บทที่ 3

อาชญากรรมทางคอมพิวเตอร์กับการหลอกลวงทางอินเตอร์เน็ต

การประกอบอาชญากรรมทางคอมพิวเตอร์นับว่าเป็นอาชญากรรมที่กำลังทวีความรุนแรงมากขึ้นในสังคมทุกวันนี้ โดยเฉพาะอย่างยิ่งการประกอบอาชญากรรมทางคอมพิวเตอร์โดยอาศัยระบบเครือข่ายอินเตอร์เน็ต ซึ่งอาชญากรได้นำเอาข้อดีของการติดต่อสื่อสารด้วยระบบเครือข่ายอินเตอร์เน็ตคือการเข้าถึงกลุ่มบุคคลได้ทั่วถึง ไม่ว่าบุคคลนั้นจะอยู่ที่ไหนในโลกก็ตาม โดยไม่มีข้อจำกัดทางด้านระยะทาง ง่าย สะดวก ค่าใช้จ่ายน้อย และการกระทำความผิดสามารถเกิดขึ้นได้ตลอด 24 ชั่วโมง โดยใช้ความสามารถของเครื่องคอมพิวเตอร์ ซึ่งในบางครั้งตัวอาชญากรเองก็ไม่จำต้องนั่งอยู่หน้าเครื่องคอมพิวเตอร์ขณะความผิดเกิดขึ้นก็ได้

การประกอบอาชญากรรมโดยผ่านทางระบบเครือข่ายอินเตอร์เน็ตนั้นมีมากมายหลายประเภท เช่น การหมิ่นประมาททางอินเตอร์เน็ต การเผยแพร่ภาพลามกอนาจารทางอินเตอร์เน็ต การพนันทางอินเตอร์เน็ต การเจาะระบบข้อมูลทางอินเตอร์เน็ต เป็นต้น และการกระทำความผิดทางอินเตอร์เน็ตที่กำลังทวีความรุนแรงมากในสังคมโลกปัจจุบันนี้คือ การหลอกลวงทางอินเตอร์เน็ต ซึ่งประเทศที่ได้รับผลกระทบจากการหลอกลวงทางอินเตอร์เน็ตมากที่สุดในขณะนี้คือประเทศสหรัฐอเมริกา เนื่องจากเป็นต้นกำเนิดของเทคโนโลยีระบบเครือข่ายอินเตอร์เน็ตและมีจำนวนผู้ใช้บริการระบบเครือข่ายอินเตอร์เน็ตมากที่สุดในโลกในปัจจุบันนี้ สำหรับประเทศไทยนั้นได้เริ่มรับเอาเทคโนโลยีระบบเครือข่ายอินเตอร์เน็ตมาใช้งานเพียงไม่กี่ปีมานี้ ซึ่งเมื่อพิจารณาจากการเจริญเติบโตของจำนวนผู้ใช้บริการระบบเครือข่ายอินเตอร์เน็ตในอดีตที่มีผู้ใช้บริการเพียงไม่กี่หมื่นคน จนกระทั่งในปัจจุบันนี้มีผู้ใช้บริการมากถึงสามล้านกว่าคนแล้ว ก็คงจะคาดเดาได้ว่าการหลอกลวงทางอินเตอร์เน็ตคงจะเป็นอาชญากรรมที่จะสร้างปัญหาให้กับกระบวนการยุติธรรมของประเทศไทยและจะสร้างความเสียหายให้กับระบบเศรษฐกิจของประเทศอย่างแน่แท้

3.1 ความหมาย ลักษณะ ประเภทของอาชญากรรมทางคอมพิวเตอร์

หลายปีก่อนคำว่าอาชญากรรมทางเศรษฐกิจยังเป็นคำใหม่ของสังคมไทย แต่ทุกวันนี้ดูเหมือนคนไทยจะคุ้นเคยกับคำนี้ดี ไม่เพียงแต่คุ้นเคยเท่านั้น เมื่อเศรษฐกิจของประเทศพังทลายลงทุกคนต่างก็ได้รับผลกระทบอย่างถ้วนหน้า จนทำให้คำว่าอาชญากรรมทางเศรษฐกิจเป็นอาชญากรรมที่คนไทยรู้จักกันเป็นอย่างดี สำหรับในปัจจุบันนี้อาชญากรรมทางเศรษฐกิจรูปแบบใหม่ที่กำลังแพร่หลายในประเทศไทยและกำลังทวีความรุนแรงและสร้างความเสียหายให้กับระบบเศรษฐกิจของประเทศ รวมทั้งกำลังสร้างปัญหาให้กับกระบวนการยุติธรรมของประเทศไทยคือ อาชญากรรมทางคอมพิวเตอร์ (Computer Crime)

วิวัฒนาการทางเทคโนโลยีสารสนเทศในโลกปัจจุบันได้ก้าวไปอย่างไม่หยุดยั้ง อันทำให้สังคมเกิดความเปลี่ยนแปลงไปอย่างมากมาย โดยเฉพาะเครื่องคอมพิวเตอร์ก่อให้เกิดความสะดวกสบายขึ้นในชีวิตประจำวัน ไม่ว่าจะเป็นทางด้านการศึกษา สุขภาพ ความบันเทิง การค้า และการประยุกต์ในเชิงสร้างสรรค์ในรูปแบบต่าง ๆ แต่ในขณะเดียวกันหากนำไปใช้ในทางก่อความเสียหายให้กับบุคคลอื่น โดยเฉพาะอย่างยิ่งในการก่ออาชญากรรมทางคอมพิวเตอร์ซึ่งนับวันจะทวีความรุนแรงและสร้างความเสียหายเป็นอย่างมาก ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์ไม่ได้ส่งผลกระทบต่อความมั่นคงของบุคคลใดบุคคลหนึ่งเท่านั้น แต่ยังส่งผลกระทบไปยังความมั่นคงของประเทศชาติ ทั้งความมั่นคงภายในและความมั่นคงภายนอกประเทศ นอกจากนั้นอาชญากรรมทางคอมพิวเตอร์ยังแตกต่างจากอาชญากรรมรูปแบบเดิม ๆ อย่างสิ้นเชิง ผู้กระทำความผิดเป็นผู้มีความรู้ความสามารถเกี่ยวกับเทคโนโลยีคอมพิวเตอร์ ทำให้การตรวจสอบการกระทำความผิดกระทำได้ลำบาก อีกทั้งไม่ค่อยจะหลงเหลือพยานหลักฐานให้เจ้าหน้าที่ใช้สำหรับการสืบสวน สอบสวน และติดตามจับกุมตัวผู้กระทำความผิดมาลงโทษ

3.1.1 ความหมายของอาชญากรรมทางคอมพิวเตอร์

หากกล่าวถึงอาชญากรรมทางคอมพิวเตอร์จะพบว่าเกิดจากบุคคลหรือคณะบุคคลกระทำความผิดอาญาโดยใช้เครื่องคอมพิวเตอร์เป็นเครื่องมือกระทำความผิด และมีผู้ได้รับความเสียหายหรืออาจได้รับความเสียหายจากการที่มีผู้บุกรุกหรือพยายามที่จะเข้าไปในระบบคอมพิวเตอร์ หรือกล่าวอีกนัยหนึ่งคือการกระทำผิดกฎหมายอาญาใดเกี่ยวกับความรู้ทางเทคโนโลยีสารสนเทศ เพื่อวัตถุประสงค์ลักลอบเข้าไป ลักลอบเข้าถึงข้อมูลคอมพิวเตอร์เพื่อ

ฉกฉวยประโยชน์อันก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล บางครั้งส่งผลกระทบต่อระบบเศรษฐกิจของประเทศหรือระบบเศรษฐกิจของโลก เนื่องจากอาชญากรรมคอมพิวเตอร์เกิดจากอาชญากรที่มีความรู้หรือที่เราเรียกว่า "โจรเสื้อนอก" หรือ "โจรเสื้อขาว" (White Collar Crime) ซึ่งเกิดขึ้นโดยการนำเอาเทคโนโลยีคอมพิวเตอร์หรือเทคโนโลยีสารสนเทศไปใช้ในการทุจริต จึงถือได้ว่าอาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง

อาชญากรรมทางคอมพิวเตอร์เป็นคำที่มีความหมายกว้างมากและมีนักกฎหมายหรือหน่วยงานต่าง ๆ จะให้คำนิยามไว้หลากหลายแตกต่างกัน ดังนี้

ปาร์คเกอร์และซูซาน (Donn B. Parker and Susan H.nycum) ได้ให้คำนิยามไว้ว่า อาชญากรรมคอมพิวเตอร์เป็นการกระทำที่ผิดกฎหมาย โดยใช้เทคนิคหรือความรู้ทางด้านเทคโนโลยี สามารถแบ่งเป็น 4 ประการ

1. ใช้เป็นวัตถุหรือกรรมของการกระทำความผิด (Object)
2. ใช้เป็นสิ่งกระทำความผิด (Subject)
3. ใช้เป็นเครื่องมือในการกระทำความผิด (Tool or Instrument)
4. ใช้เป็นสัญลักษณ์ในการกระทำความผิด (Symbol) [17]

กระทรวงยุติธรรม ประเทศสหรัฐอเมริกา (Department of Justice) ได้ให้คำนิยามคำว่า "อาชญากรรมคอมพิวเตอร์" ไว้ว่าเป็นการกระทำที่ต้องอาศัยประสบการณ์ทางคอมพิวเตอร์โดยทั่วไปอาชญากรรมประเภทนี้จะเกิดขึ้นภายในเครื่องคอมพิวเตอร์ คำว่า "อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์" เป็นคำที่กว้างกว่า หมายความถึงการกระทำความผิดทางอาญาที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศเพื่อกระทำความผิด รวมทั้งการสืบสวนสอบสวนและฟ้องร้อง คำว่า "การใช้คอมพิวเตอร์กระทำความผิด" เป็นการรวมความหมายที่กว้างคือ

---

[17] Parker,D.B. and Nycum,S.H., Computer abuse. (California: Standford Research Institute,1973) อ้างถึงใน เลิศชาย สุธรรมพร, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล,", หน้า 34-35.

การกระทำโดยเจตนาที่เป็นความผิดทางอาญา ซึ่งเป็นการกระทำโดยเจตนาใด ๆ ที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศกระทำความผิดโดยบุคคลหนึ่งหรือมากกว่านั้น เพื่อที่จะให้เหยื่อได้รับความเสียหาย [18]

สำนักงานตำรวจแห่งชาติได้ให้นิยามของคำว่า "อาชญากรรมคอมพิวเตอร์" ไว้ดังนี้ [19]

1. การกระทำใด ๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน

2. การกระทำผิดกฎหมายใด ๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือและในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำตัวผู้กระทำผิดมาดำเนินคดีก็ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์เช่นกัน

อัยการผู้เชี่ยวชาญคดีอาชญากรรมคอมพิวเตอร์ ชื่อเคนเน็ท โรเซ็นบัตต์ (Kenneth S. Rosenblatt) ผู้ซึ่งแต่งหนังสือเรื่อง High Technology Crime อธิบายความหมายของอาชญากรรมคอมพิวเตอร์ไว้ว่า

1. อาชญากรรมที่เกิดขึ้นใหม่อันเป็นผลสืบเนื่องมากจากการใช้คอมพิวเตอร์ในสังคมอย่างแพร่หลาย เช่น การบุกรุกเข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัทธุรกิจที่เชื่อมโยงผ่านเครือข่ายโทรคมนาคม

2. อาชญากรรมแบบดั้งเดิมที่แปรสภาพไป เนื่องมาจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ ซึ่งในการสืบสวนคดีประเภทนี้จำต้องมีความรู้เกี่ยวกับคอมพิวเตอร์และคุ้นเคยกับอุตสาหกรรมเทคโนโลยีขั้นสูง [20]

---

[18] เรื่องเดียวกัน, หน้า 36.

[19] www.ecid.police.go.th

[20] Kenneth Rosen Blatt, High – Technology Crime (California:O'Reiliy & Associates,1995), pp.1-2.

องค์การสหประชาชาติยอมรับว่าไม่สามารถบัญญัตินิยามศัพท์ให้ยอมรับเป็นสากลได้ ซึ่งในทางปฏิบัติจำแนกออกเป็น 2 ส่วน คือ

ส่วนที่ 1 อาชญากรรมดั้งเดิมซึ่งโดยทั่วไปมีกฎหมายระบุฐานความผิดและบทลงโทษไว้อยู่แล้ว เช่น การโจรกรรม การฉ้อโกง การปลอมแปลงและการก่อกวน ซึ่งมีกฎหมายหลักบัญญัติความผิดและบทลงโทษไว้

ส่วนที่ 2 การฝ่าฝืนกฎหรือข้อห้ามและพฤติกรรมเบี่ยงเบนต่าง ๆ ในการใช้คอมพิวเตอร์ ซึ่งยังไม่มีกฎหมายบัญญัติไว้เป็นความผิด [21]

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่านิยามของคำว่าอาชญากรรมทางคอมพิวเตอร์มีผู้ได้ให้คำนิยามไว้มากมายหลากหลาย ผู้วิจัยคงพอจะสรุปนิยามของคำว่า "อาชญากรรมทางคอมพิวเตอร์" ได้ดังนี้

ความหมายอย่างกว้าง หมายถึง การกระทำความผิดที่เกิดขึ้นในเครื่องคอมพิวเตอร์หรือกับเครื่องคอมพิวเตอร์ และความผิดดังกล่าวผู้กระทำความผิดต้องใช้ความรู้ความสามารถทางคอมพิวเตอร์เป็นพิเศษ หรือกล่าวอีกนัยคือครอบคลุมถึงการกระทำความผิดทุกอย่างที่มีเครื่องคอมพิวเตอร์เป็นส่วนประกอบ

ความหมายอย่างแคบ หมายความถึง เฉพาะการกระทำความผิดที่เกิดขึ้นกับข้อมูลภายในเครื่องคอมพิวเตอร์เท่านั้น

3.1.2 ประเภทและลักษณะของอาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ถือเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งที่ก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจ สังคม การเมือง ความมั่นคงของประเทศหรือของโลกเป็นอย่างมาก ซึ่งพอจะสรุปประเภทของการกระทำความผิดได้ดังนี้ [22]

---

[21] สุรพันธ์ มั่นคงดี, "พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์," หน้า 30.

1. การกระทำการต่อระบบคอมพิวเตอร์ซึ่งเป็นเป้าหมายของอาชญากรรมโดยตรง (The computer is the target) เพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์หรือเพื่อทำความเสียหายให้กับเครื่องโปรแกรมหรือแฟ้มคอมพิวเตอร์ต่าง ๆ เช่น การโจรกรรมทรัพย์สินทางปัญญา การโจรกรรมข้อมูลทางการตลาด การข่มขู่ การทำลายทรัพย์สินทางปัญญา การก่อวินาศกรรมต่อโปรแกรมระบบปฏิบัติการหรือแฟ้มข้อมูลคอมพิวเตอร์ การบุกรุกข้อมูลทะเบียนของทางการ การลักลอบเข้าไปในระบบคอมพิวเตอร์เพื่อความท้าทายหรือความอยากรู้อยากเห็นอันเป็นการละเมิดต่อความเป็นส่วนตัว เช่น

ก. Data Diddling คือ การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตก่อนหรือระหว่างที่กำลังบันทึกข้อมูลลงไปในระบบคอมพิวเตอร์ การเปลี่ยนแปลงข้อมูลดังกล่าวนี้สามารถกระทำโดยตัวบุคคลใดก็ได้ที่สามารถเข้าไปถึงตัวข้อมูล เช่น พนักงานเจ้าหน้าที่ที่มีหน้าที่บันทึกเวลาทำงานของพนักงานทั้งหมดทำการแก้ไขตัวเลขอันเป็นชั่วโมงการทำงาน ซึ่งข้อมูลดังกล่าวหากถูกแก้ไขแต่เพียงเล็กน้อยก็แทบจะไม่มีผู้ใดสงสัยหรือรู้ได้เลย

ข. Trojan Horse คือ การเขียนโปรแกรมคอมพิวเตอร์ที่แฝงไว้ในโปรแกรมที่มีประโยชน์ เมื่อถึงเวลาโปรแกรมที่ดีจะปรากฏตัวขึ้นมาเพื่อปฏิบัติการทำลายข้อมูล วิธีนี้มักจะใช้กับการฉ้อโกงทางคอมพิวเตอร์หรือการทำลายข้อมูลหรือระบบคอมพิวเตอร์

ค. Superzapping มาจากคำว่า "superza" เป็นโปรแกรม "Macro Utility" ที่ใช้ในศูนย์คอมพิวเตอร์ของบริษัท IBM เพื่อใช้เป็นเครื่องมือของระบบ (System Tool) ทำให้สามารถเข้าไปในระบบคอมพิวเตอร์ได้ในกรณีฉุกเฉิน เสมือนกุญแจผี (Master Key) ที่จะนำมาใช้เมื่อกุญแจดอกอื่นหาย โปรแกรมอรรถประโยชน์ (Utility Program) เช่น โปรแกรม Superzap จะมีความเสี่ยงมากหากตกในมือของผู้ไม่หวังดี

---

[22] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2) ,พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร : โรงพิมพ์เดือนตุลา จำกัด, 2544), หน้า 52-56.

ง. Logic Bobms เป็นการเขียนโปรแกรมคำสั่งอย่างมีเงื่อนไขไว้ โดยโปรแกรมจะเริ่มทำงานก็ต่อเมื่อโปรแกรมมีสภาวะหรือสภาพการณ์ตามที่ผู้สร้างโปรแกรมกำหนด สามารถใช้ติดตามดูแลความเคลื่อนไหวของระบบบัญชี ระบบเงินเดือนแล้วทำการเปลี่ยนแปลงตัวเลขดังกล่าว

จ. Asynchronous Attack เนื่องจากการทำงานของระบบคอมพิวเตอร์เป็นการทำงานแบบ Asynchronous คือสามารถทำงานหลาย ๆ อย่างพร้อมกัน โดยการประมวลผลข้อมูลเหล่านั้นจะเสร็จไม่พร้อมกัน ด้วยระบบดังกล่าวนี้ก่อให้เกิดจุดอ่อน ผู้กระทำความผิดจะฉวยโอกาสในระหว่างที่เครื่องคอมพิวเตอร์กำลังทำงานเข้าไปแก้ไขเปลี่ยนแปลงหรือกระทำการอื่นใดโดยที่ไม่ทราบว่ามีการกระทำความผิดเกิดขึ้น

2. อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (The computer is an intrumentally of a crime) เช่น การปลอมแปลงบัตรบริการเงินด่วน ATM และเลขบัญชี การลักลอบโอนเงินจากการปัดเศษตัวเลขในการคำนวณดอกเบี้ยในธนาคาร หรือแลกเปลี่ยนสกุลเงิน การปลอมแปลงบัตรเครดิต การฉ้อโกงโดยการใช้การทำรายการบนเครื่องคอมพิวเตอร์ การฉ้อโกงเงินค่าโทรศัพท์ เช่น

ก. Salami Techniques วิธีการปัดเศษจำนวนเงิน เช่น ทศนิยมตัวที่ 3 หรือปัดเศษทิ้งให้เหลือแต่จำนวนเงินที่สามารถจ่ายได้แล้วนำเศษทศนิยมหรือเศษที่ปัดทิ้งมาใส่ในบัญชีของตนเองหรือของผู้อื่น ซึ่งจะทำให้ผลรวมของบัญชียังสมดุลและจะไม่มีปัญหากับระบบควบคุม เนื่องจากไม่มีการนำเงินออกจากระบบบัญชี นอกจากการใช้กับการปัดเศษเงินแล้ววิธีนี้อาจจะใช้กับระบบตรวจนับของในคลังสินค้า

ข. Trap Doors เป็นการเขียนโปรแกรมที่เลียนแบบคล้ายหน้าจอปกติของเครื่องคอมพิวเตอร์ เพื่อลวงผู้ที่มาใช้คอมพิวเตอร์ ทำให้ทราบถึงรหัสประจำตัว (ID Number) หรือรหัสผ่าน (Password) โดยใช้โปรแกรมนี้เก็บข้อมูลที่ต้องการนี้ไว้ในแฟ้มลับ

ค. Simulation and Modeling ในปัจจุบันเครื่องคอมพิวเตอร์ถูกใช้เป็นเครื่องมือในการวางแผนการควบคุมและติดตามความเคลื่อนไหวในการประกอบอาชญากรรม และกระบวนการดังกล่าวก็สามารถใช้โดยอาชญากรในการสร้างแบบจำลองในการวางแผนเพื่อประกอบอาชญากรรมได้เช่นกัน

3. **อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์** (Computer Related offences) เช่น การฟอกเงิน การลักลอบโอนเงิน การเผยแพร่ภาพลามกอนาจาร การลอกเลียนหรือการปลอมแปลงโปรแกรมคอมพิวเตอร์ การละเมิดลิขสิทธิ์ของโปรแกรมคอมพิวเตอร์ การปลอมแปลงอุปกรณ์ การค้าอุปกรณ์ และโปรแกรมคอมพิวเตอร์ในตลาดมืด

4. **การข่มขู่ผ่านทางคอมพิวเตอร์** (Technological coercion via computer) เช่น การข่มขู่ด้วยการล่วงล้ำหรือบุกรุกเข้าไปในระบบคอมพิวเตอร์ของเหยื่อ

5. **การก่ออาชญากรรมหรือรบกวนบนเครือข่ายคอมพิวเตอร์** (Networking malfeasance) เช่น การก่อกวนทางเพศ การหมิ่นประมาทบุคคลหรือองค์การผ่านเครือข่ายคอมพิวเตอร์ การล่อลวงเยาวชนไปเพื่อทำอนาจาร ตัวอย่างเช่น

ก. Data Leakage หมายถึง การทำให้ข้อมูลรั่วไหลออกไป อาจโดยตั้งใจหรือไม่ก็ตาม เช่น การแผ่รังสีของคลื่นแม่เหล็กไฟฟ้าในขณะที่กำลังทำงาน คนร้ายอาจตั้งเครื่องดักสัญญาณไว้ใกล้กับเครื่องคอมพิวเตอร์เพื่อรับข้อมูลตามที่ตนต้องการ

ข. Wiretapping เป็นการลักลอบดักฟังสัญญาณการสื่อสาร โดยเจตนาที่จะได้รับผลประโยชน์จากการเข้าถึงข้อมูลผ่านเครือข่ายการสื่อสารหรือที่เรียกว่าโครงการพื้นฐานสารสนเทศ

ค. Scavenging คือ วิธีการที่จะได้ข้อมูลที่ทิ้งไว้ในระบบคอมพิวเตอร์หรือบริเวณใกล้เคียง หลังจากเสร็จการใช้งานแล้ว วิธีที่ง่ายที่สุด คือ ค้นหาตามถังขยะที่อาจมีข้อมูลเกี่ยวกับเบอร์โทรศัพท์ หรือรหัสผ่านหลงเหลืออยู่ หรืออาจใช้เทคโนโลยีที่ซับซ้อนทำการหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์เมื่อผู้ใช้งานเลิกใช้แล้ว

ง. Piggybacking วิธีการดังกล่าวสามารถทำได้ทั้งทางกายภาพ การที่คนร้ายจะลักลอบเข้าไปในประตูที่มีระบบรักษาความปลอดภัย คนร้ายจะรอให้บุคคลที่ได้รับอนุญาตมาใช้ประตูดังกล่าว เมื่อประตูเปิดและบุคคลนั้นได้เข้าไปแล้ว คนร้ายก็ฉวยโอกาสตอนที่ประตูยังไม่ปิดสนิทแอบเข้าไปได้ ในทางอิเล็กทรอนิกส์อาจเกิดขึ้นในกรณีที่ใช้สายสื่อสารเดียวกันกับผู้ที่มีอำนาจใช้หรือได้รับอนุญาต เช่น ใช้สายเคเบิลหรือโมเด็มเดียวกัน

จ. Impersonation คือ การที่คนร้ายแกล้งปลอมเป็นบุคคลอื่นที่มีอำนาจหรือได้รับอนุญาต เช่น เมื่อคนร้ายขโมยบัตรเอทีเอ็มของเหยื่อได้ก็จะโทรศัพท์และแกล้งว่าเป็นพนักงานของธนาคาร และแจ้งให้เหยื่อทราบว่ากำลังหาวิธีป้องกันมิให้เงินในบัญชีของเหยื่อหายไป จึงบอกให้เหยื่อเปลี่ยนรหัสประจำตัว (Personal Identification Number : PIN) โดยให้เหยื่อบอกรหัสเดิมก่อน คนร้ายจึงทราบหมายเลขรหัสและได้เงินของเหยื่อไป

ฉ. การเจาะระบบ (Hacking) หมายถึงการเข้าไปในเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) และเมื่อเข้าไปแล้วก็ทำการสำรวจทิ้งข้อความโปรแกรมลบแก้ไขเปลี่ยนแปลงหรือขโมยข้อมูล อาจส่งผลให้ความลับทางการค้า ข้อมูลที่สำคัญหรือแม้แต่เงินของหน่วยงานต้องถูกขโมยไป การกระทำดังกล่าวอาจทำจากคู่แข่งทางการค้าหรือผู้ที่ไม่หวังดีและอาจจะทำจากในหน่วยงานนั้นเองหรือจากที่อื่น ๆ ที่อยู่ห่างไกลออกไปหรือจากนอกประเทศโดยใช้เครือข่ายการสื่อสารสาธารณะหรือโทรศัพท์ นักเจาะระบบอาจได้รหัสการเข้าสู่เครือข่ายโดยการดักฟังข้อมูลทางโทรศัพท์หรือใช้เครื่องมือสื่อสารนำไปติดกับเครื่องคอมพิวเตอร์ หรือใช้เครื่องจักรแผ่รังสีจากการส่งผ่านข้อมูลที่ไม่มีการป้องกันการแผ่รังสี (Unshielded Data Transmission) เพื่อจะได้มาซึ่งรหัสผ่าน (Password)

ง. ไวรัสคอมพิวเตอร์ คือ โปรแกรมที่มีความสามารถในการแก้ไข ดัดแปลงโปรแกรมอื่น เพื่อที่จะทำให้โปรแกรมนั้น ๆ สามารถเป็นที่อยู่ของมันได้ และสามารถทำงานได้ต่อไปเรื่อย ๆ เมื่อมีการเรียกใช้โปรแกรมที่ติดเชื้อไวรัสนั้น สำหรับประวัติไวรัสคอมพิวเตอร์นั้นเดิมความคิดในเรื่องไวรัสคอมพิวเตอร์เป็นเพียงในนวนิยาย จนในปี ค.ศ.1983 นาย Fred Cohen นักศึกษาปริญญาเอก คณะวิศวกรรมไฟฟ้าที่มหาวิทยาลัยเซาท์เทอร์นแคลิฟอร์เนีย ได้คิดค้นโปรแกรมคอมพิวเตอร์ซึ่งสามารถทำลายล้างโปรแกรมคอมพิวเตอร์ด้วยกัน เปรียบเสมือนเชื้อไวรัสกระจายเข้าสู่ตัวคน และเรียกโปรแกรมดังกล่าวว่า Computer Virus และชื่อนี้ก็ได้ใช้เรียกโปรแกรมชนิดนี้นับตั้งแต่นั้นมา ตัวอย่างไวรัสคอมพิวเตอร์ที่มนุษย์สามารถคิดค้นได้ เช่น Worm, Pakistani, Michelangelo, Dark Avenger หรือแม้แต่ไวรัสที่ใช้ชื่อภาษาไทย เช่น ลาวดวงเดือน เป็นต้น [23]

---

[23] ดร.ทวีศักดิ์ กออนันตกูล, "อาชญากรรมในยุคโลกาภิวัฒน์," บทบัณฑิตย์ 55 (มีนาคม 2542) : หน้า 30-31.

3.1.3 **ลักษณะของอาชญากรคอมพิวเตอร์** (Categories of Computer Criminals) [24]

1. **พวกหัดใหม่** (Novice) บุคคลประเภทนี้มิได้เป็นอาชญากรโดยแท้จริง เพียงแค่ใช้โอกาสในตำแหน่งหน้าที่ที่มีอยู่เข้าไปดำเนินการกับข้อมูลคอมพิวเตอร์เพื่อเข้าไปยังฐานข้อมูลนั้น ๆ และมีเป็นจำนวนมากที่เป็นลูกจ้างหรือพนักงานของหน่วยงานนั้น ๆ เองหรือผู้ที่เริ่มทำการศึกษาหาความรู้ในด้านเทคโนโลยีสารสนเทศ เข้าใจและเข้าถึงวิธีการใช้และสมรรถนะของเครื่องคอมพิวเตอร์และฝึกฝนจนเกิดความชำนาญ พวกนี้ยากต่อการจับกุม เพราะจะไม่ใช่อาชญากรโดยนิสัย มิได้ดำรงชีพด้วยการกระทำความผิด เมื่อทำผิดครั้งเดียวแล้วก็จะหลบหน้าหายไปไม่สร้างความเสียหายแก่เจ้าของอีก

2. **พวกวิกลจริต** (Deranged persons) ลักษณะของบุคคลประเภทนี้มักจะทำอะไรโดยปราศจากเหตุผล ชอบทำลาย เป็นผู้ป่วยทางจิตและมีอันตรายโดยทั่วไป ไม่สามารถควบคุมตนเองได้และจะทำลายระบบซอฟท์แวร์หรือแฟ้มข้อมูลต่าง ๆ

3. **เป็นกลุ่มที่ประกอบอาชญากรรมในลักษณะองค์กร** (Organized crime) เป็นพวกที่ประกอบอาชญากรรมโดยแสวงหาผลประโยชน์จากเครื่องคอมพิวเตอร์ มีการกระทำร่วมกันเป็นกลุ่ม มีความรู้เกี่ยวกับเครื่องคอมพิวเตอร์เป็นอย่างดี สามารถใช้ในการหลบหลีกหรือยับยั้งการสืบสวนติดตามจับกุมของเจ้าหน้าที่ได้

4. **พวกมืออาชีพ** (Career) เป็นการรวมกลุ่มของผู้ที่เคยถูกดำเนินคดีในความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มาก่อน ถึงแม้ว่าจะถูกจับกุมแล้วเมื่อพ้นโทษออกมาก็จะกระทำความผิดซ้ำอีก

5. **พวกหัวพัฒนา** (Con artists) เป็นพวกที่ชอบใช้ความเจริญก้าวหน้าของเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงิน

6. **พวกช่างคิดช่างฝัน** (Ideologues) เป็นพวกที่กระทำผิดเนื่องจากมีความเชื่อถือในสิ่งหนึ่งสิ่งใดอย่างรุนแรง เป็นพวกก้าวร้าวชอบแสดงตัวเองว่ามีจุดเด่นหรือมีอำนาจเหนือบุคคลอื่น

---

[24] www.ecid.police.go.th

7. **พวก** Hacker/Cracker เป็นพวกที่จงใจและเจตนาเข้าถึงระบบของเครื่องคอมพิวเตอร์และแฟ้มข้อมูล โดยแยกความหมายของ Hacker/Cracker ได้ดังนี้

7.1 Hacker หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในเครื่องคอมพิวเตอร์โดยเจาะผ่านระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ได้ แต่ไม่แสวงหาประโยชน์

7.2 Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางเครื่องคอมพิวเตอร์เป็นอย่างดีจนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูลหรือทำให้เครื่องคอมพิวเตอร์เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

3.1.4 ความเสียหายและผลกระทบจากอาชญากรรมทางคอมพิวเตอร์

ในปัจจุบันนี้เป็นยุคของการติดต่อสื่อสารด้วยระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายอินเตอร์เน็ตหรือที่เรียกว่าสังคมยุคไอที ทำให้ทุกองค์กรไม่ว่าจะเป็นภาครัฐหรือเอกชนอาจตกเป็นเหยื่อของอาชญากรรมทางคอมพิวเตอร์ได้ เช่น ถูกบุกรุกระบบข้อมูลทางด้านความมั่นคงของประเทศ สถาบันการเงิน และธนาคาร ระบบสาธารณูปโภคของรัฐ เช่น ไฟฟ้า ประปา และการสื่อสารคมนาคม ระบบข้อมูลธุรกิจของบริษัทเอกชนอาจถูกคู่แข่งทางธุรกิจหรืออาชญากรที่มีความชำนาญล้วงความลับหรือทำลายข้อมูลได้ ตลอดถึงประชาชนผู้ใช้เครื่องคอมพิวเตอร์ทั่วไปก็ตกเป็นเหยื่อของคดีประเภทนี้ได้

เป็นที่แน่นอนว่าเมื่อมีอาชญากรรมเกิดขึ้น ความสูญเสียเป็นสิ่งที่ต้องเกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ อาชญากรรมทางคอมพิวเตอร์นั้นถ้าดูกันอย่างผิวเผินจะไม่มีความรุนแรงที่เกิดขึ้นกับเหยื่อมากนัก เพราะโดยมากมักจะไม่ทำให้เหยื่อได้รับอันตรายต่อชีวิตและร่างกาย แต่ถ้าจะพิจารณากันอย่างละเอียดรอบคอบโดยเฉพาะความเสียหายกับทรัพย์สินแล้ว จะเห็นได้ว่ามีความเสียหายเกิดขึ้นอย่างมหาศาล ความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้นไม่ได้มีผลกระทบเพียงแต่ความมั่นคงของบุคคลใดบุคคลหนึ่งเท่านั้น แต่ยังมีผลกระทบไปถึงความมั่นคงของประเทศชาติเป็นการส่วนรวม ทั้งความมั่นคงภายในและภายนอกประเทศ รวมทั้งความเสียหายทางด้านเศรษฐกิจและสังคม

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่กำลังเกิดขึ้นอยู่แล้วทุกวินาทีในปัจจุบัน และมีแนวโน้มว่าอาชญากรรมทางคอมพิวเตอร์จะเพิ่มมากขึ้น เนื่องจากบุคคลทั่วไปสามารถเข้าถึงเทคโนโลยีทางคอมพิวเตอร์ได้ง่ายขึ้น และมีราคาต่ำลง ง่ายต่อการกระทำความผิด ตรวจสอบ จับกุมยากกว่าการประกอบอาชญากรรมรูปแบบเดิมประกอบกับมีช่องโหว่ในประเด็นปัญหาข้อกฎหมายและแนวทางการปฏิบัติอีกด้วย

3.1.5 เปรียบเทียบความแตกต่างระหว่างอาชญากรรมรูปแบบเดิมกับอาชญากรรมทางคอมพิวเตอร์

รูปแบบของอาชญากรรมทางคอมพิวเตอร์จะแตกต่างจากอาชญากรรมในรูปแบบเดิม เนื่องจากวัตถุที่อาชญากรรมทางคอมพิวเตอร์มุ่งหมายกระทำต่อได้เปลี่ยนไปจากเดิมที่อาชญากรรมมุ่งกระทำต่อทรัพย์ที่มีรูปร่าง เปลี่ยนเป็นวัตถุที่ไม่มีรูปร่างคือข้อมูล เรื่องเวลาในการก่ออาชญากรรมในรูปแบบเดิมจะเป็นนาที ชั่วโมง วัน สัปดาห์ เดือน หรือปี แต่ในเรื่องอาชญากรรมคอมพิวเตอร์จะเกิดแค่เสี้ยววินาที แต่ก่อให้เกิดความเสียหาย เกิดการล้มละลายของหลาย ๆ บริษัทได้ ในแง่ของภูมิศาสตร์ อาชญากรรมแบบเดิมอาจจะเกิดขึ้นในชุมชนท้องถิ่นหรือในประเทศใดประเทศหนึ่ง แต่อาชญากรรมในรูปแบบใหม่เป็นอาชญากรรมที่เกิดบนโลกที่ไร้พรมแดน ผู้กระทำความผิดกับผู้เสียหายไม่จำเป็นต้องอยู่ประเทศเดียวกันหรือเรียกว่าเป็นอาชญากรรมข้ามชาติ และการพิสูจน์ตัวผู้กระทำความผิดก็กระทำได้ยากเพราะอาชญากรเป็นผู้มีความรู้ ความสามารถทางเทคโนโลยีคอมพิวเตอร์ ในแง่ของความเสียหายอาชญากรรมแบบเดิมจะเกิดความเสียหายไม่มากนัก เช่น การฉ้อโกงธนาคาร การฉ้อโกงทางการเงิน มีความเสียหาย 193,000 ดอลลาร์สหรัฐ ในปี คศ. 1980 การปล้นธนาคารความเสียหายประมาณ 10,000 ดอลลาร์สหรัฐ แต่สำหรับอาชญากรรมคอมพิวเตอร์ในปี คศ. 1980 ความเสียหายคือ 450,000 ดอลลาร์สหรัฐ ซึ่งในแง่ความเสียหายค่อนข้างจะสูงกว่าอาชญากรรมรูปแบบเดิม จากความแตกต่างดังกล่าวข้างต้น พอจะสรุปความแตกต่างระหว่างอาชญากรรมรูปแบบเดิมกับอาชญากรรมคอมพิวเตอร์ ได้ดังนี้ [25]

---

[25] โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. ประเทศไทยกับการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (กรุงเทพมหานคร:โรงพิมพ์เดือนตุลา, 2544), หน้า 16.

1. **วัตถุแห่งการกระทำความผิด**

อาชญากรรมรูปแบบเดิม วัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นทรัพย์ที่จับต้องได้ (Tangible Object) ตัวอย่างเช่น รถยนต์ ของมีค่า เงิน ทอง เป็นต้น

อาชญากรรมทางคอมพิวเตอร์ วัตถุแห่งการกระทำความผิดส่วนใหญ่เป็นข้อมูลข่าวสารในรูปของคลื่นแม่เหล็กไฟฟ้า (Electronic Impulse) ซึ่งเป็นสิ่งที่ไม่สามารถจับต้องได้ (Intangible Object) ข้อมูลทางการค้าของบริษัท ฐานข้อมูลบัญชีลูกค้าของบริษัท หรือค่าเงินในบัญชีของธนาคาร

2. **วิธีการกระทำความผิด**

อาชญากรรมรูปแบบเดิม เป็นการกระทำความผิดทางกายภาพ เช่น การทำลายทรัพย์ของผู้อื่น (ความผิดฐานทำให้เสียทรัพย์) หรือการเข้าไปในแดนกรรมสิทธิ์ของบุคคลอื่น (ความผิดฐานบุกรุก) เป็นต้น

อาชญากรรมทางคอมพิวเตอร์ เป็นการกระทำความผิดรูปแบบใหม่ที่อาจไม่ต้องมีการกระทำทางกายภาพ ตัวอย่างเช่น การเข้าไปในระบบคอมพิวเตอร์ที่อยู่ในบ้านเรือนของผู้อื่น โดยไม่ได้รับอนุญาต (Unauthorized Access) ซึ่งผู้กระทำความผิดไม่จำเป็นที่จะต้องเข้าไปทางกายภาพแต่ประการใด เพียงแต่นั่งอยู่ที่บ้านของผู้กระทำความผิดก็สามารถกระทำความผิดได้และนอกจากไม่ต้องอาศัยการกระทำทางกายภาพแล้ว หรือความผิดฐานลักทรัพย์ที่กฎหมายกำหนดให้ต้องมีการเอาไป แต่อาชญากรรมคอมพิวเตอร์เพียงแต่เป็นการเข้าถึงและคัดลอกข้อมูลไป ซึ่งข้อมูลดังกล่าวก็ยังคงอยู่ จะเห็นได้ว่าไม่ได้มีการ "เอาไป" แต่อย่างใด นอกจากนั้นการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ยังมีวิธีการกระทำความผิดที่แปลกใหม่และซับซ้อน ดังจะเห็นได้จากประเภทของอาชญากรรมในรูปแบบต่าง ๆ เช่น การเจาะระบบ (Hacking) ไวรัสคอมพิวเตอร์ (Virus Computer) ม้าไม้โทรจัน (Trojan Horse) เป็นต้น

3. **ระยะเวลาในการกระทำความผิด**

อาชญากรรมรูปแบบเดิม เนื่องจากการกระทำความผิดรูปแบบเดิมเป็นการกระทำทางกายภาพ ดังนั้น จึงต้องใช้ระยะเวลาในการกระทำความผิด ซึ่งอาจเป็นนาที ชั่วโมง วัน สัปดาห์ หรืออาจเป็นปี

อาชญากรรมทางคอมพิวเตอร์ เป็นการใช้เทคโนโลยีขั้นสูงของเครื่องคอมพิวเตอร์ ซึ่งมีความรวดเร็วมาก ดังนั้นระยะเวลาที่ใช้ในการกระทำความผิดจึงต้องคำนวณกันเป็นวินาที หรืออาจเป็นเสี้ยววินาที

4. **ขอบเขตในการกระทำความผิด**

อาชญากรรมรูปแบบเดิม โดยส่วนใหญ่เป็นการกระทำความผิดภายในอาณาเขตและดินแดน เพราะข้อจำกัดทางภายภาพ

อาชญากรรมทางคอมพิวเตอร์ เป็นการกระทำความผิดที่ใช้การผสมผสานระหว่างเทคโนโลยีคอมพิวเตอร์กับเทคโนโลยีโทรคมนาคมที่มีเครือข่ายเชื่อมโยงทั่วโลก ดังนั้น อาชญากรรมทางคอมพิวเตอร์จึงสามารถกระทำความผิดระหว่างประเทศได้อย่างรวดเร็วและไม่มีขอบเขต สามารถกระทำต่อบุคคลได้ทั่วโลก โดยผู้กระทำความผิดไม่จำเป็นต้องเดินทางไปยังดินแดนที่ผู้เสียหายอยู่เลย

3.1.6 ตัวอย่างอาชญากรรมทางคอมพิวเตอร์

ผู้วิจัยจะขอยกตัวอย่างการก่ออาชญากรรมทางคอมพิวเตอร์เพื่อให้ผู้มีหน้าที่เกี่ยวข้องหรือประชาชนทั่วไปเล็งเห็นถึงความเปลี่ยนแปลงของรูปแบบของอาชญากรรมและความเสียหายที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ ซึ่งการประกอบอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันมีมากมายหลายรูปแบบ แต่ผู้วิจัยจะขอยกตัวอย่างบางกรณีเท่านั้น

ก.ในต่างประเทศ

การฉ้อโกงและฆาตกรรม ปัจจุบันค่อนข้างง่ายที่จะทำอาชญากรรมเกี่ยวกับการฉ้อโกงทางเครื่องคอมพิวเตอร์โดยผ่านข้อมูลในเครื่องคอมพิวเตอร์ จะเห็นได้จากคดีฆาตกรรมหนึ่งในรัฐเท็กซัส ซึ่งมีผู้แก้ไขข้อมูลเกี่ยวกับการรักษาคนป่วยทำให้คนป่วยตายโดยผู้กระทำหวังเงินประกันชีวิต และมีคดีฆาตกรรมอีกคดีหนึ่งมีหญิงจากรัฐมารีแลนด์พบถูกฆ่าตายอยู่หลังบ้านของชายคนหนึ่งใน North Carolina อันสืบเนื่องมากจากการติดต่อแบบชู้สาวทางอีเมล์ โดยฝ่ายชายบรรยายถึงวิธีการที่จะทรมานเธอและฆ่าเธอหลังจากมีเพศสัมพันธ์กัน ซึ่งการค้นพบศพหญิงคนนั้นเนื่องจากข้อความที่หญิงแจ้งแก่สามีเธอ และเนื้อหาในอีเมล์ที่ยึดได้จากเครื่องคอมพิวเตอร์ของผู้กระทำความผิด

อาชญากรรมทางเพศ ไม่ว่าจะเป็นการเผยแพร่ภาพสื่อลามกเด็กหรือสื่อลามกอนาจารผ่านทางระบบเครือข่ายอินเตอร์เน็ต สามารถเป็นสื่อในการกระจายรูปภาพดังกล่าวได้อย่างสบาย ไม่มีการเสื่อมไปของคุณภาพในการทำสำเนาเช่นกรณีการเผยแพร่ในรูปแบบเดิมหรือจะเป็นการซื้อขายบริการทางเพศ ซึ่งสามารถเข้าถึงกลุ่มบุคคลได้มากมายการที่สามารถติดต่อสื่อสารได้อย่างกว้างขวางทำให้เป็นการง่ายในการก่ออาชญากรรม เพราะเจอเหยื่อได้ง่าย เช่น คดีในประเทศสหรัฐอเมริกา รัฐโอริกอน มีชายอายุ 19 ปี ถูกตัดสินจำคุก 30 วัน และถูกทำทัณฑ์บนไว้ 5 ปี สำหรับการกระทำความผิดทางเพศกับเด็กหญิง อายุ 14 ปี ที่รู้จักกันบนอินเตอร์เน็ต

การก่อกวนหรือรังควาญ การที่อีเมล์สามารถส่งถึงกันได้อย่างรวดเร็ว แม้จะมีบุคคลที่ต้องการส่งอีเมล์ถึงจำนวนมากก็สามารถส่งไปยังเป้าหมายได้อย่างรวดเร็ว บางกรณีที่ผู้ที่ตกเป็นผู้เสียหายในเรื่องนี้เกิดจากการเป็นสมาชิกใช้บริการอินเตอร์เน็ต เช่น พวก Hacker ได้เจาะเข้าไปในองค์การโทรศัพท์ และแก้ข้อมูลของโทรศัพท์ประจำบ้านให้กลายเป็นโทรศัพท์สาธารณะ ซึ่งทุกครั้งที่เจ้าของบ้านจะใช้โทรศัพท์จะมีเสียงบอกให้หยอดเหรียญก่อนทุกครั้ง

การเจาะระบบ (Hacking) เป็นการเข้าไปเอาข้อมูลจากเครื่องคอมพิวเตอร์ของผู้อื่นโดยที่ตนไม่มีอำนาจ ซึ่งจะเป็นกระทำโดยมุ่งหมายต่อข้อมูลของผู้อื่น เช่น ข้อมูลจากเว็บไซต์ข่าวซีเอ็นเอ็นออนไลน์ วันที่ 20 กรกฎาคม 2545 ระบุว่านางสาวดาริเอล อินสเลอร์ นักศึกษาสาววัย 22 ปี ชั้นปีที่ 3 ของมหาวิทยาลัยลีโอเนีย ในรัฐนิวเจอร์ซี ประเทศสหรัฐอเมริกา ได้บุกรุก

เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย เพื่อแก้ไขเกรดวิชาคณิตศาสตร์และวิทยาศาสตร์จาก F เป็น A รวมทั้งยังถูกกล่าวหาว่าเปลี่ยนแปลงแก้เกรดที่ยังไม่สมบูรณ์เพื่อให้เธอสามารถผ่านชั้นเรียนขึ้นสู่ปีที่สี่ของการศึกษาได้ จากคำให้การที่ได้รับการบันทึกเป็นลายลักษณ์อักษรเจ้าหน้าที่รัฐเดลาแวร์ระบุว่านางสาวอินสเลอร์ได้โทรศัพท์ไปสอบถามเจ้าหน้าที่ด้านทรัพยากรบุคคลของมหาวิยาลัยเพื่อขอรหัสผ่านของอาจารย์ผู้สอนแต่ละคนก่อนที่จะทำการเข้าสู่ระบบ ซึ่งนางสาวอินสเลอร์ยังสามารถแกะรหัสผ่านของอาจารย์ผู้สอนคนอื่น ๆ ได้เพื่อเข้าไปตรวจสอบผลการเรียนการสอนในวิชาอื่น ๆ ได้สำเร็จ และจากการกระทำของนักศึกษาผู้นี้ได้ถูกทางการตั้งข้อหาว่าโจรกรรมรหัสและลักลอบเข้าสู่ระบบคอมพิวเตอร์อย่างผิดกฎหมาย รวมทั้งใช้ข้อมูลในเครือข่ายคอมพิวเตอร์ในทางที่มิชอบ อย่างไรก็ตามนางสาวอินสเลอร์สามารถประกันตัวด้วยการวางเงินมัดจำเป็นมูลค่า 5,500 ดอลลาร์สหรัฐและรอการไต่สวนจากศาลของรัฐเดลาแวร์

ไวรัสคอมพิวเตอร์ Morris Case ในปี คศ.1988 นายโรเบิร์ต ที มอริส นักศึกษาสาขาวิชาคอมพิวเตอร์ มหาวิทยาลัยคอร์แนล ได้ทำการเพาะไวรัสคอมพิวเตอร์ซึ่งเป็นที่รู้จักกันดีในนาม “หนอนคอมพิวเตอร์” (Worm) มอริสต้องการให้เกิดความมั่นใจว่า Worm จะไม่ทำซ้ำตัวของมันเองบนเครื่องคอมพิวเตอร์ที่มันเข้าไป เพราะการทำซ้ำมาก ๆ จะทำให้ง่ายต่อการตรวจจับและจะส่งผลให้เครื่องติดขัดหรืออาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถทำงานได้เลย ดังนั้น มอริสจึงได้ออกแบบให้ Worm สามารถถามเครื่องว่ามีสำเนาของ Worm หรือไม่ ถ้าตอบว่าไม่ Worm ก็จะทำสำเนาบนเครื่องคอมพิวเตอร์ หากตอบว่ามี Worm ก็จะไม่ทำสำเนา อย่างไรก็ดีมอริสกลัวว่า Worm จะถูกฆ่าโดยโปรแกรมเมอร์อื่น ๆ ได้ หากแกล้งให้เครื่องสั่งว่ามี มอริสจึงได้เขียนโปรแกรมให้ Worm ทำซ้ำได้เพียง 7 ครั้ง หากได้รับคำตอบว่ามี โดยมอริสคิดว่า Worm จะถูกทำลายเมื่อปิดเครื่องคอมพิวเตอร์ ดังนั้นจึงไม่ส่งผลเสียมากนัก

มอริสได้ใส่โปรแกรมไวรัสนี้เข้าไปในระบบปฏิบัติการ Unix เมื่อวันที่ 2 พฤศจิกายน 1988 ที่ Massachusetts Institute of Technology เนื่องจากต้องการอำพรางเพราะมอริสเรียนอยู่ที่มหาวิทยาลัยคอแนล แต่เรื่องที่มอริสไม่คาดฝันก็เกิดขึ้น Worm แพร่ระบาดและทำซ้ำอย่างรวดเร็วเกินคาดคิด และเมื่อมอริสพยายามจะร่วมมือกับเพื่อนของเขาที่มหาวิทยาลัยฮาร์วาร์ด โดยส่งจดหมายไปบนเครือข่ายถึงวิธีการกำจัดเจ้าวายร้าย Worm แต่เนื่องจากเครือข่ายล่มลงเพราะพิษของ Worm จดหมายดังกล่าวจึงไม่สามารถส่งไปได้ เครือข่ายที่

เชื่อมโยงสถาบันการศึกษาหน่วยทหาร หรือศูนย์วิจัยในสหรัฐล้วนแต่ได้รับผลร้ายจากการระบาดของ Worm ทั้งสิ้น ในที่สุดมอริสถูกตัดสินจำคุก 3 ปี แต่ให้รอลงอาญา โดยให้ไปบริการสังคมเป็น เวลา 400 ชั่วโมง และปรับเป็นเงิน 10,050 ดอลลาร์สหรัฐ [26]

ข.ในประเทศไทย

อาชญากรรมทางคอมพิวเตอร์ในประเทศไทยมีอยู่จริง มูลค่าความเสียหายมีมากน้อยเพียงใดไม่อาจประเมินได้ เนื่องจากตำรวจและหน่วยงานที่เกี่ยวข้องอื่น ๆ มองข้ามความสำคัญของอาชญากรรมประเภทนี้ไป ประกอบกับเหยื่ออาชญากรรมประเภทนี้มักจะไม่รายงานคดีให้ทางตำรวจทราบ เนื่องจากเกรงว่าจะกระทบต่อภาพลักษณ์ของบริษัทและขาดความเชื่อมั่นในขีดความสามารถของตำรวจในการสืบสวนสอบสวนเพื่อดำเนินคดีกับอาชญากรประเภทนี้ ปัจจัยเหล่านี้ทำให้ไม่ปรากฏสถิติของอาชญากรรมประเภทนี้ อย่างไรก็ตาม ในปัจจุบันนี้ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติได้พยายามติดตามและรวบรวมกรณีปัญหาเฉพาะที่เกิดขึ้นในประเทศหรือเกี่ยวพันกับบุคคลในชาติไว้เพื่อประโยชน์ในการศึกษาหาแนวทางป้องกันปราบปรามต่อไป

กรณีตัวอย่างอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยที่จะกล่าวต่อไปนี้เป็นเพียงตัวอย่างในรูปแบบการกระทำความผิดในแต่ละรูปแบบ ซึ่งไม่ได้หมายความว่าแต่ละรูปแบบจะเกิดขึ้นเพียง 1 ราย โดยแต่ละรูปแบบอาจเกิดขึ้นหลายครั้ง ไม่ว่าจะเป็นผู้กระทำผิดคนเดียวหรือหลายคน โดยจะขอยกตัวอย่างดังนี้ [27]

กรณีเว็บไซต์ Sanook.com เป็นการแอบอ้างชื่อส่งข้อมูลไปแจ้งขอแก้ไข IP Address ที่ InterNic * ซึ่งทาง InterNic นั้นใช้เครื่องคอมพิวเตอร์ทำงานรับข้อมูลและแก้ไขแบบอัตโนมัติแทนคนทั้งหมด โดยให้แก้เป็น IP Address หมายเลขอื่น ๆ ที่ไม่มีตัวตนจริง หลังจากนั้น InterNic จะกระจายข้อมูลไปยัง Root ต่าง ๆ ให้เปลี่ยนแปลง ดังนั้น เมื่อคนทั้งโลกจะเข้าเว็บไซต์

---

[26] ทวีศักดิ์ กออนันตกูล, "อาชญากรรมในยุคโลกาภิวัฒน์," บทบัณฑิตย์. หน้า 33-34.

[27] www.police.go.th/policenews/show.

* หน่วยงานรับจดทะเบียนชื่อโดเมนเนม (Domain Name) แบบ .com , .net หรือแบบอื่น ๆ ที่ ไม่ใช่การจดทะเบียนแบบของแต่ละประเทศ

ของ Sanook.com ก็จะชี้ไปยัง IP Address ปลอมดังกล่าว ทำให้ไม่สามารถเข้าเว็บไซต์จริงได้ ทั้ง ๆ ที่เว็บไซต์ของ Sanook.com ก็เปิดให้บริการอยู่ตามปกติ

กรณีการสั่งซื้อของจากการประมูลสินค้าออนไลน์ (Online Auctions) ผ่านเว็บไซต์ eBay.com เป็นเว็บไซต์ที่เปิดโอกาสให้บุคคลทั่วไปประกาศขายสินค้าโดยการประมูลบนเว็บไซต์ กรณีปัญหาก็คือมีบุคคลในประเทศไทยได้เข้าไปในเว็บไซต์ eBay.com และพบว่ามีชายอเมริกันได้ประกาศขายเครื่องโทรทัศน์ใช้แล้วขนาดจอภาพ 50 นิ้ว จึงเกิดความสนใจได้เข้าไปร่วมประมูล ต่อมาชายอเมริกันดังกล่าวได้ส่งอีเมล์ (e-mail) ว่าเป็นผู้ชนะการประมูล ขอให้ส่งเงินเข้าบัญชีเป็นจำนวน 266,000 บาท หลังจากนั้นบุคคลในประเทศไทยได้รับกล่องพัสดุขนาดใหญ่จากบริษัทขนส่ง Fed ex ที่กล่องเขียนว่าเป็นเครื่องใช้อิเล็กทรอนิกส์ แต่เมื่อเปิดกล่องดูพบว่าเป็นเพียงตู้กตาและเครื่องแก้วที่แตกแล้ว

กรณีเว็บไซต์ที่ส่งเสริมการขายสินค้าของไทยสู่ตลาดโลก 3 เว็บไซต์ ถูกใส่ร้ายจากกลุ่มผู้ไม่หวังดีปลอม e-mail ของเว็บไซต์ดังกล่าว แล้วส่งไปยังผู้ใช้อินเตอร์เน็ตทั่วโลกประมาณ 4 ล้านฉบับ เป็นลักษณะ Spam Mail * และได้ใส่ร้ายเว็บไซต์ดังกล่าวว่า "เป็นเว็บไซต์ที่ฉ้อโกง โดยจะนำชื่อและหมายเลขบัตรเครดิตของผู้ที่สนใจเข้ามาซื้อของไปใช้ในทางที่ผิด ขอให้อย่าเข้าเว็บไซต์ไทยทั้ง 3 ดังกล่าว" ผลร้ายที่เกิดขึ้นนอกจากจะทำให้คนทั้งโลกไม่เข้าไปชมเว็บไซต์ดังกล่าวแล้วยังทำให้องค์กรต่อต้าน Spam Mail สั่งให้ Web Hosting ยุติการให้บริการเว็บไซต์ไทยทั้งสามอีกด้วย

---

* สแปมเมล (Spam Mail) หรือเมล์ขยะ (Junk Mail) คือ เมล์ที่ส่งมาจากบุคคลที่คุณไม่รู้จักมาก่อน ซึ่งส่วนใหญ่จะเป็นการโฆษณาขายสินค้าหรือบริการต่าง ๆ ออนไลน์ หรือให้ร่วมประกอบธุรกิจต่าง ๆ ถ้าจะพูดถึงที่มาของจดหมายขยะเริ่มตั้งแต่ปี ค.ศ.1994 เกิดจากทนายความคนหนึ่งที่ต้องการโฆษณาสรรพคุณการว่าความของตนเองและหวังจะใช้เป็นช่องทางประหยัดในการทำการตลาด โดยใช้อินเตอร์เน็ตเป็นเครื่องมือส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่มีเนื้อความบรรยายผลงานของตนเองให้กับกลุ่มผู้ใช้งานอินเตอร์เน็ต เมื่อบุคคลดังกล่าวได้รับเมล์แล้วจะส่งต่อให้กับบุคคลอื่น เมื่อจดหมายดังกล่าวได้แพร่กระจายไปถึงมือผู้คนนับแสนนับล้านคนทั่วโลก จึงเป็นการจุดประกายให้กับฝ่ายการตลาดของบริษัทน้อยใหญ่ต่างลอกเลียนแบบส่งจดหมายโฆษณาสินค้าของตนเองให้กับกลุ่มผู้ใช้อินเตอร์เน็ตทั่วโลก จนกลายเป็นปัญหาที่น่าเบื่อของ เจ้าของอีเมล์แอดเดรสต่าง ๆ ที่ตู้จดหมายของเขาเต็มจากเมล์ที่ไม่ต้องการ ซึ่งวิธีการดังกล่าวกลุ่มอาชญากรก็เล็งเห็นถึงผลดี จึงได้นำวิธีการดังกล่าวมาใช้เป็นเครื่องมือในการประกอบอาชญากรรมเช่นกัน

การจัดทำเว็บไซต์การพนันเป็นภาษาไทย ทั้งการพนันทายผลฟุตบอลและคาสิโน โดยเป็นส่วนหนึ่งของเว็บไซต์การพนันที่มีชื่อเสียงและถูกต้องตามกฎหมายในต่างประเทศ

การเผยแพร่ภาพลามกอนาจาร ซึ่งเครื่องเซิร์ฟเวอร์ (Server) ส่วนมากอยู่ต่างประเทศ บางรายผู้จดทะเบียนโดเมนเนมแจ้งว่ามีอยู่ในประเทศไทย บางรายใช้ฟรีเว็บ และบางเว็บไซต์ใช้ภาษาไทย บางเว็บไซต์มีการตัดต่อภาพดาราเป็นภาพลามกอนาจาร บางเว็บไซต์เสมือนเป็นธุระจัดหาชาย-หญิงเพื่อการค้าประเวณี

การโฆษณาเป็นภาษาไทยขายเทป วีดีโอ CD ละเมิดลิขสิทธิ์ บางรายให้โอนเงินเข้าบัญชีธนาคารมีทั้งในประเทศและต่างประเทศ โดยระบุเลขที่บัญชีไว้ชัดเจน จัดทำให้ Download ภาพ เพลง MP3 ที่ละเมิดลิขสิทธิ์ของผู้อื่น

เผยแพร่ข้อมูลหมิ่นประมาทใส่ร้ายบุคคลอื่นบนเว็บไซต์ กระดานข่าว (web board) หรือจดหมายอิเล็กทรอนิกส์ (e-mail)

การจัดทำเว็บไซต์ขายสินค้าออนไลน์แล้วไม่ส่งสินค้าให้หรือทำหลอกไว้เพื่อเพียงต้องการหมายเลขและข้อมูลบัตรเครดิตไปใช้ในกรณีอื่น ๆ การสั่งซื้อสินค้า โดยใช้หมายเลขบัตรเครดิตของผู้อื่นหรือเลขที่บัตรที่ไม่มีตัวตนจริงแล้วให้ไปส่งที่บ้านคนอื่น ซึ่งคนร้ายสามารถตรวจสอบทางอินเตอร์เน็ตได้ว่าของจะส่งถึงวันใดเวลาใด คนร้ายจะไปเฝ้ารออยู่หน้าบ้านแล้วแสดงตัวรับสินค้าไป ทำให้ยากแก่การสืบสวนติดตาม

การจดทะเบียนโดเมนเนมที่มีชื่อคล้ายคลึงกับบริษัทหรือองค์กรที่มีชื่อเสียง เช่น Worldphone1800.com, Worldphone800.com, IBM Thailand.com แล้วเสนอขายชื่อโดเมนเนมให้ในราคาชื่อละ 100,000 บาท หากไม่ซื้อก็ขู่ว่าจะทำเป็นเว็บไซต์ลามก ทำให้เสียชื่อเสียง กรณีนี้ได้ทำการจับกุมแล้วในข้อหาพยายามกรรโชกทรัพย์ โดยคณะทำงานอาชญากรรมทางคอมพิวเตอร์ของกองปราบปราม สำนักงานตำรวจแห่งชาติ

กรณีนี้ผู้เสียหายเข้าร้องทุกข์กับพนักงานสอบสวน กองปราบปราม ให้สืบสวนดำเนินคดีกับผู้กระทำผิดที่ได้ฝากข้อความอัตโนมัติผ่านระบบเครือข่ายอินเตอร์เน็ตไปยังบริการโฟนลิงค์ 152 หมายเลข .. ซึ่งเป็นหมายเลขโฟนลิงค์ของผู้เสียหาย โดยมีข้อความด่าหยาบคายและขู่ฆ่า ทำให้เกิดความกลัวหรือตกใจ อันเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 392 ฐานทำให้ผู้อื่นเกิดความกลัวหรือความตกใจโดยการขู่เข็ญ ต้องระวางโทษจำคุกไม่เกิน 1 เดือน หรือปรับไม่เกิน 1,000 บาท หรือทั้งจำทั้งปรับ ชุดคณะทำงานสืบสวนสอบสวนปราบปรามอาชญากรรมทางอินเตอร์เน็ต กองปราบปรามได้ทำการสืบสวนและจับกุมตัวผู้ต้องหาไว้ได้ สอบสวนแล้วให้การรับสารภาพโดยมีพฤติการณ์ในการกระทำความผิดคือผู้ต้องหานี้เคยเป็นลูกจ้างทำงานให้กับผู้เสียหายในตำแหน่งผู้จัดการประมาณ 8-9 เดือน แต่ต่อมามีทัศนคติไม่ตรงกันจึงได้ออกจากงาน แต่ในใจยังคงมีความไม่พอใจกับผู้เสียหายตลอดมา จึงได้ใช้บริการอินเตอร์เน็ต ณ สถานบริการอินเตอร์เน็ตคาเฟ่ บริเวณศูนย์การค้าบิ๊กซีพระราม 2 โดยใช้บริการผ่านเว็บไซต์ WWW.HUNSA.COM ส่งข้อความไปยังบริการโฟนลิ้งค์ 152 หมายเลข .. ของผู้เสียหายอันเป็นข้อความด่าหยาบคาย ขู่ฆ่า และแจ้งให้หน่วยงานของรัฐทำการตรวจค้นทั้งที่บ้านและโรงงานทำให้ผู้เสียหายเกิดความหวาดกลัวหรือตกใจหลายครั้ง โดยเฉพาะในช่วงเดือนสิงหาคม 2543 จนกระทั่งเจ้าหน้าที่ตำรวจกองปราบปรามได้สืบสวนและจับกุมผู้ต้องหาไว้ได้และดำเนินคดีกับผู้ต้องหาตามกฎหมาย (รายงานการจับกุมผู้ต้องหากระทำผิดผ่านระบบเครือข่ายอินเตอร์เน็ตของเจ้าหน้าที่ตำรวจ กองปราบปราม สำนักงานตำรวจแห่งชาติ) [28]

3.2 **การหลอกลวงทางอินเตอร์เน็ต** (Internet Frauds)

ระบบเครือข่ายอินเตอร์เน็ตนับว่าเป็นระบบเครือข่ายคอมพิวเตอร์ที่ใหญ่ที่สุดในโลก และมีการเชื่อมต่อกันตลอดเพื่อให้บริการแก่ผู้ใช้อินเตอร์เน็ต ซึ่งก่อให้เกิดอาชญากรรมที่กระทำการโดยผ่านระบบเครือข่ายอินเตอร์เน็ตมากหมายหลายรูปแบบ เช่น การเข้าถึงเครื่องคอมพิวเตอร์โดยมิชอบ (Computer Network Break in) หรือการล้วงความลับทางอุตสาหกรรม (Industrial Espionage) การแพร่ภาพลามกเด็ก ข้อมูลล่าสุดทั่วโลกพบว่ามีเว็บไซต์ที่เกี่ยวข้องกับภาพลามกเด็กอยู่ถึง 70,000 เว็บไซต์ การส่งไปรษณีย์อิเล็กทรอนิกส์จนท่วมหน่วยความจำที่เรียกว่า mail bombing การเล่นพนันทางอินเตอร์เน็ต

---

[28] จักริน พันธ์ทอง, "อาชญากรรมคอมพิวเตอร์ : ศึกษากรณีดำเนินคดีอาชญากรรมคอมพิวเตอร์," (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะรัฐศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2543), หน้า 55.

การฟอกเงินทางอินเตอร์เน็ต การเจาะระบบข้อมูล โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ต (Internet Fraud) ที่กำลังแพร่ระบาดเป็นอย่างมากในขณะนี้

การก่ออาชญากรรมทางคอมพิวเตอร์นั้นผู้กระทำความผิดอาจจะก่ออาชญากรรมจากที่ใดก็ได้ในโลก โดยมีการส่งคำสั่งมาคุยกับเครื่องคอมพิวเตอร์ให้ทำอะไรก็ได้และระยะเวลาในการกระทำความผิดน้อย ใช้เวลาเพียงแค่วินาทีเท่านั้น นอกจากนั้นการพบผู้กระทำความผิดขณะกระทำความผิดเป็นไปได้ยาก เนื่องจากผู้กระทำความผิดมักจะกระทำความผิดในที่ลับตาคนและไม่จำต้องมาเจอกับผู้เสียหายก็สามารถกระทำความผิดได้ เช่น จากที่บ้านหรือจากร้านอินเตอร์เน็ตคาเฟ่ เป็นต้น ทำให้การสืบหาตัวผู้กระทำความผิดเป็นไปได้ยากลำบาก ประกอบกับระบบเครือข่ายอินเตอร์เน็ตเป็น Interactive ทำให้ทุก ๆ คนที่ใช้ระบบเครือข่ายอินเตอร์เน็ตมีโอกาสเป็น publisher คือ คนกระจายข้อมูล ซึ่งบางครั้งกระจายไปภายในเวลาเพียง 1 ชั่วโมง จะมีผู้อ่านเป็นแสนคน ถ้าเขียนในกระดานข่าว (web board) กล่าวคือ ใครก็ตามก็มีสิทธิ์ที่จะกระจายข่าว ไม่ว่าจริงหรือเท็จ หรือกล่าวได้ว่าระบบเครือข่ายอินเตอร์เน็ตได้เพิ่มอำนาจให้กับบุคคลในการกระทำความผิดพอ ๆ กับทำความดี จึงทำให้อาชญากรรมทางคอมพิวเตอร์โดยเฉพาะการหลอกลวงทางอินเตอร์เน็ตเพิ่มมากขึ้นทุกปี และสร้างปัญหาให้กับกระบวนการยุติธรรมของแต่ละประเทศเป็นอย่างมาก

3.2.1 ลักษณะของการหลอกลวงทางอินเตอร์เน็ต

ก่อนที่จะพิจารณาถึงการหลอกลวงทางอินเตอร์เน็ต ควรจะพิจารณาก่อนว่าการหลอกลวงนั้นมีลักษณะการกระทำอย่างไร

การหลอกลวง คือ การแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงอันควรบอกกล่าวให้แจ้ง ซึ่งจากการกระทำดังกล่าวทำให้ผู้หลอกลวงได้ไปซึ่งทรัพย์สิน การกระทำดังกล่าวเป็นความผิดอาญา ซึ่งประมวลกฎหมายอาญากำหนดไว้ว่ามีความผิดเกี่ยวกับทรัพย์ที่กำหนดไว้ในลักษณะ 12 ฐานความผิดฉ้อโกง ตามมาตรา 341-343 แล้วแต่กรณี ซึ่งความผิดตามมาตรา 341 เป็นความผิดฐานหลอกลวงบุคคลใดบุคคลหนึ่งเท่านั้น มาตรา 342 เป็นความผิดฐานหลอกลวงโดยการแสดงตนเป็นคนอื่น เป็นบทลงโทษบทหนักของมาตรา 341 สำหรับมาตรา 343 เป็นความผิดฐานหลอกลวงประชาชนทั่วไป ซึ่งผู้กระทำความผิดจะต้องรับโทษหนักขึ้นเช่นกัน

การหลอกลวงนับเป็นการประกอบอาชญากรรมรูปแบบหนึ่งที่มีมานานแล้ว ตั้งแต่การหลอกลวงโดยผ่านการติดต่อสื่อสารรูปแบบเดิม จนกระทั่งปัจจุบันนี้มีการพัฒนาเทคโนโลยีสารสนเทศ ได้นำโลกเข้าสู่ยุคโลกาภิวัฒน์ มีความเจริญเติบโตของระบบเครือข่ายอินเตอร์เน็ต มีการค้าผ่านทางอิเล็กทรอนิกส์ (Electronic Commerce) จึงมีผู้นำเอาเทคโนโลยีเหล่านี้มาเป็นช่องทางหรือเป็นเครื่องมือในการกระทำความผิด ซึ่งการหลอกลวงโดยกระทำผ่านทางระบบเครือข่ายอินเตอร์เน็ตนั้นถือเป็นอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่ง โดยขอบเขตของอาชญากรรมทางคอมพิวเตอร์จำต้องมีการใช้เครื่องคอมพิวเตอร์ในการกระทำความผิด (Computer Abuse) คือผลสำเร็จของการกระทำความผิดต้องอาศัยความรู้ความชำนาญเกี่ยวกับเครื่องคอมพิวเตอร์เป็นสำคัญ ซึ่งการหลอกลวงดังกล่าวจะทำให้ผู้กระทำความผิดได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวง

การหลอกลวงทางอินเตอร์เน็ตนั้นนับว่าเป็นมหันตภัยที่ร้ายแรงกว่าการหลอกลวงในรูปแบบเดิม ๆ เนื่องจากอาศัยความได้เปรียบของสื่อประเภทระบบเครือข่ายอินเตอร์เน็ต ทำให้สามารถเข้าถึงกลุ่มคนได้อย่างง่ายดาย รวดเร็ว และทั่วทุกคนทั่วโลก ซึ่งเป็นการลงทุนที่ต่ำและดูสมจริงมาก เพราะว่าระบบเครือข่ายอินเตอร์เน็ตสามารถสื่อสารได้ทุกรูปแบบ ไม่ว่าจะเป็นภาพ เสียง ทำให้ผู้ถูกหลอกลวงหลงเชื่อได้อย่างง่ายดาย ซึ่งวิธีการในการเข้าถึงบุคคลต่าง ๆ สามารถกระทำได้ทั้งทางเว็บไซต์ (web site) ทางจดหมายอิเล็กทรอนิกส์ (e-mail) ทางกระดานข่าว (web board) ทางห้องสนทนาอินเตอร์เน็ต (chat room) เป็นต้น ซึ่งง่ายกว่าการสื่อสารในรูปแบบเดิม ๆ ทำให้ผู้ถูกหลอกลวงไม่จำต้องทราบชื่อ หน้าตา ของผู้กระทำความผิด ประกอบกับโอกาสในการเข้าถึงเหยื่อเป็นไปได้ง่าย สะดวก และทีละจำนวนมาก ๆ

การหลอกลวงทางอินเตอร์เน็ตกำลังเป็นที่แพร่หลายในประเทศสหรัฐอเมริกา ดังจะเห็นได้จากสถิติการร้องเรียนจากผู้เสียหายมายังสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐอเมริกา (Federal Trade Commission : FTC) ในปี ค.ศ.1997 มีการร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตถึง 1,000 กว่าคน ในปี ค.ศ.1998 ได้รับการร้องเรียนถึง 8,000 กว่าคน และในปี ค.ศ.2000 ได้รับการร้องเรียนถึง 25,000 กว่าคน นอกจากสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติแล้วประเทศสหรัฐอเมริกายังมีหน่วยงานที่รับร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตอีกหลายหน่วยงาน เช่น FBI ได้จัดตั้งหน่วยงานรับเรื่องร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต คือ Internet Fraud Complaint Center : IFCC) ซึ่งมีผู้ร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตเป็นจำนวนมากเช่นกัน จากข้อมูลดังกล่าวจะเห็นได้ว่าอัตราการขยายตัวของการหลอกลวงทางอินเตอร์เน็ตนับวันจะยิ่งทวีความรุนแรงมากขึ้นทุกที

ซึ่งการร้องเรียนส่วนใหญ่จะเป็นร้องเรียนเกี่ยวกับการหลอกลวงโดยการประมูลสินค้าออนไลน์ การหลอกลวงบัตรเครดิต การหลอกลวงธุรกิจแชร์ลูกโซ่ การหลอกลวงให้ประกอบธุรกิจต่าง ๆ โดยอ้างว่าสามารถจะสร้างผลประโยชน์ตอบแทนได้จำนวนมหาศาล แต่ในความเป็นจริงแล้ว สิ่งที่กล่าวอ้างมาทั้งหมดเป็นการหลอกลวงเพื่อให้ได้ทรัพย์สินจากผู้ถูกหลอกลวงทั้งสิ้น ซึ่งตั้งแต่ปี ค.ศ.1994 สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐได้ดำเนินการฟ้องร้องคดีเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ตมากถึง 182 คดี ซึ่งมีผู้กระทำความผิดถึง 593 คน ซึ่งศาลได้มีการตัดสินให้จ่ายค่าเสียหายชดเชยแก่ผู้เสียหายรวมกันแล้วถึง 180 ล้านดอลลาร์สหรัฐ

กระทรวงยุติธรรมของประเทศสหรัฐอเมริกา (Department of Justice)ได้ให้นิยามคำว่า "การหลอกลวงทางอินเตอร์เน็ต" หมายถึง ประเภทของการหลอกลวงประเภทหนึ่ง ซึ่งเป็นการกระทำความผิดโดยใช้ระบบเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือ เช่น เป็นการกระทำโดยผ่านห้องสนทนา (Chat Room) ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ผ่านทางเว็บไซต์ (Web Site) หรือผ่านทางกระดานข่าว (Message Boards) เป็นต้น [29]

3.2.2 ประเภทของการหลอกลวงทางอินเตอร์เน็ต

เนื่องจากการหลอกลวงทางอินเตอร์เน็ตมีมากมายหลากลายรูปแบบ จากการที่ผู้วิจัยได้ศึกษาพบว่าข้อมูลจากเว็บไซต์ www.fraud.org ซึ่งเป็นเว็บไซต์ขององค์กรคุ้มครองผู้บริโภคที่ไม่ค้ากำไรที่เก่าแก่ที่สุดของสหรัฐอเมริกา คือ National Consumer League (NCL) ได้จำแนกประเภทของการหลอกลวงทางอินเตอร์เน็ตได้ 20 ประเภท ดังนี้ [30]

1. **การหลอกลวงเกี่ยวกับกู้ยืมเงินล่วงหน้า** (Advance Fee Loans)

การหลอกลวงประเภทนี้จะเป็นการหลอกลวงสำหรับบุคคลที่มีความจำเป็นต้องใช้จ่ายเงินโดยด่วนและบุคคลนั้นไม่มีเงินพอ เช่น คนว่างงาน คนที่ได้รับเงินเดือนน้อย จึงมีความจำเป็นที่จะต้องกู้ยืมเงิน แต่บุคคลเหล่านี้จะไม่มีหลักทรัพย์หรือไม่มีเครดิตหรือมีประวัติการเงินที่แย่ ทำให้ไม่สามารถจะยืมเงินจากธนาคารหรือสถาบันการเงินต่าง ๆ ได้ ซึ่งเป็นช่องทาง

---

[29] Internet fraud [Online]. Available from:http://www.internetfraud.usdoj.gov /htm. [2002, May 8]

[30] Internet Fraud Tips [Online]. Available from : http://www.fraud.org/internet /inttip/inttip.html. [2002, April 21]

ให้อาชญากรอาศัยโอกาสนี้หลอกลวงบุคคลดังกล่าวว่าสามารถทำให้คุณกู้ยืมเงินจากสถาบันการเงินต่าง ๆ หรือธนาคารได้ โดยผู้หลอกลวงจะรับประกันว่าคุณจะได้รับเงินกู้อย่างแน่นอน ซึ่งผู้ถูกหลอกลวงจะต้องเสียเงินค่าธรรมเนียมล่วงหน้าก่อนที่จะคุณจะได้อนุมัติการกู้ยืมเงิน โดยค่าธรรมเนียมจะขึ้นอยู่กับประเภทของการขอกู้ยืม หากเป็นการกู้ยืมในลักษณะบุคคล ค่าธรรมเนียมจะอยู่ระหว่าง 25 - 100 ดอลลาร์สหรัฐขึ้นไป สำหรับกรณีเป็นการกู้ยืมเพื่อประกอบธุรกิจขนาดเล็ก จะต้องเสียเงินค่าธรรมเนียมแพงกว่าบุคคลธรรมดากู้ยืมเงิน ประมาณหมื่นดอลลาร์สหรัฐขึ้นไป เมื่อผู้ถูกหลอกลวงตกลงจ่ายเงินค่าธรรมเนียมไปแล้ว ผู้หลอกลวงจะหายตัวไปพร้อมกับเงินค่าธรรมเนียมที่ผู้ถูกหลอกลวงจ่ายล่วงหน้า โดยไม่ติดต่อกลับมาอีกเลย และผู้ถูกหลอกลวงจะไม่ได้รับการติดต่อจากธนาคารหรือสถาบันการเงินที่ผู้หลอกลวงอ้างว่าผู้ถูกหลอกลวงจะได้รับอนุมัติเงินกู้เลย [31] แต่เดิมการหลอกลวงดังกล่าวมีแต่ในหนังสือพิมพ์ท้องถิ่น หนังสือพิมพ์ต่างประเทศ นิตยสาร แต่ปัจจุบันนี้การหลอกลวงประเภทดังกล่าวได้แพร่หลายมากทางระบบเครือข่ายอินเตอร์เน็ต ซึ่งในความเป็นจริงแล้วการหลอกลวงดังกล่าวไม่มีทางเป็นจริงได้ เพราะไม่มีทางที่ผู้หลอกลวงจะสามารถรับประกันได้ว่าใครจะได้รับอนุมัติการกู้ยืมเงินหรือไม่ โดยเฉพาะบุคคลที่ไม่มีหลักทรัพย์หรือว่ามีประวัติการเงินที่ไม่ดี ไม่มีความน่าเชื่อถือทางการเงินหรือคล้ายละลายมาก่อน

ซึ่งสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐอเมริกา (FTC) ได้เปิดเผยว่าตั้งแต่เดือนกันยายน ค.ศ.1999 ถึงเดือนมิถุนายน ค.ศ. 2000 มีผู้ร้องเรียนเข้ามาเกี่ยวกับการหลอกลวงประเภทนี้ 4,200 ราย มูลค่าความเสียหายมากกว่า 1 ล้านดอลลาร์สหรัฐ และมีการฟ้องร้องคดีสู่ศาลหลายคดี เช่น คดีระหว่าง FTC กับ Christopher Puma ว่าได้กระทำการหลอกลวงเกี่ยวกับการกู้ยืมเงินล่วงหน้า โดยเรียกเก็บค่าธรรมเนียมตั้งแต่ 149-189 ดอลลาร์สหรัฐ แล้วแต่ประเภทของการกู้ยืมเงิน ซึ่งศาลได้สั่งให้จำเลยชดใช้ความเสียหายให้แก่ผู้เสียหาย 4,932 คน เป็นเงิน 120,000 ดอลลาร์สหรัฐ และได้ตัดสินจำคุกจำเลย 120 วัน และได้สั่งคุมประพฤติจำเลยเป็นระยะเวลา 3 ปี อีกด้วย [32] หรือคดีบริษัท Navestar DM ซึ่งตั้งอยู่ที่

---

[31] FTC, Easy Credit? Not So Fast : The Truth About Advance-Fee Loan Scams [Online]. Available from: http://www.ftc.gov/bcp/conline/pibs/tmarkg/loans.htm. [2002, January 9]

[32] FTC, ftc refunds more than $120,000 lost by consumers in advance fee loan scam [Online]. Available from: http://www.ftc.gov/opa/1996/9603/south.htm. [2002, June 10]

นิวยอร์ก ได้ดำเนินกิจการหลอกลวงโดยอ้างว่าสามารถหาเงินกู้ให้ โดยเรียกเก็บค่าธรรมเนียมล่วงหน้า 45-60 ดอลลาร์สหรัฐ โดยกระทำผ่านจดหมายอิเล็กทรอนิกส์ (e-mail) เมื่อผู้ถูกหลอกลวงหลงเชื่อจ่ายเงินค่าธรรมเนียมไป ก็ไม่ได้รับการกู้ยืมเงินอย่างที่ผู้หลอกลวงกล่าวอ้าง และก็ไม่ได้รับการติดต่อจากบริษัทนี้อีกเลยคดีนี้อยู่ระหว่างการพิจารณาคดีของศาล ซึ่งขณะนี้ศาลได้สั่งระงับการประกอบกิจการดังกล่าวและสั่งยึดทรัพย์ของจำเลยแล้ว [33]

2. **การหลอกลวงเกี่ยวกับการประกอบธุรกิจ** (Business Opportunities and Franchises)

การหลอกลวงประเภทนี้จะกระทำโดยผ่านทางเว็บไซต์ (Web Site) จดหมายอิเล็กทรอนิกส์ (E-Mail) โดยจะหลอกลวงว่าการเริ่มต้นประกอบธุรกิจด้วยตนเองหรือการเป็นเจ้าของธุรกิจหนึ่งธุรกิจใดเป็นเป็นสิ่งที่ง่ายดาย และจะได้รับผลตอบแทนที่แน่นอนเป็นจำนวนมหาศาลโดยไม่มีการเสี่ยง บางธุรกิจอ้างว่าผู้เข้าร่วมธุรกิจดังกล่าวจะได้รับผลประโยชน์ตอบแทนมากถึงวันละ 140 ดอลลาร์สหรัฐ ถึง 1,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น ซึ่งในความเป็นจริงแล้วการประกอบธุรกิจทุกประเภทย่อมมีความเสี่ยงทั้งสิ้น ถ้าธุรกิจใดได้ผลประโยชน์ตอบแทนน้อย อัตราความเสี่ยงก็น้อย ถ้าธุรกิจใดที่จะได้รับผลประโยชน์ตอบแทนมาก ย่อมต้องมีอัตราความเสี่ยงสูงมากขึ้นเป็นเงาตามตัวด้วยเช่นกัน

การหลอกลวงเกี่ยวกับการประกอบธุรกิจมีมากหมายหลายรูปแบบ เช่น การเป็นเจ้าของธุรกิจตู้ขายสินค้าอัตโนมัติ (Automatic Machine) เช่น ตู้ขายน้ำอัตโนมัติ ตู้ขายหนังสือพิมพ์ ซึ่งผู้หลอกลวงจะโฆษณาว่าหากร่วมประกอบธุรกิจในการซื้อตู้ขายสินค้าอัตโนมัติจะสามารถสร้างรายได้เป็นพันดอลลาร์จากการขายสินค้าดังกล่าว โดยผู้หลอกลวงอ้างว่าจะเป็นผู้ติดต่อหาทำเลในการนำตู้ขายสินค้าอัตโนมัติดังกล่าวไปตั้งไว้ เช่น สนามบิน ห้างสรรพสินค้า โรงแรม แม้ตู้ขายสินค้าดังกล่าวจะมีราคาแพงกว่าปกติ แต่ผู้ซื้อจะได้รับเงินคืนกลับมาอย่างรวดเร็วเพียงเวลาไม่กี่เดือน และยังได้มีการนำเอาบุคคลที่เคยร่วมประกอบธุรกิจดังกล่าวมาบรรยายถึงรายได้ที่บุคคลเหล่านั้นเคยได้รับมาเป็นเงินก้อนโต้แล้ว ซึ่งในความเป็นจริงแล้วเมื่อผู้ถูกหลอกลวงซื้อตู้ขายสินค้าอัตโนมัติดังกล่าว ผู้หลอกลวงจะไม่หาทำเลที่ตั้งให้อย่างที่กล่าวอ้าง แต่จะหาสถานที่ตั้งที่ไม่ดีและขายสินค้าไม่ได้ ซึ่งทำให้ผู้ถูกหลอกลวงสูญเสียเงินในการซื้อตู้ขายสินค้าอัตโนมัติดังกล่าวไปในราคาที่แพงกว่าปกติและไม่มีทางที่จะถอนทุนคืนมาได้

---

[33] FTC, State and Canadian Province Launch Crackdown On Outfits Falsely Promising Credit Cards and Loans for an Advance Fee [Online]. Available from: http:// www. ftc.gov/ opa/2000/06/afl2000.htm. [2002, July 9]

เลย [34] เช่น คดีที่เกิดขึ้นที่มลรัฐแมรีแลนด์ ได้มีสามีภรรยาคู่หนึ่งจ่ายเงิน 35,000 ดอลลาร์สหรัฐ เพื่อซื้อตู้ขายสินค้าอัตโนมัติจากผู้ขาย ซึ่งบอกว่าจะสามารถสร้างรายได้เดือนละ 7,500 บาท เมื่อได้รับตู้สินค้าดังกล่าวแล้วปรากฏว่า 6 เดือน ผู้ซื้อได้รับเงินจากการขายสินค้าเพียง 50 ดอลลาร์สหรัฐเท่านั้น[35] หรือกรณีหลอกลวงว่าคุณจะสามารถหาเงินได้เป็นแสน ๆ จากทางระบบเครือข่ายอินเตอร์เน็ต ซึ่งผู้หลอกลวงจะทำหน้าที่เป็นที่ปรึกษาให้คำแนะนำแก่ผู้ที่ต้องการประกอบธุรกิจทางระบบเครือข่ายอินเตอร์เน็ต โดยจะมีการจัดสัมมนาให้ความรู้เกี่ยวกับการประกอบธุรกิจทางระบบเครือข่ายอินเตอร์เน็ตว่าต้องกระทำอย่างไรถึงจะได้รับผลประโยชน์ตอบแทนจำนวนมหาศาล ซึ่งผู้ถูกหลอกลวงจะต้องเสียเงินค่าอบรม เมื่อผู้ถูกหลอกลวงจ่ายเงินค่าอบรมไปแล้ว ปัญหาที่ตามว่าคือผู้ถูกหลอกลวงจะไม่ได้รับความรู้เกี่ยวกับการประกอบธุรกิจทางระบบเครือข่ายอินเตอร์เน็ตแต่อย่างใด หรือว่าได้รับการอบรม แต่ในความเป็นจริงแล้วการประกอบธุรกิจดังกล่าวไม่มีทางที่จะสร้างรายได้ให้กับผู้ถูกหลอกลวงได้[36] ซึ่งส่วนใหญ่แล้วการหลอกลวงรูปแบบนี้จะกระทำโดยผ่านทางจดหมายอิเล็กทรอนิกส์ (e-mail)

การหลอกลวงประเภทนี้สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ได้พบการกระทำความผิดดังกล่าวผ่านทางระบบเครือข่ายอินเตอร์เน็ตอย่างแพร่หลาย จากการสำรวจเมื่อวันที่ 21 เมษายน 1997 พบว่ามีเว็บไซต์ที่ต้องสงสัยว่าประกอบอาชญากรรมดังกล่าว 215 เว็บไซต์ ซึ่งสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐได้ส่งอีเมล์เตือนเว็บไซต์ดังกล่าวว่าการกระทำของเว็บไซต์นั้นเข้าข่ายผิดกฎหมาย จากการส่งอีเมล์เตือนดังกล่าวปรากฏว่า 24 เว็บไซต์ได้ปิดตัวลงไป ส่วนที่เหลืออีก 191 เว็บไซต์ยังเปิดประกอบกิจการอยู่ต่อไป ซึ่งสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐจะได้ดำเนินการฟ้องร้องต่อศาลต่อไป

---

[34] FTC, Net – Based Business Opportunities: Beware of Flop– portunities [Online]. Available from:http://www..ftc.gov/bcp/conline/pbs/alerts/netalrt.htm. [2002, August 8]

[35] FTC, Can you Recognize a Business Opportunity Fraud [Online]. Available from: http://www.ftc.gov/bcp/conline/features/bizopps.htm.[2002, February 15]

[36] FTC, Net Based Business Opportunity : Are some Flop-portunities? [Online]. Available from:http://www.ftc.gov/bcp/conline/pubs/online/netbizop.htm. [2002,June 20]

เมื่อการชำระเงินสามารถกระทำได้โดยง่าย โดยผู้ซื้อและผู้ขายไม่จำเป็นต้องเห็นหน้ากัน เพียงกรอกรายละเอียดเกี่ยวกับบัตรเครดิตเท่านั้น ทำให้เป็นช่องทางที่มีผู้นำข้อมูลบนบัตรเครดิตของผู้อื่นไปชำระค่าสินค้าหรือค่าบริการ โดยที่ตัวเองไม่มีอำนาจกระทำได้ ซึ่งวิธีการหลอกลวงประเภทนี้กระทำได้อย่างง่ายดาย เพียงแต่ใส่หมายเลขบัตร ชื่อ และวันหมดอายุของบัตรเครดิตเท่านั้น โดยร้านค้าที่ได้รับชำระค่าสินค้าดังกล่าวสามารถตรวจสอบได้เพียงว่าบัตรดังกล่าวเป็นบัตรที่ออกโดยผู้ออกบัตรจริง แต่ไม่สามารถตรวจสอบได้ว่าผู้เป็นเจ้าของบัตรเป็นผู้ชำระบริการหรือสินค้าจริงหรือไม่ ซึ่งการหลอกลวงดังกล่าวมีหลากลายรูปแบบเพื่อที่ผู้หลอกลวงจะได้ไปซึ่งข้อมูลบนบัตรเครดิตของผู้อื่น เช่น

1. การเปิดเว็บไซต์ให้บริการหรือดาว์นโหลดดูภาพลามกอนาจารฟรี สำหรับผู้ที่มีอายุตั้งแต่ 18 ปีขึ้นไป (ตามกฎหมายสหรัฐอเมริกา บุคคลที่อายุเกิน 18 ปี สามารถเข้าดูเว็บไซต์ลามกได้โดยไม่ผิดกฎหมาย ดังนั้นเว็บไซต์ดังกล่าวจะทำการกล่าวอ้างว่าเผื่อเป็นการป้องกันตนเอง จึงต้องขอตรวจสอบก่อนว่าผู้เข้าดูมีอายุถึงตามเกณฑ์ที่กฎหมายกำหนดหรือไม่) โดยวิธีการที่จะยืนยันว่าผู้เข้าดูมีอายุถึง 18 ปี หรือไม่ ผู้หลอกลวงจะอ้างว่าให้ผู้เข้าใช้บริการกรอกรายละเอียดเกี่ยวกับบัตรเครดิต โดยผู้หลอกลวงอ้างว่าจะนำไปตรวจสอบดูว่าผู้เข้าดูมีอายุถึงตามเกณฑ์ที่กฎหมายกำหนดไว้หรือไม่ เมื่อผู้ถูกหลอกลวงให้รายละเอียดเกี่ยวกับบัตรเครดิตของตนเองแล้ว โปรแกรมบนเครื่องคอมพิวเตอร์ก็จะบันทึกรายละเอียดเกี่ยวกับบัตรเครดิตไว้ และผู้หลอกลวงก็จะนำรายละเอียดนั้นไปใช้จ่ายซื้อสินค้าทางเว็บไซต์อื่น ๆ ที่ถูกกฎหมายได้

2. การเปิดเว็บไซต์ขายสินค้าราคาถูก (เมื่อเปรียบเทียบราคากับเว็บไซต์อื่น ๆ ที่ขายของถูกกฎหมาย) เมื่อผู้ซื้อตัดสินใจซื้อสินค้าแล้ว เว็บไซต์ดังกล่าวจะระบุให้ผู้ซื้อชำระเงินด้วยบัตรเครดิตเท่านั้น เมื่อผู้ให้บริการบัตรเครดิตหรือธนาคารเรียกเก็บเงินค่าสินค้า ผู้ซื้อจะพบว่ามีค่าใช้จ่ายรายการอื่นที่ตนเองไม่ได้ใช้จ่ายปรากฏอยู่ในใบเรียกเก็บเงินด้วย เพราะผู้หลอกลวงจะนำข้อมูลบัตรเครดิตนั้นไปชำระค่าสินค้าหรือบริการอื่น ๆ จากเว็บไซต์ที่ขายสินค้าถูกกฎหมาย

3. เป็นกรณีซื้อขายสินค้าหรือให้บริการผ่านเว็บไซต์และกำหนดให้ชำระเงินค่าสินค้าหรือบริการด้วยบัตรเครดิตเท่านั้น ซึ่งเว็บไซต์ดังกล่าวจะขายสินค้าที่มีมูลค่าสูง เช่น กล้องวิดีโอ นาฬิกา แต่จะเสนอขายให้ในราคาถูกมาก (เมื่อเปรียบเทียบกับราคาของจริงหรือเปรียบเทียบกับเว็บไซต์อื่นที่ขายของถูกกฎหมาย) เพื่อเป็นการจูงใจให้ผู้ซื้อตัดสินใจซื้อสินค้าดังกล่าว โดยเมื่อผู้ถูกหลอกลวงตกลงซื้อสินค้าดังกล่าวแล้วยังไม่ต้องชำระเงินค่าสินค้าหรือค่าบริการล่วงหน้า

แต่จะต้องมีการแจ้งชื่อและรหัสบัตรเครดิตของผู้ซื้อให้ผู้ขายทราบ โดยอ้างว่าเพื่อป้องกันการที่ผู้ขายไม่ได้รับเงินค่าสินค้าเมื่อผู้ซื้อได้รับสินค้าแล้ว ทำให้มีผู้ถูกหลอกลวงหลายคนหลงเชื่อเพราะคิดว่าเมื่อได้รับของแล้วจึงจ่ายเงินค่าสินค้า ไม่มีการหลอกลวงที่จะให้ชำระเงินค่าสินค้าไปก่อนแล้วไม่ได้รับสินค้า ซึ่งความจริงหาเป็นเช่นนั้นไม่ เพราะผู้หลอกลวงจะเอาชื่อและรหัสบัตรเครดิตของผู้ซื้อไปซื้อสินค้าจากเว็บไซต์อื่นที่ถูกกฎหมายและนำสินค้านั้นส่งมาให้ผู้ซื้อ เมื่อผู้ซื้อได้รับสินค้าแล้วและพบว่าสินค้าดังกล่าวตรงตามที่กล่าวอ้าง จึงจ่ายเงินค่าสินค้าให้ผู้หลอกลวงไป สิ่งที่ตามมาคือผู้ซื้อจะต้องชำระค่าสินค้าที่ชำระด้วยบัตรเครดิตซึ่งมาจากการซื้อสินค้าจากเว็บไซต์ที่ถูกกฎหมายอีกด้วย

สำหรับการหลอกลวงประเภทนี้ได้สร้างความเสียหายให้กับประเทศสหรัฐอเมริกาเป็นจำนวนมากและประเทศไทยก็ยังได้รับอิทธิพลจากการหลอกลวงประเภทดังกล่าว ดังจะเห็นได้จากธนาคารไทยพาณิชย์ได้ประกาศแจ้งเตือนผู้ซื้อสินค้าและบริการผ่านทางอินเตอร์เน็ตให้อ่านเงื่อนไขทั้งหมดโดยละเอียดและให้เข้าใช้บริการเว็บไซต์ที่น่าเชื่อถือได้เท่านั้น และได้ประเมินมูลค่าความเสียหายที่เกิดขึ้นจากการถูกฉ้อโกงบัตรเครดิตทั้งจากการซื้อของทางอินเตอร์เน็ตและการซื้อของโดยทั่วไป คิดเป็นมูลค่ากว่า 100 ล้านบาทต่อปี [37]

ความรับผิดทางกฎหมายสำหรับกรณีการหลอกลวงเกี่ยวกับบัตรเครดิตนั้น ประเทศสหรัฐอเมริกาได้มีการบัญญัติกฎหมาย The Fair Credit Billing Act (FCBA) กำหนดกรณีที่ไม่ได้ใช้จ่ายบัตรเครดิตด้วยตนเองหรือว่าบัตรเครดิตสูญหายหรือถูกขโมย เจ้าของบัตรเครดิตไม่ต้องรับผิดชอบค่าใช้จ่ายที่เกิดจากบัตรเครดิตดังกล่าว โดยเจ้าของบัตรเครดิตจะต้องแจ้งหายต่อบริษัทเจ้าของบัตรทันทีที่ทราบ โดยบริษัทส่วนใหญ่จะมีบริการรับแจ้งบัตรเครดิตหายหรือถูกขโมยตลอด24 ชั่วโมง แต่ถ้าเจ้าของบัตรเครดิตไม่ได้แจ้งแก่บริษัทหรือแจ้งหลังจากบัตรเครดิตนั้นได้ถูกนำไปใช้แล้ว เจ้าของบัตรเครดิตจะต้องรับผิดชอบต่อค่าใช้จ่ายที่เกิดขึ้นเป็นจำนวนเงินไม่เกิน 50 ดอลลาร์สหรัฐอเมริกา สำหรับกรณีที่ปรากฏว่าในใบแจ้งหนี้มียอดค่าใช้จ่ายที่เจ้าของบัตรเครดิตไม่ได้ใช้จ่ายนั้น กฎหมายกำหนดว่าเจ้าของบัตรเครดิตไม่จำต้องรับผิดชอบในค่าใช้จ่ายที่เกิดขึ้น[38] สำหรับกฎหมายประเทศไทยนั้นกำหนดไว้ในพระราชบัญญัติคุ้มครอง

---

[37] http://www.police.go.th/policenews/show.php?news.

[38] FTC, Billed for Merchandise You Never Received [Online]. Available from : http:// www.ftc.gov/bcp/conline/pubs/credit/billed.htm [2002,September 30]

ผู้บริโภค พ.ศ.2522 (แก้ไขเพิ่มเติม พ.ศ. 2542) กำหนดให้ธุรกิจบัตรเครดิตเป็นธุรกิจที่ควบคุมสัญญา ซึ่งหมายความว่า ข้อกำหนดเงื่อนไขต่าง ๆ ในการใช้บัตรเครดิตที่ธนาคารหรือผู้ให้บริการบัตรเครดิตกำหนดไว้ในบัตรเครดิตนั้นจะต้องอยู่ภายใต้กฎหมาย ซึ่งข้อกำหนดดังกล่าวบังคับใช้กับบัตรเครดิตที่ทำขึ้นหลังวันที่ 1 มกราคม 2543 (วันที่กฎหมายฉบับนี้บังคับใช้) หรือบัตรเครดิตที่ทำขึ้นก่อนหน้าวันที่ 1 มกราคม 2543 และมีระยะเวลาครบ 1 ปี ต้องมีข้อกำหนดในการให้บริการบัตรเครดิตแก่ผู้บริโภคว่าในกรณีที่ธนาคารหรือผู้ให้บริการบัตรเครดิตมีข้อตกลงว่าผู้บริโภคสามารถสั่งซื้อสินค้าหรือบริการได้โดยใช้บัตรเครดิต เพียงแค่แจ้งหมายเลขบัตรเครดิตด้วยวาจาหรือลายลักษณ์อักษรให้แก่ผู้ขายสินค้าหรือผู้ให้บริการทำการเรียกเก็บเงิน ต้องมีข้อความต่อไปนี้

1. หากผู้บริโภคทักท้วงว่าไม่ได้ซื้อสินค้าหรือรับบริการจากผู้ขายหรือผู้ให้บริการ ธนาคารหรือผู้ให้บริการบัตรเครดิตต้องระงับการเรียกเก็บเงินจากผู้บริโภคก่อนทันที หรือหากเรียกเก็บไปแล้วก็ต้องคืนแก่ผู้บริโภค

2. ผู้บริโภคมีสิทธิยกเลิกการซื้อสินค้าหรือรับบริการภายใน 45 วันนับแต่วันที่ผู้บริโภคสั่งซื้อหรือขอรับบริการหรือภายใน 30 วันนับแต่วันถึงกำหนดส่งมอบสินค้าหรือบริการ หากผู้บริโภคพิสูจน์ได้ว่าตนเอง (1) ไม่ได้รับสินค้า (2) ไม่ได้รับบริการ (3) ได้รับสินค้าและบริการแต่ไม่ตรงตามกำหนดเวลา หรือได้รับสินค้าหรือบริการแต่ไม่ครบถ้วน หรือชำรุดบกพร่องหรือไม่ถูกต้องตามความประสงค์ โดยธนาคารหรือผู้ให้บริการบัตรเครดิตต้องระงับการเรียกเก็บเงินจากผู้บริโภค และหากธนาคารหรือผู้ให้บริการบัตรเครดิตเรียกเก็บเงินไปแล้ว ถ้าเป็นการซื้อสินค้าหรือบริการโดยใช้บัตรเครดิตภายในประเทศ ธนาคารหรือผู้ให้บริการบัตรเครดิตต้องคืนเงินให้กับผู้บริโภคภายใน 30 วัน นับแต่วันที่ผู้บริโภคแจ้ง แต่ถ้าเป็นการสั่งซื้อสินค้าหรือบริการจากต่างประเทศ ธนาคารหรือผู้ให้บริการบัตรเครดิตต้องคืนเงินให้กับผู้บริโภคภายใน 60 วันนับแต่วันที่ผู้บริโภคแจ้ง

จากหลักกฎหมายดังกล่าวเมื่อผู้ซื้อซื้อสินค้าหรือบริการผ่านเว็บไซต์ต่าง ๆ ซึ่งต้องกรอกหมายเลขบัตรเครดิต ชื่อ นามสกุล และวันหมดอายุของบัตรเครดิต ให้แก่เว็บไซต์ผู้ขายหรือให้บริการเพื่อชำระค่าสินค้าและบริการนั้น หากมีบุคคลอื่นนำหมายเลขบัตรเครดิตของผู้ซื้อไปใช้โดยมิชอบหรือการเจาะระบบเข้ามาเอาข้อมูลดังกล่าวและนำข้อมูลไปใช้โดย

ไม่ได้รับอนุญาต ผู้ซื้อจะได้รับสิทธิตามกฎหมายคุ้มครองผู้บริโภคฉบับนี้ที่จะปฏิเสธที่จะไม่ชำระเงินแก่ธนาคารหรือผู้ให้บริการบัตรเครดิตได้ หากผู้ซื้อสามารถพิสูจน์ได้ว่าไม่ได้ซื้อสินค้าหรือบริการดังกล่าวจริงหรือซื้อสินค้าหรือบริการแต่ไม่ถูกต้องครบถ้วน

ปัญหาประการต่อมาคือหากธนาคารหรือผู้ให้บริการบัตรเครดิตไม่ระบุถึงข้อสัญญาในการให้บริการบัตรเครดิตถึงสิทธิดังกล่าวของผู้บริโภคในการปฏิเสธการชำระเงินเอาไว้ในสัญญาให้บริการบัตรเครดิตระหว่างผู้ใช้บริการกับธนาคาร กรณีดังกล่าวนี้ผลในทางกฎหมายจะแตกต่างกันหรือไม่ มาตรา 35 ตรี ของพระราชบัญญัติคุ้มครองผู้บริโภคว่าด้วยการคุ้มครองผู้บริโภคในด้านสัญญา พ.ศ.2542 * กำหนดให้ข้อกำหนดในเรื่องที่ธนาคารหรือผู้ให้บริการบัตรเครดิตต้องคืนเงินแก่ผู้บริโภคในกรณีที่ผู้บริโภคไม่ได้ใช้บัตรเครดิตนั้นซื้อสินค้าหรือบริการ ไม่ได้รับสินค้าหรือบริการ หรือสินค้าชำรุดบกพร่อง ว่าเป็นข้อสัญญาที่จำเป็นต้องระบุไว้ หากธนาคารหรือผู้ให้บริการบัตรเครดิตไม่ได้กำหนดสิทธิของผู้บริโภคดังกล่าวไว้ในข้อสัญญา โดยหลักกฎหมายถือว่าสัญญาให้บริการบัตรเครดิตของธนาคารมีข้อสัญญาดังกล่าวโดยปริยายและมีผลบังคับใช้โดยทันที หรือพูดง่าย ๆ ก็คือ ถึงแม้สัญญาไม่ได้เขียนไว้ก็ให้ถือเสมือนเขียนไว้ด้วย

แม้ว่าจะมีกฎหมายให้ความคุ้มครองผู้บริโภคกำหนดหลักเกณฑ์ให้ผู้ถูกหลอกลวงไม่ต้องรับผิดชอบเกี่ยวกับค่าใช้จ่ายที่เกิดจากบัตรเครดิตที่ตนไม่ได้ใช้ก็ตาม แต่การพิสูจน์ว่าตนไม่ได้เป็นผู้ใช้บัตรเครดิตดังกล่าวชำระค่าสินค้าหรือบริการ หรือการขอรับเงินคืนจากธนาคารก็จะเสียเวลามาก ดังนั้นเพื่อป้องกันปัญหาการชำระค่าสินค้าด้วยบัตรเครดิตนั้น ธนาคารและบริษัทผู้ให้บริการบัตรเครดิตได้พยายามหามาตรการต่าง ๆ เช่น ประเทศสหรัฐอเมริกา เพียงแต่บอกชื่อและเลขที่บัตรเครดิตกรอกลงในแบบฟอร์มบนหน้าจอภาพแล้วส่งผ่านระบบเครือข่ายอินเตอร์เน็ต ผู้ขายก็จะสามารถไปเก็บเงินจากธนาคารเป็นค่าสินค้านั้นได้ทันที ข้อที่ต้องพึงระวังก็คือเวลากรอกข้อมูลเหล่านี้ลงไป ข้อมูลอาจถูกดักฟังหรือดักอ่านโดยมือที่สาม เพื่อเอาชื่อและเลขที่บัตรเครดิตของเราไปใช้จ่ายอย่างอื่นที่เราไม่รู้ไม่เห็นได้ ดังนั้นในการส่งข้อมูลส่วนนี้จึงต้อง

---

* พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522 แก้ไขเพิ่มเติม พ.ศ.2542 มาตรา 35 ตรี กำหนดว่าเมื่อคณะกรรมการว่าด้วยสัญญากำหนดให้สัญญาการประกอบธุรกิจที่ควบคุมสัญญาต้องใช้ข้อสัญญาใดหรือต้องใช้ข้อสัญญาใด โดยมีเงื่อนไขในการใช้ข้อสัญญานั้น ด้วยมาตรา 35 ทวิ แล้ว ถ้าสัญญานั้นไม่ใช้ข้อสัญญาดังกล่าวหรือใช้ข้อสัญญาดังกล่าวแต่ไม่เป็นไปตามเงื่อนไข ให้ถือว่าสัญญานั้นใช้ข้อสัญญาดังกล่าวหรือใช้ข้อสัญญาดังกล่าวตามเงื่อนไขนั้นแล้วแต่กรณี

มีการพัฒนาวิธีการเข้ารหัสแบบต่าง ๆ เพื่อมิให้ผู้ไม่เกี่ยวข้องซึ่งอยู่กลางทางดักอ่านไปได้ นอกจากนี้แล้วยังมีการพัฒนาวิธีการชำระเงินผ่านระบบเครือข่ายอินเตอร์เน็ตในรูปแบบอื่น ๆ ที่ไม่ใช่บัตรเครดิตโดยตรงอีกหลายแบบ ซึ่งมักจะทำผ่านบริษัทผู้ให้บริการคนกลางในเรื่องการจ่ายเงิน ไม่ว่าจะเป็น Digi Cash (E cash), Cyber Cash, First Virtual เป็นต้น E cash ของบริษัท Digi Cash เป็นการนำเอาเงินจริงไปซื้อ "เงินสดอิเล็กทรอนิกส์" จากบริษัทไว้ก่อน เวลาจะซื้อของหรือจ่ายค่าบริการใด ๆ ผ่านทางระบบเครือข่ายอินเตอร์เน็ตก็จ่ายด้วยเงินอิเล็กทรอนิกส์ โดยไม่ต้องเสี่ยงส่งเลขที่บัตรเครดิตให้ใคร มีเงินอยู่เท่าไร เมื่อใช้หมดก็จบแล้วก็ไปแลกมาเพิ่ม[39] หรือในประเทศไทยได้เพิ่มมาตรการที่เข้มงวดรัดกุม โดยการใช้วิธีการสื่อสารอื่น ๆ เข้าช่วย เช่น แฟกซ์ใบสั่งซื้อมาให้ผู้ซื้อกรอกเลขที่บัตรเครดิตและเซ็นชื่อกำกับ จากนั้นจึงแฟกซ์กลับ หรือกรณีธนาคารกสิกรไทยได้ออกบริการใหม่เป็น Virtual Shopping Card บัตรเครดิตสำหรับการจับจ่ายผ่านระบบเครือข่ายอินเตอร์เน็ตโดยเฉพาะ ซึ่งไม่มีตัวบัตรจริง มีแต่รหัสเลขที่บัญชี (Account) และแยกต่างหากจากบัตรเครดิตธรรมดา คือสำหรับใช้เฉพาะการซื้อสินค้าออนไลน์เท่านั้น โดยมีลักษณะเป็นบัตรเดบิต (Debit Card) คล้ายกับบัตรเดบิตที่เป็นบัตรจริง เช่น Visa Electron คือการตรวจสอบวงเงินในบัญชีและหักเงินไว้ชำระค่าสินค้าทันที โดยไม่มีการให้เครดิตผ่อนชำระแต่อย่างใด บัตรช็อปปิ้งออนไลน์นี้จะใช้ได้ตามวงเงินที่ทิ้งไว้ในบัญชีที่ผูกกับบัตรใบนั้นจริง ๆ ทำให้ไม่ต้องกังวลเรื่องความปลอดภัยของบัตรเครดิตจริงที่ใช้อยู่[40]

5. **การหลอกลวงเกี่ยวกับซื้อขายสินค้าออนไลน์** (General Merchandise Sales)

เนื่องจากข้อดีของระบบเครือข่ายอินเตอร์เน็ตที่ทำให้เกิดเครือข่ายสารสนเทศขนาดใหญ่ที่มีการเชื่อมโยงไปทั่วทุกมุมโลก เมื่อนำเทคโนโลยีดังกล่าวมาประยุกต์เข้ากับธุรกิจที่มีอยู่ ทำให้เกิดการค้าอิเล็กทรอนิกส์หรือที่เราเรียกว่า E-Commerce (Electronics Commerce) ซึ่งส่งผลให้รูปแบบการค้า การติดต่อสื่อสารระหว่างธุรกิจ การทำธุรกรรมทางการค้าเปลี่ยนโฉมหน้าไปมาก ระบบเครือข่ายอินเตอร์เน็ตกลายเป็นเครื่องมือในด้านการตลาดที่มีความรวดเร็วในการตอบสนองความต้องการของลูกค้า สามารถเพิ่มช่องทางการจำหน่ายสินค้าให้เข้าสู่ผู้บริโภคได้อย่างรวดเร็ว กว้างขวาง ทั่วโลก และสามารถให้บริการได้ตลอดเวลา

---

[39] ตัณ ตัณฑ์สุทธิวงศ์, รอบรู้ Internet และ World Wide Web (กรุงเทพมหานคร: โปรวิชั่น, 2539), หน้า 21.

[40] ชวลิต อัตถศาสตร์และคณะ, Cyberlaw กฎหมายกับอินเตอร์เน็ต (กรุงเทพมหานคร: บริษัทโปรวิชั่น จำกัด, 2544), หน้า 128-129.

24 ชั่วโมง ทุกวัน และยังเป็นการลดต้นทุนการทำธุรกิจ เช่น ด้านการขายและการตลาด บริษัทไม่จำเป็นต้องจ้างพนักงานขายหรือพนักงานบริการลูกค้าเป็นจำนวนมาก ทำให้ผู้ที่ต้องการซื้อสินค้าไม่จำเป็นต้องเดินที่ไปที่ร้านค้าแล้ว ไม่ว่าผู้บริโภคจะอยู่ที่ใดก็ตามในโลกก็สามารถจับจ่ายใช้สอยได้ และมีสินค้าให้เลือกซื้อมากมายจากทั่วทุกมุมโลก ประหยัดเวลา ไม่ต้องเดินทางและสามารถหาซื้อของได้ตลอด 24 ชั่วโมง ซึ่งในปัจจุบันนี้ประเทศไทยมีเว็บไซต์ที่ให้บริการซื้อขายสินค้าออนไลน์หลายเว็บไซต์ เช่น www.thaisecondhand.com, www.thai4thai.com, www.siamplaza.com เป็นต้น

จากข้อดีของการค้าอิเล็กทรอนิกส์ทำให้มีอาชญากรนำมาประกอบอาชญากรรมโดยการโฆษณาขายสินค้าทางเว็บไซต์ ซึ่งจะเป็นขายสินค้าที่กำลังเป็นที่ได้รับความนิยมและขายในราคาถูก ทำให้ผู้ซื้อที่อยากได้สินค้าในราคาถูกตัดสินใจซื้อและจ่ายเงินก่อนที่จะได้รับสินค้า ซึ่งเมื่อได้รับสินค้าแล้วปรากฏว่าสินค้านั้นไม่ตรงตามที่โฆษณาไว้หรืออาจจะไม่ได้รับสินค้าดังกล่าวเลย หรืออาจเป็นการหลอกขายสินค้าโดยโฆษณาสรรพคุณเกินความเป็นจริง เช่น การหลอกลวงขายยามหัศจรรย์ ที่ผู้หลอกลวงอ้างว่าสามารถรักษาโรคหรืออาการเจ็บป่วยโรคร้ายแรง เช่น โรคมะเร็ง โรคภูมิคุ้มกันบกพร่อง โรคความดันโลหิตสูง ฯลฯ หรือสามารถบรรเทาความเจ็บป่วยได้ภายในระยะเวลาอันสั้น และมักอ้างว่ายาเหล่านี้ได้รับการรับรองหรือการพิสูจน์ทางวิทยาศาสตร์แล้ว ซึ่งในความเป็นจริงแล้วยาดังกล่าวไม่สามารถรักษาได้ตามสรรพคุณที่ผู้หลอกลวงอ้าง ดังนั้นผู้ซื้อจะต้องสูญเสียเงินไปอย่างเปล่าประโยชน์

สำนักงานข่าวเอเอฟพีรายงานว่าที่ประเทศฮ่องกงได้มีการตัดสินลงโทษผู้ต้องหาสองคน จำคุก 3 ปี 4 เดือน เนื่องจากดำเนินการฉ้อฉลผ่านสื่ออิเล็กทรอนิกส์ ซึ่งทำให้ผู้ต้องหาทั้งสองคนได้เงินจากการฉ้อโกงไปเป็นมูลค่า 1 ล้านดอลลาร์สหรัฐ โดยผู้ต้องหาทั้งสองได้ตั้งบริษัทธุรกิจขึ้น 6 แห่งบนเกาะฮ่องกง พร้อมกับดำเนินการชักจูงให้บรรดานักการค้าร่วมทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ ระหว่างเดือนกุมภาพันธ์ พ.ศ. 2541 ถึงเดือนสิงหาคม พ.ศ. 2544 โดยเสนอขายสินค้าราคาถูกหรือมีบริการสมนาคุณที่น่าสนใจ เพื่อล่อลวงบริษัทคู่ค้าให้จองสินค้าของพวกเขา ปรากฏว่ามีบริษัทธุรกิจ 32 บริษัทจากหลายประเทศทั่วโลกได้ทำธุรกกรรมเพื่อสั่งจองสินค้า แต่ก็ไม่มีการจัดส่งสินค้าให้หลังจากที่ได้สั่งจองแล้ว ทั้งนี้ ผู้ต้องหาในคดีฉ้อฉล

ผ่านระบบอินเตอร์เน็ตดังกล่าวถูกเจ้าหน้าที่ของสำนักงานปราบปรามอาชญากรรมเศรษฐกิจของประเทศฮ่องกงจับกุมตัวได้เมื่อเดือนสิงหาคม พ.ศ.2544[41]

6. การหลอกลวงเกี่ยวกับการใช้บริการอินเตอร์เน็ต (Internet Access Service)

เป็นการหลอกลวงว่าให้ใช้บริการต่าง ๆ ในอินเตอร์เน็ต อันทำให้ผู้ใช้บริการอินเตอร์เน็ตเข้าใจผิดในสาระสำคัญของเงื่อนไขของสัญญา ทำให้หลงเชื่อตกลงตามสัญญาดังกล่าว ซึ่งการหลอกลวงทางด้านการให้บริการทางอินเตอร์เน็ตมีหลายรูปแบบ เช่น กรณีโฆษณาขายเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ในราคาถูกเพียง 199 ดอลลาร์สหรัฐ หรือว่าให้เครื่องคอมพิวเตอร์ฟรี โดยผู้ซื้อจะต้องสมัครเป็นสมาชิกกับบริษัทผู้ให้บริการอินเตอร์เน็ต (ISP) ด้วยการชำระค่าบริการรายเดือน 20-30 ดอลลาร์สหรัฐ ซึ่งกำหนดให้ทำสัญญาสามปีขึ้นไป (แม้จะเป็นเงินจำนวนเพียงเล็กน้อย แต่เมื่อคิดระยะเวลาสามปีแล้วจะเป็นเงินถึงพันดอลลาร์สหรัฐ) สิ่งที่ผู้ซื้อพึงต้องระวังคือเทคโนโลยีระบบเครือข่ายอินเตอร์เน็ตเป็นสิ่งที่มีเสรีภาพมาก ดังนั้นเป็นไปได้ที่ภายในระยะเวลาสามปีบริษัทผู้ให้บริการดังกล่าวอาจจะปิดบริการไปวันใดวันหนึ่งหรือว่าการใช้บริการช้ามาก หากผู้ซื้อต้องการจะยกเลิกสัญญาก็จะต้องจ่ายเงินค่าธรรมเนียมการยกเลิกก่อนเวลาที่กำหนดในสัญญาเป็นจำนวนเงิน 50 ดอลลาร์สหรัฐ ทำให้ผู้ซื้อต้องทนใช้บริการอินเตอร์เน็ตที่ไม่มีคุณภาพต่อไปโดยที่ไม่มีทางเลือก[42] หรือการสมัครเป็นสมาชิกกับบริษัทผู้ให้บริการอินเตอร์เน็ตดังกล่าว ทำให้ต้องต่อโทรศัพท์ทางไกลในการเข้าใช้บริการ ซึ่งบริษัทดังกล่าวจะเสนอบริการโทรผ่านระบบ 800 888 หรือ 877 (toll-free) แทนที่จะต้องเสียเงินค่าโทรศัพท์ทางไกล แต่ต้องเสียค่าธรรมเนียมชั่วโมงละ 5-6 ดอลลาร์สหรัฐ

หรือกรณีหลอกลวงว่ามีการให้บริการบนอินเตอร์เน็ต เช่น การให้พื้นที่ในการเปิดเว็บเพจเป็นเวลา 30 วัน เพื่อประกอบธุรกิจเล็ก ๆ บนโลกอินเตอร์เน็ต โดยไม่เสียค่าใช้จ่าย และหากสนใจจะต่อใช้บริการก็จะเสียเงินค่าธรรมเนียมเพียง 25-30 ดอลลาร์สหรัฐต่อเดือน และสามารถยกเลิกการใช้บริการเมื่อไรก็ได้ ซึ่งในความเป็นจริงแล้วเมื่อครบกำหนดระยะเวลา 30 วัน หากผู้ใช้บริการไม่ยกเลิกบริการดังกล่าวจะถือว่าผู้ใช้บริการต่อสัญญาการใช้พื้นที่ดังกล่าว

---

[41] FTC, "Free" and "Low Cost" PC. Offers go figure [Online]. Available from: htpp://www.police.go.th/policenews/show.php?news_id=42&cat=CRC1&id=33. [2002,June 25]

[42] FTC, Website Woes:Avoiding Web Service Scams [Online]. Available from: http:// www.ftc.gov/bcp/conline/pubs/alerts/pcalrt.htm. [2002,May 2]

โดยอัตโนมัติ โดยไม่มีการถามก่อนว่าผู้ใช้บริการจะต่อสัญญาการใช้หรือไม่ หรือแม้กรณีผู้ใช้บริการอินเตอร์เน็ตตกลงเช่าพื้นที่ดังกล่าวเพื่อประกอบธุรกิจ โดยผู้ให้บริการจะมีการสอบถามถึงรายละเอียดเกี่ยวกับการประกอบธุรกิจของผู้ใช้บริการนั้น โดยอ้างว่าจะนำไปขึ้นเว็บไซต์ให้ก็ตาม แต่ความเป็นจริงแล้วจะเป็นการขึ้นข้อมูลที่ไม่ตรงกับความเป็นจริง หรือว่าไม่ได้มีการนำเอาข้อมูลเว็บไซต์ของผู้ถูกหลอกลวงไปบันทึกไว้ในเว็บไซต์ค้นหาข้อมูล (Search Engine) แม้จะมีเว็บไซต์จริงแต่หากว่าผู้เข้าใช้บริการอินเตอร์เน็ตไม่สามารถเข้าชมเว็บไซต์ดังกล่าวได้ก็ไม่เกิดประโยชน์อะไรกับธุรกิจดังกล่าว [43]

7. การหลอกลวงเกี่ยวกับการหางาน (Job Scams)

การหลอกลวงประเภทนี้เป็นการหลอกลวงโดยการโฆษณาทางระบบเครือข่ายอินเตอร์เน็ตว่าจะช่วยให้คุณได้ทำงานที่ได้รับค่าตอบแทนที่สูงหรือเป็นงานที่มั่นคง เช่น งานในหน่วยงานของรัฐหรือจะได้ทำงานในพื้นที่ที่ผู้ถูกหลอกลวงอาศัยอยู่ ซึ่งมีเงินเดือนสูงและสวัสดิการดี โดยจะต้องจ่ายเงินค่าธรรมเนียมในการหางานให้ หรือผู้หลอกลวงอาจจะเปิดเว็บไซต์ที่เกี่ยวกับการหางานโดยการจัดอบรมสัมมนา ผู้เข้าร่วมสัมมนาจะต้องจ่ายเงินในการเข้าร่วมสัมมนา 45-80 ดอลลาร์สหรัฐ เป็นค่าใบสมัครและค่าอบรมในการทดสอบเพื่อได้เข้าทำงาน ซึ่งผู้หลอกลวงจะรับประกันว่าผู้ที่เข้ารับการอบรมหลักสูตรดังกล่าวจะสามารถได้งานตามที่ผู้เข้ารับการอบรมอยากจะได้อย่างแน่นอน เมื่อผู้ถูกหลอกลวงชำระเงินค่าธรรมเนียมในการหางานหรือในการฝึกอบรมแล้ว ก็จะไม่ได้เข้าทำงานในหน่วยงานของรัฐหรือบริษัทที่ผู้หลอกลวงกล่าวอ้างแต่อย่างใด ซึ่งในความเป็นจริงแล้วการได้รับข้อมูลเกี่ยวกับการทำงานในองค์กรของรัฐหรือใบสมัครงานผู้สมัครงานสามารถหาได้เอง โดยไม่เสียค่าใช้จ่ายและไม่มีหน่วยงานใดที่สามารถจะรับรองได้ว่าผู้สมัครงานจะได้ทำงานในองค์กรของรัฐได้อย่างแน่นอน [44]

การหลอกลวงดังกล่าวปรากฏให้เห็นมากมาย ซึ่งศาลสหรัฐอเมริกาได้ตัดสินคดีเกี่ยวกับการหลอกลวงประเภทดังกล่าวแล้วหลายคดี เช่น คดีที่บริษัท Indiana-based operation หลอกลวงว่าสามารถหางานใน U.S.Postal Service ได้ โดยผู้สมัครจะต้องเสียค่าธรรมเนียมล่วงหน้า ศาลได้ตัดสินห้ามมิให้จำเลยกระทำการเกี่ยวข้องกับการโฆษณาหางานตลอดชีพ

---

[43] FTC, Website Woes : Avoiding Web Service Scams [Online]. Available from: htpp:// www. ftc.gov/bcp/conline/pubs/alerts/webalrt.htm. [2002, June 16]

[44] FTC, FTC Continues to "Stamp Out" Job Fraud [Online]. Available from: htpp://www. ftc.gov/opa/2001/03/stampout2001.htm. [2002, April 8]

และริบทรัพย์จำเลยทั้งสิ้น 28 ล้านดอลลาร์สหรัฐ หรือคดีบริษัท Federal Data Service (FDS) ได้กระทำการหลอกลวงผู้สมัครงานว่าสามารถหางานประจำได้ในองค์กรของรัฐ ซึ่งศาลได้ตัดสินริบทรัพย์ของจำเลยเป็นเงิน 800,000 ดอลลาร์สหรัฐ และห้ามประกอบอาชีพเกี่ยวกับการบริการหางานอีกต่อไป แต่มีข้อยกเว้นว่าหากจะกลับมาประกอบธุรกิจอย่างเดิมจะต้องวางหลักทรัพย์ค้ำประกันจำนวน 100,000 ดอลลาร์สหรัฐก่อน หรือคดีที่เพิ่งตัดสินไปเมื่อเดือนเมษายน ค.ศ.2001 บริษัท Carrer Network (CNI) ตั้งอยู่ที่มลรัฐอินเดียน่า ได้ดำเนินการหลอกลวงเกี่ยวกับหางาน ซึ่งศาลได้ตัดสินห้ามจำเลยประกอบธุรกิจเกี่ยวกับการหางานดังกล่าวอีก และปรับเป็นเงิน 25,000 ดอลลาร์สหรัฐ [45]

8. การหลอกลวงโดยการโอนเงินจากประเทศไนจีเรีย (Nigerian Money Offers)*

การหลอกลวงดังกล่าวเป็นที่รู้จักกันอย่างดีทั่วโลกหรือที่รู้จักกันในนามของการฉ้อโกง 419 (มาจากมาตราในประมวลกฎหมายอาญาของประเทศไนจีเรียซึ่งบัญญัติเกี่ยวกับความผิดฐานการฉ้อโกง)[46] การหลอกลวงดังกล่าวถือกำเนิดขึ้นตั้งแต่ปี คศ. 1980 โดยเริ่มต้นด้วยรูปแบบการส่งจดหมายธรรมดา จนในปัจจุบันได้วิวัฒนาการจนเป็นทางโทรศัพท์และทางระบบเครือข่ายอินเตอร์เน็ตแล้ว โดยการหลอกลวงประเภทนี้จะเป็นการเสนอให้เงินจากประเทศไนจีเรียหรือประเทศอื่นในทวีปแอฟริกา ซึ่งผู้ใช้บริการอินเตอร์เน็ตจะได้รับข้อความเชิญชวนทางจดหมายอิเล็กทรอนิกส์ (e-mail) จากบุคคลที่กล่าวอ้างว่ามีความสำคัญในประเทศไนจีเรียหรือผู้จัดการธนาคารในแอฟริกา เพื่อขอความช่วยเหลือในการโอนเงินจำนวนมากเพชร หรือสิ่งของมีค่าต่าง ๆ ไปยังต่างประเทศ เนื่องจากตัวเองไม่สามารถโอนเงินดังกล่าวได้ โดยผู้ถูกหลอกลวงจะได้รับเงินส่วนแบ่งจำนวนนับล้านเหรียญสหรัฐจากการให้ความช่วยเหลือในการโอนดังกล่าว ซึ่งในบางครั้งจะมีการเชิญชวนผู้ถูกหลอกลวงไปพบปะกันที่ประเทศไนจีเรียก่อนมีการโอนเงินก็ได้ เพื่อให้ผู้ถูกหลอกลวงหลงเชื่อโดยอ้างว่าสถานที่จะนัดเจอกันเป็นสถานที่

---

[45] FTC,Indiana Company Agress to Settle Charge of Misrepresenting Availability of U.S.? Postal Service and Government Jobs [Online]. Available from: http://www. ftc.gov/opa/2201/11/ careernetwork .htm. [2002, July 20]

* ตัวอย่างของการหลอกลวงประเภทนี้ ดูได้ในภาคผนวก ก.

[46] FBI, Nigerian Letter Scams [Online]. Available from: http://www.lfccfbi.gov/strategy/ nls.asp [2002, October 30]

สำคัญของประเทศ ทำให้ผู้ถูกหลอกลวงหลงเชื่อว่าคำพูดที่ผู้หลอกลวงกล่าวอ้างเป็นความจริง และเชื่อมั่นว่าตนเองจะได้รับผลประโยชน์ตอบแทนจำนวนมหาศาล เมื่อผู้ถูกหลอกลวงแจ้งข้อมูลเกี่ยวกับบัญชีเงินฝากของตนให้กับผู้หลอกลวงแล้ว ผู้หลอกลวงจะอ้างว่าการโอนเงินเข้าบัญชีผู้ถูกหลอกลวงได้ ผู้ถูกหลอกลวงจะต้องเสียเงินค่าธรรมเนียมหรือค่าใช้จ่ายในการดำเนินการต่าง ๆ เอง โดยให้ผู้ถูกหลอกลวงโอนเงินเข้าบัญชีผู้หลอกลวง เมื่อผู้หลอกลวงเบิกเงินจากบัญชีดังกล่าวไปแล้วก็ไม่มีการโอนเงินหรือสิ่งของมีค่าเข้ามายังบัญชีของผู้ถูกหลอกลวงแต่อย่างใด

หน่วยรับร้องเรียนการหลอกลวงทางอินเตอร์เน็ตของ FBI ประเทศสหรัฐอเมริกา (The Internet Fraud Complaint Center : IFCC) แจ้งว่าได้รับการร้องเรียนเกี่ยวกับการหลอกลวงดังกล่าวมากถึง 600 ฉบับ นับตั้งแต่หน่วยงานนี้เริ่มก่อตั้งขึ้นเมื่อเดือนเมษายน ปี คศ. 2000 จนถึงเดือนสิงหาคม 2001 ซึ่งในจำนวนผู้ร้องเรียนดังกล่าวมีเพียงสองคนเท่านั้นที่แจ้งว่าตัวเองได้เสียเงินไปแล้วเป็นจำนวนเงินถึง 31,000 ดอลลาร์สหรัฐอเมริกา และอีกรายหนึ่งเป็นเงิน 1,000 ดอลลาร์สหรัฐ หรือสมาคมคุ้มครองผู้บริโภค (The National Consumers League) ซึ่งเป็นหน่วยงานเอกชนได้รับแจ้งเกี่ยวกับอาชญากรรมประเภทนี้เพิ่มขึ้น 900 เปอร์เซ็นต์ จากปี ค.ศ.2000 ถึงปี ค.ศ. 2001 [47]

9. การหลอกลวงเกี่ยวกับการได้รับรางวัล (Prizes and Sweepstakes)

การหลอกลวงประเภทนี้ผู้ถูกหลอกลวงจะได้รับจดหมายอิเล็กทรอนิกส์ว่าได้รับรางวัลจากการชิงโชครางวัลใหญ่ เช่น ข้อความที่ว่า Prize Offers : You Don't' Have to Pay to Play! หรือข้อความในทำนองที่ว่า "Congratulations, it's your lucky day! You've just won $5,000! You're guaranteed to win a fabulous diamond ring, luxury vacation or all-terrain vehicle!" โดยจะมีเนื้อความว่าคุณเป็นผู้โชคดีได้รับรางวัล ซึ่งส่วนมากจะเป็นโทรศัพท์มือถือ หรือรถยนต์ ของมีค่าจำพวกเครื่องประดับต่าง ๆ โดยผู้ได้รับรางวัลจะต้องจ่ายเงินค่าธรรมเนียมเล็กน้อยล่วงหน้าก่อนที่จะได้รับรางวัลเป็นค่าขนส่ง ค่าภาษี เมื่อผู้ถูกหลอกลวงหลงเชื่อและชำระค่าธรรมเนียมดังกล่าวไปแล้วจะพบว่ารางวัลที่ได้รับไม่เหมือนกับที่ผู้หลอกลวงกล่าวอ้างไว้ ซึ่งเมื่อเปรียบเทียบจำนวนเงินที่เราจะจ่ายไปนั้นกับมูลค่ารางวัลที่ได้รับจะพบว่าเงินที่ผู้ถูกหลอกลวงเสียไปจะมีราคาแพงกว่ามูลค่ารางวัลที่ได้รับจริงหรือผู้ถูกหลอกลวงอาจจะไม่ได้รับรางวัลเลยก็ได้

---

[47] Internet Fraud Lurks in Your Inbox [Online]. Available from:http://www. nclnet .org/ emailscamspr02.htm. [2002, September 30]

โดยส่วนใหญ่การแจกรางวัลเป็นการกระทำที่ถูกต้องตามกฎหมายของประเทศสหรัฐอเมริกา ดังจะเห็นได้จากผลการสำรวจพบว่ามากกว่าครึ่งหนึ่งของประชากรสหรัฐอเมริกาได้รับจดหมายเกี่ยวกับการได้รับรางวัลที่ถูกกฎหมาย ซึ่งถือว่าเป็นกลไกทางการตลาดอย่างหนึ่งของบริษัทผู้ขายสินค้า แต่ก็มีบุคคลจำนวนมากที่ถูกหลอกลวงและไม่ได้รับรางวัลตามที่กล่าวอ้าง ซึ่งสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) ได้รับแจ้งมากกว่า 10,000 ครั้ง สำหรับการหลอกลวงประเภทนี้ ซึ่งในความเป็นจริงแล้วการที่จะได้รับรางวัลต่าง ๆ บุคคลนั้นไม่จำต้องเสียค่าใช้จ่ายในการขนส่งสินค้าแต่อย่างใด หรือหากจะต้องเสียค่าภาษีก็จะต้องชำระเมื่อได้รับสินค้าแล้ว จะไม่มีการให้จ่ายเงินล่วงหน้าก่อนได้รับรางวัลจริง เช่น คดีที่ศาลมลรัฐแมรีแลนด์ได้ ตัดสินคดีระหว่าง FTC กับ Deborah C. Taylor ให้จ่ายเงินชดเชยจำนวน 1.25 ล้านดอลลาร์สหรัฐ ให้แก่ผู้เสียหายและยังห้ามจำเลยประกอบอาชีพเกี่ยวกับการแจกรางวัลดังกล่าวอีกด้วย [48]

10. การหลอกลวงเกี่ยวกับทุนการศึกษา (Scholarship Scams)

เมื่อมีการเปิดภาคเรียนการศึกษาในปีหนึ่ง ๆ จะมีเด็กนักเรียนและผู้ปกครองจำนวนไม่น้อยที่ไม่สามารถจ่ายเงินค่าเทอมในมหาวิทยาลัยหรือโรงเรียนได้ ประกอบกับการขึ้นค่าเทอมการศึกษาที่เพิ่มมากถึง 600 เปอร์เซ็นต์ ตั้งแต่ปี ค.ศ.1969 จนถึงปัจจุบันนี้ (ข้อมูลจากประเทศสหรัฐอเมริกา)[49] จึงมีความจำเป็นที่นักเรียนหรือผู้ปกครองจะต้องหาทุนการศึกษา ซึ่งผู้หลอกลวงจะกล่าวอ้างผ่านทางจดหมายอิเล็กทรอนิกส์หรือเปิดเว็บไซต์หลอกลวงว่าสามารถหาทุนการศึกษาให้ได้ตามที่ต้องการ เช่น "The scholarship is guaranteed or your money back" หรือ "You've been selected by a national foundation to receive a scholarship or You're a finalist in a contest you never entered" โดยการจะได้รับทุนการศึกษาดังกล่าวผู้ถูกหลอกลวงจะต้องเสียเงินค่าธรรมเนียมในการดำเนินการค่าธรรมเนียมดังกล่าวมีราคาตั้งแต่ 10-400 ดอลลาร์สหรัฐ แม้ว่าเงินจำนวนดังกล่าวจะเป็นเงินเพียงเล็กน้อยแต่เมื่อคูณกับจำนวนผู้เสียหายที่ปีหนึ่งมีจำนวนเป็นหมื่นคนแล้ว สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐได้

---

[48] FTC, Ftc Settlement in Massive sweepstakes – entry scam to net $1.25 million for consumer redress [Online]. Available from: http://www.ftc.gov/opa/1996/9602/scam.htm. [2002, August 31]

[49] FTC, Federal Agencies Release First Annual Report to Congress on College Scholarship Fraud [Online]. Available from : http://www.ftc.gov/opa/2002/05/ scholarshipfraud.htm. [2002, December 15]

แจ้งว่ามีมูลค่าความเสียหายมากถึง 10 ล้านดอลลาร์สหรัฐต่อปี[50] เมื่อผู้ถูกหลอกลวงจ่ายเงินค่าธรรมเนียมไปแล้วก็จะไม่ได้รับการตอบกลับจากทุนที่ตนเองสมัครแต่อย่างใด การหลอกลวงประเภทนี้บางครั้งทุนต่างๆ ที่ผู้หลอกลวงแนะนำนั้นเป็นทุนซึ่งผู้ถูกหลอกลวงไม่มีทางได้รับทุนการศึกษาอย่างแน่นอน เช่น ทุนที่ปิดรับสมัครไปแล้ว หรือว่ามีคุณสมบัติไม่ตรงตามที่ทุนกำหนด ซึ่งในความเป็นจริงแล้วการจะได้รับทุนการศึกษาหรือไม่ ต้องดูตามคุณสมบัติของผู้สมัครว่าตรงตามที่ทุนนั้นกำหนดหรือไม่ ซึ่งข้อมูลต่าง ๆ เหล่านี้ผู้สมัครสามารถหาได้ทั่วไป โดยไม่เสียค่าใช้จ่ายแต่อย่างใด ซึ่งผู้ที่ต้องการได้รับทุนจะต้องจัดการทำทุกอย่างด้วยตัวเอง ตั้งแต่การเขียนเรียงความ (Assay) จนถึงขั้นตอนการขอสมัครรับทุน และไม่มีทางเป็นไปได้ที่จะมีใครมารับประกันได้ว่าผู้สมัครจะได้รับทุนตามที่ต้องการอย่างแน่นอน

การปราบปรามการหลอกลวงดังกล่าวสภาครองเกรสของสหรัฐได้ออกพระราชบัญญัติการป้องกันการหลอกลวงเกี่ยวกับการให้ทุนการศึกษา (College Scholarship Fraud Prevention Act) ในปี ค.ศ. 2000 ซึ่งเป็นความร่วมมือระหว่างสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (FTC) กระทรวงศึกษา (Department of Education) และกระทรวงยุติธรรม (Department of Justice) ในการป้องกันและปราบปรามอาชญากรรมดังกล่าว ซึ่งศาลสหรัฐอเมริกาได้ตัดสินผู้กระทำความผิดเกี่ยวกับการหลอกลวงประเภทนี้ไว้แล้วหลายคดี เช่น บริษัท Career Assistance Planning ตั้งอยู่ที่มลรัฐจอร์เจีย ซึ่งให้บริการหลอกลวงเกี่ยวกับแนะนำให้คำปรึกษาเกี่ยวกับการได้รับทุนการศึกษา คดีนี้มีผู้เสียหายถึง 30,000 คน มูลค่าความเสียหาย 6 ล้านดอลลาร์สหรัฐ ซึ่งศาลได้สั่งให้ผู้กระทำความผิด (David Chaim Levy และ Donna M. Levy) ต้องจ่ายเงินจำนวน 6 ล้านดอลลาร์สหรัฐ เพื่อชดเชยแก่ผู้เสียหาย และถูกสั่งห้ามประกอบธุรกิจดังกล่าว เว้นแต่จะจ่ายเงิน 6 ล้านเหรียญดอลลาร์สหรัฐเพื่อเป็นค่าประกันความเสียหายก่อนจึงจะสามารถประกอบธุรกิจดังกล่าว หรือคดีบริษัท College Assistance Service ตั้งอยู่ที่มลรัฐฟลอริด้า ได้กระทำการหลอกลวงว่าจะสามารถหาทุนการศึกษาให้ ปรากฏว่าภายในเวลาเพียงแค่ 6 เดือน มีผู้ถูกหลอกลวงถึง 6,000 คน มูลค่า

---

[50] FTC, FTC Cautions : Do Your Own Homework to Avoid Scholarship Service Rip-Offs [Online]. Available from: http://www.ftc.gov/opa/1996/9609/scholar.htm. [2002, June 16.]

ความเสียหายถึง 1 ล้านดอลลาร์สหรัฐ ซึ่งศาลได้ตัดสินห้ามจำเลย (Linda Love, Conni Canella, Randolph Cannella และ John Giuffrida) ประกอบอาชีพเกี่ยวกับบริการหาทุนการศึกษาดังกล่าวอีก เว้นแต่จะจ่ายเงินประกันความเสียหายจำนวน 200,000 ดอลลาร์สหรัฐก่อนเข้ากลับมาประกอบธุรกิจดังกล่าวอีก[51]

11. การหลอกลวงเกี่ยวกับการประกอบธุรกิจที่บ้าน (Work at Home Scams)

การหลอกลวงประเภทนี้ผู้หลอกลวงจะอ้างว่าเป็นการประกอบธุรกิจที่บ้าน โดยใช้เวลาทำงานเพียงวันละไม่กี่ชั่วโมง สำหรับผลประโยชน์ตอบแทนที่จะได้รับเป็นเงินจำนวนมาก ซึ่งผู้ถูกหลอกลวงจะต้องเสียเงินค่าอุปกรณ์เพื่อใช้ในการประกอบธุรกิจดังกล่าวหรือค่าสอนวิธีการในการประกอบธุรกิจดังกล่าว ซึ่งมีราคาตั้งแต่ 35 ดอลลาร์สหรัฐ ถึง 100 ดอลลาร์สหรัฐ [52] เมื่อผู้ถูกหลอกลวงจ่ายเงินไปแล้วก็ไม่ได้รับอุปกรณ์ในการประกอบธุรกิจดังกล่าวแต่อย่างใด หรือจะไม่ได้รับโอกาสในการประกอบธุรกิจที่บ้านตามที่ผู้หลอกลวงกล่าวอ้าง เช่น คดีที่มลรัฐ Los Angeles จำเลยสี่คนถูกฟ้องอาญาต่อศาล Central District of California เมื่อเดือนพฤศจิกายน ค.ศ.1999 เนื่องจากกระทำการหลอกลวงด้วยการส่งจดหมายอิเล็กทรอนิกส์ประมาณ 50 ล้านฉบับ ว่าให้ประกอบธุรกิจที่บ้าน โดยเรียกเก็บค่าอุปกรณ์ในการทำธุรกิจที่บ้านคนละ 35 ดอลลาร์สหรัฐ

12. การหลอกลวงเกี่ยวกับการสมัครบัตรเครดิต (Bogus Credit Card Offers)

การหลอกลวงประเภทนี้ผู้หลอกลวงจะอ้างว่าผู้ถูกหลอกลวงสามารถจะได้รับการพิจารณาอนุมัติบัตรเครดิตได้อย่างง่ายดาย แม้ว่าผู้นั้นจะมีฐานะการเงินที่ไม่ค่อยดีหรือว่ามีคุณสมบัติไม่ครบตามหลักเกณฑ์ที่ธนาคารหรือบริษัทผู้ให้บริการบัตรเครดิตกำหนดไว้ โดยจะต้องเสียค่าธรรมเนียมในการทำบัตรเครดิตเพียงเล็กน้อยเท่านั้น แต่ในความเป็นจริงแล้วการที่บุคคลใดจะได้รับอนุมัติบัตรเครดิตหรือไม่ ธนาคารหรือผู้ให้บริการบัตรเครดิตจะต้องดูว่าบุคคลนั้นมีฐานะการเงินเป็นอย่างไร มีความน่าเชื่อถือทางการเงินหรือไม่ ดังนั้นจึงเป็นไปไม่ได้ที่ธนาคารหรือบริษัทผู้ให้บริการบัตรเครดิตจะมีการอนุมัติบัตรโดยไม่คำนึงถึงฐานะการเงินของ

---

[51] FTC, Scholarship Scam [Online]. Available from : http://www.ftc.gov/bcp/conline /edcams/scholarship/cases.htm. [2002, June 25]

[52] Internet Fraud [Online]. Available from: http://www.usdoj.gov/criminal /fraud/internet. htm. [2002, June 25]

ผู้ขอใช้บริการบัตรเครดิตตามที่ผู้หลอกลวงกล่าวอ้าง เช่น คดีที่ศาลได้ตัดสินห้ามบริษัทหนึ่งที่ตั้งอยู่ที่ประเทศแคนนาดาซึ่งได้สัญญากับผู้ถูกหลอกลวงว่าสามารถสมัครบัตรเครดิตของ Visa หรือบัตร Master ได้ มีวงเงินใช้จ่ายบัตรเครดิตระหว่าง 2,500 – 5,000 ดอลลาร์สหรัฐ และไม่ต้องเสียค่าธรรมเนียมรายปี ดอกเบี้ยกรณีผิดนัดเพียง 3.9 % เท่านั้น โดยผู้ถูกหลอกลวงจะต้องจ่ายเงินค่าธรรมเนียมในการได้รับอนุมัติบัตรเครดิตในราคา 175-199 ดอลลาร์สหรัฐ แต่ในที่สุดผู้ถูกหลอกลวงก็ไม่ได้รับอนุมัติบัตรเครดิต สำหรับผู้เสียหายในคดีนี้มีแต่ชาวอเมริกันเท่านั้น มูลค่าความเสียหายประมาณ 5 ล้านดอลลาร์สหรัฐ ซึ่งศาลได้สั่งจำเลยห้ามประกอบธุรกิจเกี่ยวกับการสมัครบัตรเครดิตอีก และให้จ่ายเงินชดเชยให้ผู้เสียหาย[53]

13. การหลอกลวงเกี่ยวกับการแก้ไขประวัติทางการเงิน (Credit Repair)

การที่บุคคลใดบุคคลหนึ่งมีความน่าเชื่อถือทางด้านการเงินหรือมีเครดิตเป็นสิ่งที่สำคัญมาก เพราะจะทำให้บุคคลนั้นสามารถจับจ่ายใช้สอยได้โดยไม่ต้องใช้เงินสดหรือจ่ายเงินในทันที ซึ่งการที่บุคคลใดบุคคลหนึ่งจะได้รับสิทธิดังกล่าวธนาคารหรือบริษัทที่ให้บริการบัตรเครดิตจะต้องพิจารณาจากประวัติความน่าเชื่อถือการเงิน แต่ในทางตรงกันข้ามสำหรับคนที่เคยมีประวัติเครดิตที่ไม่ดี อาจจะเนื่องมาจากการชำระเงินไม่ตรงตามกำหนดหรือการปฏิเสธการจ่ายเงิน อันจะทำให้บุคคลนั้นมีประวัติการเงินที่ไม่ดีและสูญเสียความน่าเชื่อถือทางการเงิน ส่งผลให้บุคคลนั้นถูกยกเลิกบัตรเครดิตและไม่ได้รับการอนุมัติบัตรเครดิตในครั้งต่อไปหรือบัตรเครดิตของบริษัทอื่น ๆ ทำให้มีกลุ่มอาชญากรเล็งเห็นถึงช่องทางในการหลอกลวงโดยกล่าวอ้างว่าบุคคลที่มีประวัติการเงินที่ไม่ดีมีโอกาสแก้ไขประวัติทางการเงินดังกล่าวได้ เพื่อที่จะได้รับสิทธิในการสมัครเป็นสมาชิกบัตรเครดิต ผู้หลอกลวงจะกล่าวอ้างว่าตนสามารถแก้ไขประวัติทางการเงินให้ได้ หรือสามารถจะแก้ไขประวัติการเงินที่แย่ให้เป็นประวัติใหม่เหมือนไม่เคยมีประวัติที่แย่ดังกล่าวมาก่อน โดยเปลี่ยนหมายเลขบัตรประชาชน หมายเลขใบขับขี่ หมายเลขผู้เสียภาษี หมายเลขบัตรประกันสังคม และกำหนดรหัสใหม่เป็นข้อมูลใหม่ไปขอสมัครบัตรเครดิตใหม่และจะได้รับอนุมัติบัตรเครดิตในที่สุด เนื่องจากบริษัทเครดิตต่าง ๆ จะไม่พบประวัติที่ไม่ดีของบุคคลนั้นเลย ซึ่งผู้ถูกหลอกลวงจะเสียเงินค่าธรรมเนียมในการลบประวัติดังกล่าวล่วงหน้า ซึ่งในความเป็นจริงบุคคลต่าง ๆ ไม่สามารถแก้ไขข้อมูลทางการเงินที่แย่ให้เป็นประวัติการเงินใหม่ได้ เช่น คดีที่เคยเกิดขึ้นแล้วในประเทศสหรัฐอเมริกา สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐ (Federal Trade Commission : FTC) ได้ฟ้องบริษัท National Credit Management

---

[53] FTC, Cross-Border Credit Card Fraud Halted [Online]. Available from: http://www. ftc.gov/ opa/ 2002/12/fristfederal.htm [2002, June 25]

Group's (NCMG) ที่กล่าวอ้างว่าสามารถลบประวัติทางการเงินที่ไม่น่าเชื่อถือได้ และทำให้บุคคลดังกล่าวได้รับอนุมัติบัตรเครดิตอย่างแน่นอน แต่ต้องเสียธรรมเนียมในการสมัครบัตรเครดิตล่วงหน้าเป็นเงินจำนวน1,000 ดอลลาร์สหรัฐ ซึ่งคดีนี้ศาลได้ตัดสินให้บริษัทดังกล่าวชดใช้ค่าเสียหายเป็นเงินจำนวน 350,000 ดอลลาร์สหรัฐ และสั่งปิดบริษัทดังกล่าวในเดือนเมษายน 1998

14. การหลอกลวงเกี่ยวกับการให้บริการข้อมูลต่าง ๆ (Information/Adult Service)

การหลอกลวงประเภทนี้จะเป็นการให้เข้าไปใช้บริการดาวน์โหลดโปรแกรมหรือบริการต่าง ๆ บนระบบเครือข่ายอินเตอร์เน็ตได้ ไม่ว่าจะเป็นการดูรูปภาพ การเล่นเกมส์ การฟังเพลง หรือว่าทำกิจกรรมอื่น ๆ โดยไม่เสียค่าบริการแต่อย่างใด แต่ต้องระวังว่าการดาวน์โหลด เพราะอาจจะทำให้เครื่องคอมพิวเตอร์มีปัญหาที่คาดไม่ถึง เช่น การติดเชื้อไวรัส การต้องเสียค่าโทรศัพท์ทางไกลต่างประเทศหรือถูกเจาะข้อมูล โดยผู้ใช้บริการจะต้องติดตั้งโปรแกรมคอมพิวเตอร์เพื่อดูภาพดังกล่าวหรือผู้ใช้บริการจะต้องติดตั้งโปรแกรมคอมพิวเตอร์เพื่อดูภาพดังกล่าว หรือเรียกว่าโปรแกรม "viewer" หรือ "dialer" ของผู้ให้บริการ ซึ่งโปรแกรมดังกล่าวจะมีการดัดแปลงให้สามารถเข้าควบคุมโมเด็มของบุคคลอื่นได้ เมื่อผู้ใช้บริการเปิดดูภาพด้วยโปรแกรมข้างต้นแล้ว โปรแกรมจะควบคุมการทำงานของโมเด็มและสั่งให้หยุดการทำงานโดยที่ผู้ใช้บริการไม่รู้ตัว และสั่งให้มีการต่อเชื่อมผ่านโมเด็มอีกครั้งหนึ่ง ซึ่งเป็นการต่อโทรศัพท์ทางไกล ทำให้ผู้ใช้บริการต้องเสียเงินค่าโทรศัพท์ทางไกล มีราคาระหว่าง 2-7 ดอลลาร์สหรัฐต่อนาที ตลอดระยะเวลาที่เข้าใช้บริการดังกล่าวนั้น[54] หรือโปรแกรมดังกล่าวจะเข้าเจาะระบบข้อมูลของผู้ใช้บริการเพื่อทราบรายละเอียดเกี่ยวกับการใช้บริการอินเตอร์เน็ตแล้วนำข้อมูลนั้นไปใช้หรือขายให้กับผู้อื่น ทำให้ผู้ถูกหลอกลวงต้องเสียเงินค่าใช้บริการอินเตอร์เน็ต ทั้ง ๆ ที่ตัวเองไม่ได้ใช้บริการดังกล่าว

---

[54] FTC, When Your Computer Calls Oversea ... Without Your Okay [Online] Available from: www.ftc.gov/bcp/conline/pubs/alerts/modmalrt.htm. [2002, June 30]

15. **การหลอกลวงเกี่ยวกับการลงทุน** (Investment Scams)

การหลอกลวงประเภทนี้ผู้หลอกลวงจะหลอกให้บุคคลต่าง ๆ นำเงินมาลงทุนในธุรกิจ เช่น ลงทุนซื้อหุ้นในตลาดหลักทรัพย์ โดยอ้างว่าไม่ว่าผู้ถูกหลอกลวงจะมีเงินมากหรือว่าเงินน้อย จะได้รับผลตอบแทนมหาศาล และไม่มีความเสี่ยงจากการประกอบธุรกิจนั้นเลย ซึ่งในความเป็นจริงต้องยอมรับว่าการลงทุนทำธุรกิจทุกประเภทย่อมมีความเสี่ยง ถ้าผลตอบแทนน้อยอัตราการเสี่ยงก็น้อย แต่หากผลตอบแทนมากอัตราการเสี่ยงก็ย่อมมากขึ้นเช่นเดียวกัน เมื่อผู้ถูกหลอกลวงหลงเชื่อนำเงินไปลงทุนในธุรกิจดังกล่าวแล้วจะไม่ได้รับผลประโยชน์ตอบแทนจำนวนมากอย่างที่ผู้หลอกลวงบอก รวมทั้งจะสูญเสียเงินต้นที่ลงทุนด้วย เช่น การส่งจดหมายอิเล็กทรอนิกส์ (E- Mail) เกี่ยวข่าวการลงทุนในตลาดหลักทรัพย์ไปให้บุคคลต่าง ๆ โดยให้ข้อมูลคำแนะนำเกี่ยวกับหุ้นในตลาดหลักทรัพย์ที่น่าเชื่อถือในการลงทุน ซึ่งอ้างว่าเมื่อลงทุนในหุ้นดังกล่าวแล้วจะได้รับผลประโยชน์ตอบแทนเป็นจำนวนมาก โดยบริษัทที่เป็นเจ้าของหุ้นดังกล่าวจะจ่ายเงินให้กับบุคคลซึ่งเขียนข่าววิเคราะห์สถานการณ์หุ้นในตลาดหลักทรัพย์ หรือให้เขียนข่าวหลอกลวงโฆษณาว่าหุ้นตัวนี้น่าลงทุน โดยยกเหตุผลต่าง ๆ ประกอบมากมายในการเลือกลงทุนในหุ้นของบริษัทดังกล่าว หรืออาจจะเป็นการกล่าวอ้างข้อมูลที่ไม่ถูกต้องถึงงานวิเคราะห์หุ้น ซึ่งหุ้นที่แนะนำให้ไปลงทุนดังกล่าวจะเป็นหุ้นที่ไม่มีทางได้กำไร ไม่มีผลการประกอบการที่ดีตามที่กล่าวอ้าง เมื่อมีผู้สนใจเข้ามาร่วมซื้อหุ้นดังกล่าวมากส่งผลให้ราคาหุ้นพุ่งสูงขึ้นอย่างรวดเร็ว ซึ่งจะสร้างความเชื่อมั่นให้กับผู้ลงทุนว่าหุ้นตัวนี้มีความมั่นคง ทำให้ผู้ถูกหลอกลวงเพิ่มการลงทุนเข้าไปในหุ้นอีก จนในที่สุดเมื่อหุ้นราคาพุ่งขึ้นสูง เจ้าของบริษัทหรือผู้หลอกลวงจะเทขายหุ้นทั้งหมดที่ตนเองมีอยู่ ทำให้ราคาหุ้นตกลงอย่างรวดเร็วหรือที่เราเรียกว่าการปั่นหุ้นนั่นเอง ส่งผลให้ผู้หลอกลวงได้รับผลกำไรจากการขายหุ้นจำนวนมหาศาล ในขณะที่ผู้ถูกหลอกลวงจะต้องสูญเสียเงินที่นำไปลงทุนดังกล่าว ซึ่งการกระทำความผิดดังกล่าวส่วนใหญ่จะพบทางจดหมายอิเล็กทรอนิกส์และทางกระดานข่าว

เช่น คดีบริษัท Francis A. Tribble and Sloane Fitzgerald ที่ได้ส่งจดหมายอิเล็กทรอนิกส์มากกว่าหกล้านฉบับ สร้างเว็บไซต์หลอกลวง และลงข้อความในกระดานข่าวเป็นเวลานานกว่า 10 เดือน เพื่อโฆษณาหุ้นสองตัวของบริษัท microcap ว่าจะสามารถให้ผลประโยชน์ตอบแทนสูง แต่ในความเป็นจริงแล้วหุ้นดังกล่าวมีการซื้อขายกันน้อยมาก หากผู้ลงทุนนำเงินไปลงจะต้องสูญเสียเงินอย่างแน่นอน ศาลได้ตัดสินให้จำเลยเสียค่าปรับเป็นเงิน 15,000 ดอลลาร์สหรัฐ หรือคดี Charles O. Huttoe และจำเลยอื่นอีก 12 คน ได้ทำการหลอกขายหุ้นของบริษัท Systems of Excellence หรือที่รู้จักกันในนามของ “SEXI” จำนวน

42 ล้านหุ้น ด้วยการร่วมมือกับบริษัท SGA Goldstar ซึ่งเป็นบริษัทให้ข้อมูลเกี่ยวกับตลาดหุ้น โดยการส่งข้อความให้ซื้อหุ้นของบริษัทตนผ่านทางจดหมายอิเล็กทรอนิกส์ หัวข้อ "Whisper Stocks" คดีนี้จำเลยได้ถูกศาลยึดทรัพย์ที่ได้มาจากการกระทำความผิดประมาณ 11 ล้านดอลลาร์สหรัฐ และจำคุกจำเลย[55]

16. การหลอกลวงเกี่ยวกับการสมัครสมาชิกนิตยสาร (Magazine Sales)

การหลอกลวงโดยจะเสนอให้สิทธิพิเศษในการสั่งจองหนังสือหรือการสมัครเป็นสมาชิกกับหนังสือดังกล่าว ไม่ว่าจะเป็นการได้รับส่วนลด การได้ของสมนาคุณพิเศษ แต่ในท้ายที่สุดแล้วหากผู้ถูกหลอกลวงจองหรือสมัครสมาชิกแล้วจะไม่ได้รับหนังสือดังกล่าวเลย หรือเป็นกรณีที่หลอกลวงว่าจะให้สิทธิพิเศษโดยการได้รับหนังสือไปอ่านฟรี แต่ต้องเสียเงินค่าธรรมเนียมในการส่งหนังสือเป็นรายเดือนทุกเดือนเป็นเวลาหลายปีติดต่อกัน ซึ่งผู้ถูกหลอกลวงไม่สามารถเลิกสัญญาส่งหนังสือได้ ทำให้ผู้ถูกหลอกลวงต้องเสียค่าใช้จ่ายในการส่งทุกเดือน ซึ่งเมื่อเทียบกับค่าหนังสือที่ได้รับแล้วพบว่าค่าธรรมเนียมดังกล่าวแพงกว่าราคาหนังสือเสียอีก เช่น บริษัท Dixie Reader's Service ที่ให้บริการหลอกลวงเกี่ยวกับการสมัครสมาชิกนิตยาสารดังกล่าว ศาลได้สั่งให้จำเลยเสียค่าปรับ 55,000 ดอลลาร์สหรัฐ และให้เลิกกิจการดังกล่าวทันที [56]

17. การหลอกลวงเกี่ยวกับการประมูลสินค้าออนไลน์ (Online Auctions)

ในปัจจุบันการประมูลสินค้าออนไลน์กำลังเป็นที่นิยมมากสำหรับผู้ที่ต้องการจับจ่ายใช้สอยสินค้าราคาถูก สำหรับการประมูลสินค้าออนไลน์เริ่มต้นมีครั้งแรกเมื่อปี ค.ศ. 1995 ซึ่งในปัจจุบันมีเว็บไซต์ที่เปิดให้บริการเกี่ยวกับการประมูลสินค้าออนไลน์จำนวนมากมาย ซึ่งเว็บไซต์ที่กำลังเป็นที่นิยม คือ www.ebay.com เว็บไซต์ดังกล่าวมีผู้ซื้อและผู้ขายที่ใช้บริการของเว็บไซต์ดังกล่าวถึง 3.8 ล้านราย มีสินค้ามากกว่า 2 ล้านชิ้น มีรายได้ของบริษัทรวมถึง 47.1 ล้านดอลลาร์สหรัฐ หรือ www.amazon.com ซึ่งมีชื่อเสียงเริ่มต้นจากการขายหนังสือ

---

[55] Internet Fraud:How to avoid Internet Investment Scams [Online]. Available from: http://www.sec.gov/investor/pubs/cyberfraud.htm. [2002, August 30]

[56] FTC, FTC Recovers $55,000 from magazine – sales firm for failing to give prompt refunds [Online]. Available from:http://www.ftc.gov/opa/predawn/F85/dixie.htm. [2002, December 31]

ในประเทศไทยก็มีเว็บไซต์เกี่ยวกับการประมูลสินค้าออนไลน์มากมายเช่นเดียวกัน เช่น www.pramol.com ซึ่งเริ่มเปิดให้บริการตั้งแต่ราวกลางปี พ.ศ. 2542 หรือ www.auction.thaicentral.com เป็นต้น [57]

สำหรับขั้นตอนและวิธีการทั่วไปของการซื้อสินค้าด้วยประมูลสินค้านั้น เริ่มจากผู้ที่ต้องการจะซื้อหรือขายสินค้าต้องสมัครเป็นสมาชิกของเว็บไซต์นั้น ๆ ก่อน โดยไม่ต้องจ่ายเงินค่าสมัครแต่จะต้องกรอกรายละเอียดของตน เช่น ชื่อ ที่อยู่ อีเมล์แอดเดรสและสถานที่รับส่งสินค้า และเมื่อสมัครแล้วสมาชิกจะได้รหัสผ่าน (password) เพื่อนำไปใช้ในการประมูลหรือขายสินค้าบนระบบเครือข่ายอินเตอร์เน็ต การประกาศขายสินค้าบนระบบเครือข่ายอินเตอร์เน็ตทำโดยผู้ขายจะระบุข้อมูลรายละเอียดของสินค้าที่จะขาย ให้ผู้ซื้อพิจารณาและให้เข้าใจว่าสินค้ามีลักษณะและคุณภาพเป็นอย่างไร โดยอาจจะต้องระบุถึงสภาพของสินค้าว่าเป็นสินค้าใหม่หรือสินค้าที่ใช้แล้ว อายุของสินค้ามีประกันหรือไม่ ถ้ามีอายุของการประกันเหลือเท่าไร ฯลฯ ซึ่งผู้ขายอาจมีภาพตัวอย่างของสินค้าประกอบด้วย นอกจากนี้ผู้ขายจะต้องระบุจำนวนเงินขั้นต่ำที่จะเปิดประมูลพร้อมทั้งวิธีการชำระเงินค่าสินค้า เมื่อผู้ซื้อสนใจจะซื้อสินค้าก็ต้องเสนอราคาที่จะซื้อสินค้าภายในกำหนดระยะเวลาที่ผู้ขายกำหนดไว้ โดยเมื่อสิ้นระยะเวลาที่ประกาศไว้ผู้ซื้อที่เสนอราคาสูงสุดจะได้รับแจ้งทางอีเมล์ว่าเป็นผู้ประมูลสินค้าได้ หลังจากนั้นผู้ซื้อจะติดต่อกับผู้ขายโดยตรงถึงการชำระเงินและรับสินค้า ซึ่งเว็บไซต์ต่าง ๆ ที่เป็นผู้ดำเนินการประมูลจะไม่เกี่ยวข้องกับขั้นตอนหลังจากนี้ กระบวนการซื้อขายทั้งหมดจะใช้คอมพิวเตอร์เซิร์ฟเวอร์เพียงเครื่องเดียวของเว็บไซต์ที่ให้บริการประมูลในการจับคู่ตัวเลขในการซื้อขายนับพัน ๆ รายและใช้เวลาเพียงไม่กี่วินาทีเท่านั้น

การหลอกลวงโดยการประมูลนี้ซึ่งนับว่าเป็นตลาดที่มีสินค้ามากมายหลากหลายทำให้ผู้ที่ต้องการซื้อสินค้าสามารถเข้าไปเลือกดูได้ โดยจะมีการแบ่งแยกประเภทสินค้าตามจำพวก เช่น เครื่องใช้ไฟฟ้า กล้อง เสื้อผ้า เป็นต้น ผู้บริโภคสามารถที่จะเลือกดูได้ บางเว็บไซต์จะมีรูปภาพสินค้าให้ดูและมีการบรรยายสรรพคุณสินค้าไว้ ซึ่งลักษณะของการหลอกลวงประเภทนี้จะนำเอาสินค้าที่มีราคาสูง เช่น เครื่องคอมพิวเตอร์ นาฬิกา นำมาขายในราคาที่ถูกมากเพื่อเป็นการดึงดูดลูกค้าให้เข้ามาสนใจได้มาก เมื่อลูกค้าตัดสินใจซื้อสินค้าดังกล่าวแล้ว

---

[57] ชวลิต อัตถศาสตร์ และคณะ, Cyberlaw กฎหมายกับอินเตอร์เน็ต. หน้า 66-68.

ผู้ขายจะกำหนดให้ลูกค้าจ่ายเงินค่าสินค้าก่อน ซึ่งมีให้เลือกหลายทาง เช่น ทางบัตรเครดิต ทางแคชเชียร์เช็ค ทางธนาณัติ ซึ่งเมื่อผู้บริโภคส่งเงินให้ไปแล้วจะไม่ได้รับสินค้าตามที่โฆษณากล่าวอ้างหรือว่าไม่ได้รับสินค้าเลย

หน่วยงานรับร้องเรียนเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต (Internet Fraud Complaint Center : IFCC) ของ FBI ประเทศสหรัฐอเมริกา ได้ทำวิจัยเกี่ยวกับการประมูลสินค้าออนไลน์เมื่อเดือนเมษายน ค.ศ.2001 ระบุว่าการหลอกลวงประเภทนี้นับว่าเป็นการหลอกลวงที่ได้รับการร้องเรียนมากที่สุดในขณะนี้ ซึ่งส่วนใหญ่จะเป็นสินค้าประเภทเครื่องคอมพิวเตอร์ กล้องวีดีโอ เครื่องประดับ เทป เกมส์ โดยได้รับการร้องเรียนมากกว่า 30,000 ฉบับ ซึ่งเป็นการร้องเรียนในช่วงเดือนมกราคม - มีนาคม ค.ศ.2001 ถึงจำนวน 4,000 ฉบับ คิดเป็นมูลค่าความเสียหาย 253,300 ดอลลาร์สหรัฐ ซึ่งจำนวนตัวเลขความเสียหายดังกล่าวเป็นเพียงแค่ส่วนหนึ่งเท่านั้น เพราะว่ามีผู้ถูกหลอกลวงอีกจำนวนมากที่ไม่ได้ร้องเรียนเข้ามาจากการร้องเรียนดังกล่าวจะพบรูปแบบการหลอกลวงประเภทนี้หลายวิธีการ เช่น กรณีไม่ได้รับสินค้าตามที่ประมูลหรือไม่ได้สินค้าตรงตามที่โฆษณากล่าวอ้าง กรณีมีการประมูลสินค้าหลอกลวงคือผู้ขายจะเป็นผู้เข้าร่วมประมูลสินค้าดังกล่าวด้วย โดยจะเพิ่มราคาสินค้าที่ประมูลเรื่อย ๆ ทำให้ผู้ที่อยากได้สินค้าต้องประมูลราคาสินค้าสูงขึ้นตามไปด้วย เมื่อใกล้จะหมดเวลาของการประมูลผู้ขายจะยกเลิกการประมูลสินค้าดังกล่าว ทำให้บุคคลที่ประมูลราคาเป็นอันดับที่สองได้รับสินค้าไป ซึ่งเป็นการซื้อสินค้าในราคาสูงหรือการประมูลขายสินค้าที่ผิดกฎหมาย เป็นต้น ซึ่งหน่วยงาน IFCC ได้เตือนผู้ใช้บริการอินเตอร์เน็ตให้พึงระวังเกี่ยวกับการใช้บริการประมูลสินค้าออนไลน์ โดยเฉพาะกรณีผู้ขายสินค้าใช้อีเมล์แอดเดรสของบริการอีเมล์แอดเดรสฟรี เช่น aol.com, hotmail.com, yahoo.com, cs.com, home.com และ earthlink.net เป็นต้น เพราะจะแสดงให้เห็นว่าหากมีการกระทำความผิดเกิดขึ้น ผู้ถูกหลอกลวงไม่สามารถที่จะค้นหาได้เลยว่าผู้ขายคือใคร เพราะใคร ๆ ก็สามารถเข้าไปขออีเมล์แอดเดรสได้และในการขอก็ไม่จำเป็นต้องใส่ประวัติส่วนตัวที่แท้จริงอีกด้วย และสำหรับกรณีชำระค่าสินค้าด้วยบัตรเครดิตให้ผู้ถูกหลอกลวงรีบติดต่อบริษัทบัตรเครดิตโดยเร็ว เพราะนั่นหมายความว่าหากเจ้าของบัตรเครดิตแจ้งข้อเท็จจริงดังกล่าวเร็วเท่าไร ก็จะได้รับการคุ้มครองตามกฎหมายเร็วขึ้นเท่านั้น

การหลอกลวงดังกล่าวได้มีคำตัดสินของศาลแล้วหลายคดี เช่น คดีที่มลรัฐ California ชายคนหนึ่งได้ถูกฟ้องต่อศาล Western District of Washington ว่ากระทำการหลอกลวงโดยผ่านทางเว็บไซต์ประมูลสินค้าออนไลน์ โฆษณาขายกล้องดิจิตอลและเครื่องคอมพิวเตอร์พกพา (Laptop) เมื่อผู้บริโภคตัดสินใจซื้อสินค้าดังกล่าวและจ่ายเงินไป

กลับไม่ได้รับสินค้าตามที่ชายคนนั้นกล่าวอ้าง ซึ่งศาลได้ตัดสินเมื่อวันที่ 1 พฤศจิกายน ค.ศ.1999 ตัดสินให้จำคุก 14 เดือน และปรับเป็นเงิน 36,000 ดอลลาร์สหรัฐ หรือคดีที่มลรัฐ Florida ชายคนหนึ่งได้หลอกลวงขายสินค้าของตนเองผ่านทางเว็บไซต์ประมูลสินค้าออนไลน์ ขายสินค้าเกี่ยวกับอุปกรณ์คอมพิวเตอร์ แต่ผู้ซื้อไม่ได้รับสินค้าที่มีคุณภาพตรงตามที่ชายคนนั้นกล่าวอ้าง ซึ่งศาล Southern District of Florida ได้ตัดสินกักขังบริเวณ 6 เดือน และสั่งปรับเป็นเงิน 22,000 ดอลลาร์สหรัฐ หรือคดี FTC กับ Hare จำเลยได้นำสินค้าคือเครื่องคอมพิวเตอร์ไปประมูลขายในเว็บไซต์ประมูลสินค้าทางอินเตอร์เน็ต ซึ่งมีผู้สนใจเข้ามาซื้อในราคา 1,450 ดอลลาร์สหรัฐ โดยผู้ซื้อกับผู้ขายอยู่คนละต่างประเทศ เมื่อผู้ซื้อจ่ายเงินไปแล้วแต่ไม่ได้รับสินค้าดังกล่าว ซึ่งคดีดังกล่าวยังอยู่ในระหว่างการพิจารณาคดีของศาลสหรัฐ หรือคดีที่มลรัฐ Mississippi ผู้หญิงคนหนึ่งที่ได้กระทำการขายอุปกรณ์คอมพิวเตอร์รวมทั้งอุปกรณ์ฮาร์ดแวร์ ซอฟท์แวร์ ทางเว็บไซต์ แต่เมื่อมีผู้ซื้อตกลงซื้อสินค้าดังกล่าวแล้วกลับไม่ได้รับสินค้าตามที่โฆษณา คดีนี้ศาล Northen District of Mississippi ได้ตัดสินในวันที่ 27 สิงหาคม ค.ศ.1998 ให้จำคุกจำเลย 15 เดือน และปรับเป็นเงิน 9,432 ดอลลาร์สหรัฐ เพื่อชดเชยความเสียหายที่เกิดขึ้น

18. **การหลอกลวงเกี่ยวกับแชร์ลูกโซ่** (Pyramids and Multilevel Marketing)

การหลอกลวงประเภทนี้มีมานานแล้วตั้งแต่ในอดีต โดยผู้ถูกหลอกลวงจะอ้างว่าสามารถหาเงินได้ง่าย ๆ ด้วยการหาสมาชิกเข้าร่วมในธุรกิจดังกล่าว ยิ่งหาสมาชิกได้มากเท่าไร จะได้รับผลประโยชน์ตอบแทนมากขึ้นเท่านั้น โดยผู้เข้าร่วมธุรกิจดังกล่าวจะต้องนำเงินมาลงทุนตามที่ผู้ประกอบการกล่าวอ้าง เช่น อ้างว่าจะนำเงินไปลงทุนในธุรกิจระหว่างประเทศและจะได้รับผลประโยชน์ตอบแทน แต่แท้จริงแล้วเป็นนำเอาเงินของผู้เข้าร่วมธุรกิจภายหลังมาจ่ายเป็นผลประโยชน์ตอบแทนให้แก่คนก่อนหรือเรียกว่ามันนี่เกม (Money Game) เช่น แชร์แม่ชม้อย แชร์นกแก้ว หรือกรณีบริษัทบลิชเชอร์ เป็นต้น เมื่อเทคโนโลยีระบบเครือข่ายอินเตอร์เน็ตได้พัฒนาขึ้นมาก ทำให้กลุ่มอาชญากรนำแชร์ลูกโซ่มาหาสมาชิกโดยผ่านทางเว็บไวต์ จดหมายอิเล็กทรอนิกส์ กระดานข่าว ซึ่งสามารถเข้าถึงกลุ่มบุคคลได้ในวงกว้างและง่ายกว่าการสื่อสารในรูปแบบเดิม

วิวัฒนาการของแชร์ลูกโซ่ไม่ได้จบลงเพียงเท่านี้ ปัจจุบันได้มีผู้คิดที่จะเอานำระบบการตลาดคือระบบขายตรงแบบหลายชั้น (Multilevel Marketing) มาประยุกต์ใช้กับการประกอบอาชญากรรมดังกล่าว โดยอ้างว่าเป็นการประกอบธุรกิจขายสินค้ามาบังหน้าในการประกอบอาชญากรรม เช่น เครื่องสำอาง ผลิตภัณฑ์เพื่อสุขภาพ โดยอาจจะกำหนดให้ผู้ร่วมลงทุน

ต้องเสียเงินซื้อสินค้าดังกล่าวเพื่อนำไปขาย ซึ่งเมื่อพิจารณาสินค้าที่ได้รับกับจำนวนเงินที่ต้องเสียไปแล้วจะพบว่าคุณภาพสินค้าไม่คุ้มกับจำนวนเงินที่สูญเสียไป และหากต้องการได้รับผลประโยชน์ตอบแทนมากกว่านี้จะต้องหาสมาชิกมาสมัครเป็นลูกข่ายในการขายสินค้า ซึ่งผู้ที่สามารถหาสมาชิกได้จะได้รับเงินส่วนแบ่งจากการขายสินค้าของลูกข่ายของตนด้วย ยิ่งมีลูกข่ายมากเท่าไรจะได้รับผลประโยชน์ตอบแทนมากเท่านั้น หากพิจารณากันโดยผิวเผินแล้วหลายคนจะเข้าใจว่าการประกอบอาชญากรรมดังกล่าวเป็นการประกอบธุรกิจขายตรงที่ถูกกฎหมาย แต่เมื่อพิจารณาอย่างลึกซึ้งแล้วจะพบว่าการประกอบธุรกิจขายตรงที่ถูกกฎหมายกับการประกอบอาชญากรรมดังกล่าวจะแตกต่างกันโดยสิ้นเชิง ซึ่งมีข้อสังเกตง่าย ๆ คือหากเป็นการประกอบธุรกิจขายตรง ผลประโยชน์ที่สมาชิกจะได้รับจะเกิดจากการขายสินค้าดังกล่าว แต่การประกอบอาชญากรรม ผลประโยชน์ที่ผู้ร่วมกิจการได้รับจะเกิดจากการหาสมาชิกเข้าร่วม หาได้เกิดจากการขายสินค้าแต่อย่างใดไม่ ซึ่งในความเป็นจริงเมื่อพิจารณาตามหลักคณิตศาสตร์แล้วจะพบว่าการหาสมาชิกไปเรื่อย ๆ ในที่สุดก็คงมีวันหนึ่งที่ไม่สามารถหาสมาชิกมาเพิ่มได้ ซึ่งจะเป็นวันที่การประกอบธุรกิจดังกล่าวต้องล่มสลาย โดยผู้ที่สมัครเข้าเป็นสมาชิกในภายหลังจะไม่ได้รับผลประโยชน์ รวมทั้งเงินต้นก็สูญเปล่าด้วย บุคคลที่จะได้รับประโยชน์มากที่สุดก็คือผู้เริ่มต้นประกอบการนั่นเอง การหลอกลวงประเภทนี้มักจะกระทำผ่านเว็บไซต์ เนื่องจากสามารถเข้าถึงกลุ่มบุคคลได้จำนวนมากและทั่วโลก เพียงแต่เปิดเว็บไซต์ไว้และรอให้ผู้อื่นเปิดเข้าชม ซึ่งเมื่อการประกอบอาชญากรรมดังกล่าวดำเนินการมาได้ระยะหนึ่งก็จะปิดตัวเองโดยรวดเร็ว ทำให้ยากต่อการติดตามสืบหาตัวผู้กระทำความผิดมาลงโทษ

ในปัจจุบันนี้มีเว็บไซต์ที่ประกอบกิจการแชร์ลูกโซ่มากมายหลายเว็บไซต์ ทั้งที่มีต้นตอจากในประเทศและต่างประเทศ เช่น www.skybiz2000.com, www.successforever.com, www.mlmtoday.com, www.make1000000us.com เป็นต้น [58]

1. www.skybiz2000.com จัดทำโดยบริษัท skybiz จดทะเบียนในรัฐโอกาโลมา ประเทศสหรัฐอเมริกา ซึ่งเว็บไซต์ดังกล่าวจะแนะนำให้สมัครเป็นสมาชิกโดยเสียค่าธรรมเนียมแรกเข้า 25 ดอลลาร์สหรัฐ หรือประมาณ 1,000 บาท และเสียค่าธรรมเนียมรายปี 100 ดอลลาร์สหรัฐต่อปี หรือประมาณ 4,000 บาท วิธีการสมัครก็กระทำได้ง่าย ๆ โดยสมัครผ่านเว็บไซต์และชำระค่าสมัครโดยผ่านบัตรเครดิต เมื่อสมัครแล้วผู้สมัครจะได้รับพื้นที่ 15 Mb เพื่อนำไปประกอบธุรกิจในระบบเครือข่ายอินเตอร์เน็ตหรือจะนำไปสร้างเว็บไซต์ของครอบครัวก็ได้ ซึ่งในเว็บไซต์นี้

---

[58] หนังสือพิมพ์สยามธุรกิจ, วันที่ 30 กรกฎาคม - 5 สิงหาคม 2543, หน้า 15.

จะมีโปรแกรมการสร้างเว็บไซต์อย่างง่ายให้ด้วย เว็บไซต์ดังกล่าวมีทั้งหมด 20 กว่าภาษา รวมทั้งภาษาไทยด้วย และมีสมาชิกมากกว่า 230 ประเทศทั่วโลก โดยผู้สมัครเป็นสมาชิกจะได้รับค่าคอมมิสชั่นจากการขายเว็บไซต์ให้กับคนอื่นด้วย ซึ่งวิธีการหาสมาชิกจะกระทำในรูปแบบการขายแบบไบนารี (Binary) หรือระบบสองขา โดยสมาชิกจะต้องหาลูกทีมโดยขายเว็บไซต์ดังกล่าวให้กับบุคคลอื่นสองคนและลูกทีมแต่ละคนก็จะกระทำการขายเว็บไซต์ในลักษณะเดียวกัน โดยสมาชิกจะได้รับค่าคอมมิสชั่นเพิ่มขึ้นตามจำนวนลูกทีมที่หาได้ ดังนี้

หาลูกทีมได้ 9 คน จะได้ 70 ดอลลาร์สหรัฐ
หาลูกทีมได้ 18 คน จะได้ 35 ดอลลาร์สหรัฐ
หาลูกทีมได้ 27 คน จะได้ 35 ดอลลาร์สหรัฐ
หาลูกทีมได้ 36 คน จะได้ 70 ดอลลาร์สหรัฐ
หาลูกทีมได้ 50 คน จะได้ 70 ดอลลาร์สหรัฐ

ซึ่งจะจ่ายค่าคอมมิสชั่นผ่านทางเช็ค โดยสมาชิกจะต้องเสียค่าธรรมเนียม 2 ดอลลาร์สหรัฐต่อเช็คหนึ่งใบ แม้ว่าเว็บไซต์ดังกล่าวจะกล่าวอ้างว่าเป็นการประกอบธุรกิจแบบขายตรงที่มีตัวสินค้าคือเว็บไซต์ แต่ในความเป็นจริงแล้วการได้รับค่าคอมมิสชั่นจะขึ้นอยู่กับการหาสมาชิกมาสมัคร หาได้ขึ้นอยู่กับการขายสินค้าไม่

2. www.successforever.com เป็นเว็บไซต์ที่มีต้นตอมาจากประเทศไต้หวัน โดย Mr.Steve Chen เว็บไซต์ดังกล่าวจะมีหลายภาษา เช่น ภาษาไทย ภาษาจีน ภาษาฝรั่งเศส ภาษาเยอรมัน ฯลฯ โดยผู้สมัครจะต้องเสียค่าสมัคร 110 ดอลลาร์สหรัฐ และเมื่อหาสมาชิกได้ 9 คน จะได้รับค่าคอมมิสชั่น 100 ดอลลาร์สหรัฐ ผลประโยชน์ตอบแทนจะได้เพิ่มขึ้นตามจำนวนสมาชิกที่แต่ละคนหามาได้

3. เว็บไซต์ที่คนไทยสร้างขึ้นมาเพื่อหาสมาชิกให้เข้ามาสร้างรายได้ โดยการแนะนำสมาชิกและมีการจ่ายค่าตอบแทนกันเป็นทอด ๆ ตามโครงสร้างหลายชั้น ซึ่งดูผิวเผินเหมือนกับมีสินค้าคือตัวเว็บไซต์ (เช่นเดียวกับ skybiz) แต่เมื่ออ่านดูวิธีการในการสร้างรายได้จากการร่วมธุรกิจแล้วกลับเป็นการล่าหัวคิวเป็นหลัก ซึ่งจะกล่าวอ้างว่าเนื่องด้วยบริษัทเปิดตัวใหม่ในการทำธุรกรรมผ่านระบบเครือข่ายอินเตอร์เน็ต จึงต้องการประชาสัมพันธ์ธุรกิจบนอินเตอร์เน็ตให้เป็นที่รู้จักว่าเป็นสื่อที่มีคุณภาพที่สุดในปัจจุบันและเข้าถึงทุกแห่งทั่วโลก ใช้ต้นทุนที่ต่ำที่สุด โดยผู้เข้าร่วมธุรกิจไม่ต้องลงทุนอะไรเลย จึงตัดประเด็นที่ว่าจะขาดทุนไปเลยและยังง่ายต่อ

การดำเนินงานเพราะเป็นธุรกิจ MLM เพียงท่านรู้จักคนเพียง 3 คน เท่านั้น ท่านก็ดำเนินธุรกิจได้แล้วและยังมีรายได้ถึง 6 หลัก ซึ่งจากรายละเอียดเว็บไซต์ดังกล่าวจะกำหนดการลงทะเบียนแรกเข้ารายละ 600 บาท หาสมาชิกต่อท้ายได้ 3 รายจะได้ 1 คะแนน และให้สมาชิกทั้ง 3 รายไปหาสมาชิกต่อแบบแตก 3 จะทำให้ท่านมีรายได้ดังนี้ สัปดาห์ที่ 1 หากหาสมาชิกได้ 3 ราย ได้ 1 คะแนน และทุก ๆ สัปดาห์สมาชิกที่เป็นลูกข่ายท่านก็ขยายออกไปเหมือนที่ท่านทำภายในสัปดาห์ที่ 5 ท่านจะมีสมาชิกรวม 243 คน หรือ 81 คะแนน จะได้รับเงินจำนวน 11,400 บาท [59]

จะเห็นได้ว่าจากตัวอย่างทั้งสามเว็บไซต์ดังกล่าวเป็นการหาสมาชิกโดยอาศัยระบบการตลาดขายตรงแบบหลายชั้น (Multi-Level marketing : MLM) แม้ว่าผู้หลอกลวงจะอ้างว่าเป็นการประกอบธุรกิจโดยมีตัวมีสินค้า คือ พื้นที่ในระบบเครือข่ายอินเตอร์เน็ต ซึ่งนับว่าเป็นสินค้าที่เป็นนามธรรมมากในการที่จะตีราคาว่าเท่าไร แต่สิ่งที่ยืนยันได้ว่าทั้งหมดเป็นการหลอกลวงประเภทแชร์ลูกโซ่ก็คือการเน้นหาสมาชิกและการได้รับผลประโยชน์ตอบแทนขึ้นอยู่กับจำนวนสมาชิกที่แต่ละคนหามาได้

ซึ่งรูปแบบการหลอกลวงดังกล่าวได้พบมากในประเทศสหรัฐอเมริกา ซึ่งได้มีการดำเนินคดีกับเว็บไซต์ที่หลอกลวงดังกล่าวมาแล้วมากมายหลายเว็บไซต์ เช่น คดีระหว่าง FTC กับบริษัท Fortuna Alliance ซึ่งเป็นการหาสมาชิกทางระบบเครือข่ายอินเตอร์เน็ต โดยกล่าวอ้างว่าผู้หลอกลวงจะได้รับเงินประมาณ 250 – 5,000 ดอลลาร์สหรัฐต่อเดือน ในการหาสมาชิกทำให้ความเสียหายที่เกิดขึ้นเป็นวงกว้าง และเนื่องจากการกระทำดังกล่าวเป็นการหาสมาชิกบนระบบเครือข่ายอินเตอร์เน็ต ซึ่งสามารถกระทำได้โดยง่าย รวดเร็ว ปรากฏว่าร้อยละ 95 ของคนที่เข้าร่วมหาสมาชิกดังกล่าวไม่ได้รับเงินค่าคอมมิสชั่นแต่อย่างใด สมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐอเมริกาจึงได้ฟ้องร้องบริษัทดังกล่าวว่ากระทำความผิดกฎหมาย ซึ่งศาลได้สั่งให้บุคคลดังกล่าวห้ามกระทำการหาสมาชิกทางอินเตอร์เน็ตและให้ชดใช้ค่าเสียหายให้แก่ผู้เสียหายเป็นจำนวนเงินถึง 2 ล้านดอลลาร์สหรัฐ พร้อมดอกเบี้ยให้แก่ผู้เสียหาย และล่าสุดยังมีคดีฟ้องบริษัท Credit Development International ซึ่งบริษัทดังกล่าวอ้างว่าบริษัทสามารถอนุมัติบัตรเครดิตวีซ่าหรือบัตรเครดิตมาสเตอร์การ์ด โดยมีวงเงินให้ 5,000 ดอลลาร์สหรัฐ และกรณีผิดนัดจะเสียดอกเบี้ยในอัตราที่ต่ำและจะได้รับรายได้เป็นค่าคอมมิสชั่นถึงเดือนละ 18,000 ดอลลาร์สหรัฐ หรือมากกว่านั้น จากการหาสมาชิกเข้ามาร่วมกับบริษัทดังกล่าวปรากฏว่า

---

[59] หนังสือพิมพ์สยามธุรกิจ, วันที่ 19 – 25 มีนาคม 2543, หน้า 20.

มีผู้เข้าร่วมกับบริษัทดังกล่าวถึง 30,000 คน ประมาณมูลค่าความเสียหายได้ 3-4 ล้านดอลลาร์สหรัฐ [60] ซึ่งคดีดังกล่าวกำลังอยู่ระหว่างการพิจารณาของศาลสหรัฐ รวมทั้งคดีของเว็บไซต์ Skybiz ด้วยที่กำลังมีการฟ้องร้องอยู่ในชั้นศาลของหลายประเทศ เช่น ประเทศสหรัฐอเมริกา ประเทศมาเลเซีย ประเทศอินเดีย เป็นต้น

19. การหลอกลวงเกี่ยวกับการท่องเที่ยว (Travel Fraud)

เป็นการหลอกลวงว่าได้รับรางวัลให้เดินทางไปท่องเที่ยวยังสถานที่ต่าง ๆ โดยมีการบรรยายสถานที่พักว่าเป็นโรงแรมระดับห้าดาวพร้อมอาหารให้ โดยที่ผู้ได้รับรางวัลไม่ต้องเสียค่าใช้จ่ายใด ๆ เลย หรือเสียเงินในราคาที่ถูกมาก ซึ่งเมื่อผู้ได้รับรางวัลตกลงรับข้อเสนอรางวัลดังกล่าวแล้วและเดินทางไปจะพบว่าสถานที่จริงกับที่กล่าวอ้างนั้นไม่ตรงกัน โรงแรมที่พักเป็นโรงแรมที่แย่มาก โดยผู้หลอกลวงจะบอกว่าถ้าต้องการที่จะพักในห้องอีกแบบหนึ่ง ผู้ได้รับรางวัลจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เพิ่มขึ้นเอง ซึ่งผู้ได้รับรางวัลส่วนใหญ่ก็ต้องยอมชำระเงินเพิ่มเติมเนื่องจากได้เดินทางไปถึงแล้ว หรือเป็นกรณีที่โฆษณาแพ็คเก็จทัวร์ราคาถูก โดยเมื่อผู้ถูกหลอกลวงจ่ายเงินไปและเมื่อเดินทางจะพบว่ามีค่าใช้จ่ายบางรายการที่ไม่ได้พูดถึงในข้อตกลงซึ่งผู้ถูกหลอกลวงต้องรับผิดชอบเอง เช่น ค่าธรรมเนียมสนามบิน ค่าธรรมเนียมโรงแรม หรือค่าบริการต่าง ๆ อีกมาก ซึ่งเมื่อรวมกันแล้วจะมีราคาแพงกว่าแพ็คเก็จทัวร์ธรรมดาเสียอีก เช่น ศาลสหรัฐอเมริกาได้ตัดสินคดีบริษัท Your Travel and Tours ว่าเป็นการกระทำความผิดหลอกลวงเกี่ยวกับการท่องเที่ยว โดยจำเลยต้องชดใช้ค่าเสียหายถึง 84,000 ดอลลาร์สหรัฐ และจะต้องจ่ายเงินล่วงหน้าเพื่อรับประกันความเสียหายอีก 150,000 ดอลลาร์สหรัฐ หากต้องการที่จะเปิดบริษัทดำเนินการต่อไปในอนาคต [61]

---

[60] FTC, The ftc on "consumer protection cyberspace: combating fraud on the internet" [Online]. Available from: http://www.ftc.gov/os/1998/9806/test.623.htm. [2002, May 20]

[61] FTC, Travel Promoter Settles FTC Charges Foreign Nationals were Targeted in scam [Online]. Available from: http://www.ftc.gov/opa/1998/9809/alam.2.thml. [2002, June 30]

20. การหลอกลวงเกี่ยวกับการอุปกรณ์คอมพิวเตอร์และอุปกรณ์ซอฟท์แวร์ (Computer Equipment/Software)

เป็นการหลอกลวงให้ผู้ใช้บริการระบบเครือข่ายอินเตอร์เน็ตสามารถสั่งซื้ออุปกรณ์คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ต่าง ๆ ได้ในราคาถูก ซึ่งมีทั้งในรูปแบบของการส่งสินค้าหรือว่าเป็นการให้ดาว์นโหลดข้อมูลได้ โดยที่โปรแกรมต่าง ๆ จะเป็นโปรแกรมที่ไม่มีลิขสิทธิ์ทำให้เกิดปัญหาในภายหลัง เช่น จะมีระยะเวลากำหนดในการใช้งาน ซึ่งผู้ที่ซื้อโปรแกรมดังกล่าวมาจะไม่ทราบ ในขณะที่ถ้าซื้อโปรแกรมที่ถูกกฎหมายสามารถใช้งานได้ตลอด หรือว่าเป็นโปรแกรมที่ไม่มีคุณภาพตามที่ผู้หลอกลวงกล่าวอ้าง [62]

3.2.3 สถิติเกี่ยวกับการหลอกลวงทางอินเตอร์เน็ต

ก. ความเสียหายจากการหลอกลวงทางอินเตอร์เน็ต

ข้อมูลสถิติจาก National Consumer League (NCL) ของประเทศสหรัฐอเมริกาพบว่าการหลอกลวงทางอินเตอร์เน็ตในประเภทต่าง ๆ ได้ก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจเป็นอย่างมาก ดังจะเห็นได้จากความเสียหายในปี ค.ศ. 2000 มีความเสียหายทั้งสิ้น 3,387,530 ดอลลาร์สหรัฐ สำหรับความเสียหายในปี ค.ศ. 2001 มีความเสียหายถึง 6,152,070 ดอลลาร์สหรัฐ ซึ่งจากจำนวนตัวเลขความเสียหายดังกล่าวจะเห็นได้ว่าเพิ่มมากขึ้นจากปีก่อนถึงเท่าตัว หรือเมื่อคิดความเสียหายต่อจำนวนประชากรแล้วจะพบว่า ในปี ค.ศ. 2000 ความเสียหายจากการหลอกลวงทางอินเตอร์เน็ต ต่อ 1 คน เป็นเงิน 427 ดอลลาร์สหรัฐ ในปี ค.ศ. 2001 ความเสียหายจากการหลอกลวงทางอินเตอร์เน็ตต่อ 1 คน เป็นเงิน 518 ดอลลาร์สหรัฐ จากจำนวนความเสียหายที่เพิ่มขึ้นทุกปีแสดงให้เห็นถึงว่าอาชญากรรมประเภทนี้กำลังทวีความรุนแรงมากขึ้นทุกขณะ ซึ่งนับว่าเป็นความเสียหายต่อระบบเศรษฐกิจอย่างมหาศาล และหน่วยงานดังกล่าวยังได้จัดอันดับการหลอกลวงทางอินเตอร์เน็ตไว้ด้วย ดังนี้ [63]

---

[63] 2001 Internet Fraud Statistics [Online]. Available from: http://www.fraud.org/internet/ 2201stats.htm. [2002, June 9]

หน่วย : ร้อยละ (%)

ประเภทของการหลอกลวง	คศ.2001	คศ.2000	คศ.1999
1. Online Auctions	70	78	87
2. General Merchandise Sales	9	10	7
3. Nigerian Money Offers	9	1	-
4. Computer Equipment/ Software	2	1	1.3
5. Internet Access Service	2	3	2
6. Information/Adult Service	2	1	0.2
7. Work at Home Scams	2	3	0.9
8. Advance Fee Loans	1	2	0.2
9.Credit Card Offers	0.5	0.5	-
10.Business Opportunities/ Franchises	0.5	-	-

และข้อมูลจากเว็บไซต์เดียวกันนี้ได้มีการแบ่งแยกความเสียหายจากการหลอกลวงทางอินเตอร์เน็ตแต่ละประเภทต่อ 1 คน ดังนี้

หน่วย : ดอลลาร์สหรัฐ

ประเภทของการหลอกลวง	คศ.2001	คศ.2000	คศ.1999
1. Online Auctions	411	326	284
2. General Merchandise Sales	730	784	465
3. Nigerian Money Offers	5,957	3,000	-
4. Computer Equipment / Software	1,048	724	580
5. Internet Access Service	535	631	438
6. Information/Adult Service	209	310	-
7. Work at Home Scams	121	145	383
8. Advance Fee Loans	1,121	881	-
9.Credit Card Offers	309	138	-
10.Business Opportunities/ Franchises	10,147	-	-

ข. บุคคลผู้ถูกหลอกลวง

และข้อมูลจากเว็บไซต์เดียวกันยังได้แบ่งกลุ่มบุคคลที่ถูกหลอกลวง โดยแยกประเภทตามอายุไว้ดังนี้

หน่วย : ร้อยละ(%)

อายุ	คศ.2001	คศ.2000	คศ.1999
ต่ำกว่า 20 ปี	4	2	2.3
20-29	26	20	19
30-39	28	28	29
40-49	24	29	28
50-59	13	15	15
60-69	4	6	4
70 ขึ้นไป	1	1	0.7

3.2.4 วิธีการหลอกลวงทางอินเตอร์เน็ต

การหลอกลวงทางอินเตอร์เน็ตสามารถแยกวิธีการหลอกลวงได้เป็น 4 วิธีการ คือ

1. การหลอกลวงทางจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นการส่งจดหมายทางอิเล็กทรอนิกส์เหมือนกับการส่งจดหมายธรรมดา เพียงแต่ว่าสะดวกและรวดเร็วกว่าการส่งจดหมายธรรมดา ผู้ส่งสามารถส่งจดหมายฉบับเดียวไปให้ผู้รับได้ครั้งละหลาย ๆ คน ซึ่งเป็นการประหยัดต้นทุนและประหยัดเวลาในการส่ง โดยผู้ส่งจะหาที่อยู่ของผู้รับได้จากการที่ผู้ใช้อินเตอร์เน็ตเข้าไปใส่อีเมล์แอดเดรสของตนไว้ในเว็บไซต์ต่าง ๆ เพื่อขอข้อมูลจากเว็บไซต์ทั่วไป โดยผู้ได้รับอีเมล์ดังกล่าวจะไม่รู้จักว่าผู้ส่งเป็นใครหรือบางครั้งเราเรียกจดหมายอิเล็กทรอนิกส์ที่ได้รับจากบุคคลที่ไม่รู้จักนี้ว่าสแปมเมล์ (Spam Mail) เช่น ส่งจดหมายอิเล็กทรอนิกส์หลอกลวงว่าผู้ถูกหลอกลวงสามารถให้ท่านทำงานที่บ้านได้และจะได้รับผลประโยชน์ตอบแทนเดือนละหลายหมื่นบาท หากสนใจรายละเอียดให้เข้าไปดูที่เว็บไซต์ที่

ระบุหรืออาจจะให้ติดต่อกลับไปยังเบอร์โทรที่ผู้ส่งได้ให้ไว้ ซึ่งโดยส่วนใหญ่แล้วการหลอกลวงที่กระทำผ่านทางจดหมายอิเล็กทรอนิกส์มักจะเป็นการหลอกลวงเกี่ยวกับการโอนเงินจากประเทศไนจีเรีย (Nigerian Money) การหลอกลวงเกี่ยวกับการสมัครบัตรเครดิต (Credit Card Offer) การหลอกลวงเกี่ยวกับการประกอบธุรกิจที่บ้าน (Work at Home) เป็นต้น

2. การหลอกลวงทางเว็บไซต์ (Web site) จะพบว่าการหลอกลวงด้วยรูปแบบต่าง ๆ มักจะกระทำโดยการเปิดเว็บไซต์ เนื่องจากเป็นการหลอกลวงที่ลงทุนน้อยมากและสามารถเข้าถึงกลุ่มคนได้อย่างทั่วถึง ซึ่งการเข้าถึงเว็บไซต์ดังกล่าวก็กระทำได้ไม่ยาก แม้ว่าบุคคลทั่วไปจะไม่รู้ชื่อเว็บไซต์ก็ไม่ใช่ปัญหาแต่อย่างใด เพราะสามารถค้นหาได้จากเว็บไซต์ที่ให้บริการค้นหา (Search Engine) เพียงระบุคำสำคัญที่ต้องการจะค้นหาเท่านั้น เว็บไซต์นั้นก็จะปรากฏรายชื่อเว็บไซต์ที่เราต้องการค้นหาให้ ซึ่งในปัจจุบันนี้เว็บไซต์ที่ให้บริการค้นหาโดยไม่คิดค่าบริการมีหลายเว็บไซต์ เช่น www.yahoo.com, www.google.com เป็นต้น ซึ่งการหลอกลวงทางเว็บไซต์จะมีความน่าเชื่อถือมากเพราะว่าสามารถแสดงการหลอกลวงได้โดยทางรูปภาพ เสียง ข้อความ หรือแม้กระทั่งมีการเอาวีดีโอบันทึกบุคคลที่ประสบความสำเร็จจากการร่วมประกอบธุรกิจดังกล่าวมาลงในเว็บไซต์เพื่อหลอกลวงผู้อื่นได้อีกด้วย

โดยผู้กระทำความผิดอาจจะทำการเปิดเว็บไซต์ด้วยตัวเอง เพราะว่าปัจจุบันนี้การสร้างเว็บไซต์ไม่ใช่สิ่งที่ยากอีกต่อไป เนื่องจากมีโปรแกรมในการสร้างเว็บไซต์สำเร็จรูป ซึ่งเว็บไซต์ดังกล่าวจะโฆษณาวิธีการหลอกลวงต่าง ๆ โดยจัดทำหน้าโฮมเพจให้ดึงดูดผู้ที่เข้ามาชมและรอให้บุคคลอื่นเข้ามาอ่านเว็บไซต์ดังกล่าวเท่านั้น โดยจะมีถ้อยคำเชิญชวนให้ผู้เข้าชมหลงเชื่อจนต้องสูญเสียเงินในที่สุด ซึ่งวิธีการหลอกลวงวิธีนี้จะเป็นการเข้าถึงบุคคลทั่วไปได้อย่างทั่วถึงครอบคลุมได้มากกว่าการส่งจดหมายอิเล็กทรอนิกส์ ดังจะเห็นได้จากการเปิดเว็บไซต์แชร์ลูกโซ่ที่กำลังแพร่หลายอย่างหนักอยู่ในขณะนี้ โดยเว็บไซต์ดังกล่าวจะมีการนำเอาผู้ที่เคยเข้าร่วมงานดังกล่าวมาเล่าถึงความสำเร็จของตนเอง ทำให้ผู้เข้าชมหลงเชื่อจนสูญเสียเงินไปเป็นจำนวนมาก หรือการเปิดเว็บไซต์ประมูลสินค้าออนไลน์ หรืออาจเป็นการหลอกลวงโดยแอบแฝงในเว็บไซต์ที่ประกอบธุรกิจที่ถูกกฎหมาย เป็นต้น

3. การหลอกลวงทางห้องสนทนาอินเตอร์เน็ต (Internet Relay Chat:IRC) โปรแกรม IRC เป็นโปรแกรมที่ใช้สำหรับสนทนาทางระบบเครือข่ายอินเตอร์เน็ต มีลักษณะคือ ผู้ใช้โปรแกรม IRC สามารถเข้าไปสนทนากับผู้อื่นได้ใน Server ที่จัดเตรียมไว้ โดยจะมีการแบ่งเป็นห้อง ๆ ตามหัวข้อเรื่องที่แต่ละคนสนใจ ซึ่งปัจจุบันนี้ได้มีการควบคุมจำนวนคนแต่ละ

ห้องไม่ให้มากเกินไปจนไม่สามารถสนทนากันได้ ช่องสนทนาบางช่องอาจจะเปิดกว้างสำหรับคนทั่วไป แต่บางช่องจะสงวนสิทธิ์ไว้สำหรับกลุ่มสมาชิกและผู้ที่มีรหัสผ่านเท่านั้น โดยผู้ที่ใช้บริการอินเตอร์เน็ตทั่วไปไม่สามารถเข้าใช้บริการได้ สำหรับวิธีการสนทนากระทำโดยบุคคลใดบุคคลหนึ่งพิมพ์ข้อความที่ต้องการสนทนาแล้ว บุคคลอื่นที่อยู่ในห้องสนทนาเดียวกันจะเห็นข้อความทั้งหมด โดยบุคคลอื่น ๆ สามารถแสดงความคิดเห็นตอบโต้ได้ทันที ซึ่งการหลอกลวงด้วยวิธีการนี้เป็นการหลอกลวงเกี่ยวกับการประกอบธุรกิจ หรือการขายสินค้าออนไลน์ ซึ่งจะเป็นช่องสนทนาที่เปิดเผยและพบเห็นได้ง่าย

4. การหลอกลวงทางกระดานข่าว (Web board) บนระบบเครือข่ายอินเตอร์เน็ตมีช่องข่าวอยู่มากมายหลายช่อง แต่ละช่องล้วนมีเนื้อหาแตกต่างกันไปตามหัวข้อช่องข่าวเหล่านี้เปิดสำหรับผู้ที่ใช้บริการอินเตอร์เน็ตทุกคนสามารถเข้าไปเยี่ยมชมได้ ซึ่งในช่องข่าวนี้ใครก็สามารถแลกเปลี่ยนข้อมูลของตนกับผู้อื่นที่มีความสนใจในเรื่องเดียวกันได้แม้จะอยู่ห่างกันคนละซีกโลก ส่วนใหญ่ เช่น สนใจเรื่องการประกอบธุรกิจที่บ้าน การลงทุน การเริ่มประกอบธุรกิจด้วยตัวเอง การขายสินค้าทางอินเตอร์เน็ต เป็นต้น ซึ่งบุคคลดังกล่าวจะเข้ามาพบปะและแลกเปลี่ยนข้อมูลกัน

ข้อมูลจากหน่วยงาน National Consumer League พบว่าวิธีการหลอกลวงส่วนใหญ่จะเป็นการหลอกลวงโดยกระทำผ่านทางเว็บไซต์ (Web site) เพราะว่าเป็นวิธีการหลอกลวงที่เข้าถึงกลุ่มบุคคลได้มากที่สุด และวิธีการต่อมาคือทางจดหมายอิเล็กทรอนิกส์ (E-Mail) และรองลงมา คือ การหลอกลวงโดยกระทำผ่าน Newsgroups ดังจะเห็นได้จากข้อมูลดังนี้ [64]

หน่วย : ร้อยละ (%)

วิธีการ	ค.ศ.2001	ค.ศ.1999	ค.ศ.1998
1. ทางเว็บไซต์	83	84	90
2.ทางจดหมายอิเล็กทรอนิกส์	15	12	9
3.ทางกระดานข่าว	1	4	1
4. อื่น ๆ	1	0	1

[64] Ibid.

สำหรับประเทศไทยจากจำนวนสถิติจำนวนผู้ใช้อินเตอร์เน็ตของประเทศไทยที่ได้เริ่มมีการใช้งานอินเตอร์เน็ตเป็นครั้งแรกเมื่อประมาณปี พ.ศ. 2530 โดยเริ่มมีจุดพัฒนาอย่างจริงจังเมื่อมีการก่อตั้งเครือข่ายไทยสารในปี พ.ศ. 2535 เรื่อยมาจนปี พ.ศ. 2538 จึงมีการก่อตั้งบริษัทอินเตอร์เน็ตประเทศไทย (Internet Thailand) ขึ้นเป็นผู้ให้บริการอินเตอร์เน็ตหรือไอเอสพี (Internet Service Provider) รายแรกของไทย ซึ่งเป็นจุดเริ่มต้นของการเปิดบริการอินเตอร์เน็ตให้แก่ประชาชนทั่วไป หลังจากนั้นระบบเครือข่ายอินเตอร์เน็ตก็ได้รับความนิยมแพร่หลายอย่างก้าวกระโดด จากจำนวนผู้ใช้เพียงไม่กี่หมื่นคนในปี พ.ศ. 2538 กลายเป็นประมาณ 3.5 ล้านคน ในปัจจุบัน ซึ่งน่าจะเป็นสิ่งที่แสดงให้เห็นว่าปัญหาอาชญากรรมทางคอมพิวเตอร์กำลังจะกลายปัญหาใหญ่ในสังคมไทยในอนาคตอันใกล้นี้