเว็บไซต์ของ ICANN (Internet Corporation for Assigned Names and Numbers) ([www.icann.org](http://www.icann.org))
3. ควรใช้บริการจดทะเบียนโดเมนเนมกับหน่วยงานที่น่าเชื่อถือ เช่น ผู้ให้บริการอินเทอร์เน็ต, บริษัทที่ประกอบธุรกิจเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ หรือใช้บริการของ "ศูนย์สารสนเทศเครือข่ายแห่งประเทศไทย" (Thailand Network Information Center – THNIC) ([www.thnic.net](http://www.thnic.net))

## 10. การหลอกลวงโฆษณาหรือขายยามหัศจรรย์ (miracle products)

ลักษณะการหลอกลวง:

การโฆษณาหรือขายยาทางอินเทอร์เน็ตที่อ้างสรรพคุณว่าสามารถรักษาโรคหรืออาการเจ็บป่วยด้วยโรคร้ายแรง เช่น โรคมะเร็ง, โรคภูมิคุ้มกันบกพร่อง (HIV/AIDS), โรคความดันโลหิตสูง ฯลฯ หรือสามารถบรรเทาความเจ็บป่วย

ได้ภายในระยะเวลาอันสั้น และมักอ้างว่ายานเหล่านี้ได้รับการรับรองหรือการ  
พิสูจน์ทางวิทยาศาสตร์แล้ว

ความเสียหายที่อาจเกิดขึ้นได้:

ผู้ป่วยที่ซื้อยาดังกล่าวโดยเชื่อว่าสามารถรักษาความเจ็บป่วยได้ อาจต้องสูญเสียเงินหรือโอกาสในการได้รับการรักษาอย่างถูกต้อง นอกจากนี้ ยังอาจได้รับอันตรายจากการใช้ยาเหล่านั้นด้วย

วิธีการป้องกัน:

การใช้ยารักษาโรคควรได้รับคำแนะนำจากแพทย์หรือเภสัชกรเท่านั้น

แหล่งข้อมูล <http://www.ecommerce.or.th>

- **National Fraud Information Center, Internet Fraud Statistics (2001-2000),**  
<http://www.fraud.org/internet/2001stats10mnt.htm>
- **National Fraud Information Center, Six-Month Data Trends Report May-November 2000**  
<http://www1.ifccfbi.gov/strategy/6monthreport.pdf>
- **Federal Trade Commission, Operation Top Ten Dot Cons (October 2000),** <http://www.ftc.gov>
- **Ministry of Consumer Affairs, Scam Watch!,**