บทที่ 2

ขอบเขตของอาชญากรรมคอมพิวเตอร์

บทบาทและความสำคัญของคอมพิวเตอร์ เป็นที่ยอมรับของสังคมมนุษย์ในปัจจุบันและนับวันบทบาทของคอมพิวเตอร์จะเพิ่มขึ้นเรื่อย ๆ จนกลายเป็นความจำเป็นที่จะต้องมีไว้ใช้ในชีวิตประจำวัน ไม่ใช่มีความสำคัญเพียงเฉพาะบริษัทหรือหน่วยงานของรัฐเท่านั้น เมื่อคอมพิวเตอร์ได้มีการพัฒนาและขยายเครือข่ายออกไปอย่างรวดเร็วและกว้างขวางมากเท่าใด ปัญหาการกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-Related Crime) หรือเรียกสั้น ๆ ว่าอาชญากรรมคอมพิวเตอร์ (Computer Crime) ย่อมทวีความรุนแรงมากขึ้นเท่านั้น

วิทยานิพนธ์ฉบับนี้ศึกษาถึงปัญหาอาชญากรรมคอมพิวเตอร์ในด้านพยานหลักฐาน ในเบื้องต้นจึงควรทราบถึงโครงสร้างขั้นพื้นฐานของคอมพิวเตอร์และคำนิยามศัพท์ ของระบบคอมพิวเตอร์เพื่อจะได้มีความเข้าใจกับอาชญากรรมคอมพิวเตอร์ในแง่มุมต่าง ๆ ซึ่งผู้เขียนจะได้นำเสนอต่อไป

2.1 พื้นฐานทางด้านเทคนิค

2.1.1 เครื่องคอมพิวเตอร์คืออะไร

เครื่องคอมพิวเตอร์หรือนิยมเรียกกันอีกอย่างหนึ่งว่า "สมองกล" เป็นเครื่องจักรทางอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นมาให้มีความสามารถพิเศษ 3 ลักษณะ ดังนี้

(1) ความรวดเร็วในการทำงานสูงมาก สามารถทำการรับข้อมูลเพื่อคำนวณหรือเปรียบเทียบได้รวดเร็วกว่าเครื่องคิดเลขธรรมดา จึงต้องมีการบัญญัติหน่วยวัดความเร็วใหม่เป็น Millisecond (10^{-3} วินาที), Microsecond (10^{-6} วินาที) Nanosecond (10^{-9} วินาที)

(2) มีหน่วยความจำภายในเครื่อง (Internal Memory) สามารถรับข้อมูล

(Data) และคำสั่งต่าง ๆ (Instructions) เก็บไว้ในหน่วยความจำ (Memory) ตามลำดับก่อนหลังและนำไปประมวลผลได้เองโดยอัตโนมัติ

(3) ความสามารถในการเปรียบเทียบ (Comparability) คอมพิวเตอร์มีหน่วยคำนวณและตรรกซึ่งนอกจากสามารถทำงานด้านการคำนวณต่าง ๆ ได้แล้วยังสามารถทำการเปรียบเทียบได้ด้วยและสามารถทำงานตามวิธีการทำการกำหนดซ้ำ ๆ กันจนกระทั่งหมดข้อมูล (นรินทร์ เนาวประทีป, 2529 : 1)

เครื่องคอมพิวเตอร์คือ เครื่องใช้ไฟฟ้าหรือเครื่องอิเล็กทรอนิกส์ชนิดหนึ่ง ซึ่งมีหน่วยความจำ และสามารถทำการคำนวณเปรียบเทียบ และคัดเลือกข้อมูลต่าง ๆ ที่เป็นตัวเลข ตัวอักษร รูปสัญลักษณ์ รูปภาพหรือแม้กระทั่งเสียงต่าง ๆ ได้ โดยใช้วงจรไฟฟ้าจำนวนมาก และทำงานเป็นไปตามชุดคำสั่งที่เรียกว่าโปรแกรม (Program) ซึ่งเขียนขึ้นเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามที่ต้องการ

2.1.2 **ขนาดของเครื่องคอมพิวเตอร์** ปัจจุบันนี้สามารถแบ่งขนาดออกได้ ดังนี้

(1) ซุปเปอร์คอมพิวเตอร์ (Supercomputer) เป็นคอมพิวเตอร์ขนาดใหญ่ ซึ่งสามารถทำงานได้เร็วและมีราคาแพงมาก ใช้ในโครงการค้นคว้าทางวิทยาศาสตร์ การพยากรณ์อากาศ งานด้านวิศวกรรม ผลิตอาวุธสมัยใหม่และโครงการอวกาศ

(2) เมนเฟรมคอมพิวเตอร์ (Mainframe) คือคอมพิวเตอร์ขนาดใหญ่รองลงมาในธุรกิจและหน่วยงานใหญ่ ๆ ตลอดจนมหาวิทยาลัยและหน่วยงานรัฐบาลมักใช้คอมพิวเตอร์เมนเฟรม เนื่องจากมีความสามารถเก็บข้อมูลได้มหาศาล เช่น เก็บข้อมูลของนิสิตนักศึกษาทั้งมหาวิทยาลัย คอมพิวเตอร์ชนิดนี้ยังสามารถเชื่อมโยงการใช้งานกับเครื่องปลายทางในระยะทางไกลต่าง ๆ กัน เช่นเชื่อมโยงและควบคุมการใช้เครื่องบริการฝากถอนเงินอัตโนมัติ (ATM) ของลูกค้าธนาคารตามสถานที่ต่าง ๆ ก่อให้เกิดความสะดวกสบายมากในชีวิตปัจจุบัน

(3) มินิคอมพิวเตอร์ (Minicomputer) มีความคล้ายคลึงกับเมนเฟรม แต่ว่ามีขนาดเล็กกว่า ความเร็วในการทำงานต่ำกว่า นิยมใช้ในธุรกิจขนาดกลาง คอมพิวเตอร์ประเภทนี้สามารถเชื่อมโยงกับเครื่องปลายทางหลาย ๆ เครื่องได้

(4) ไมโครคอมพิวเตอร์ (Microcomputer) คือ คอมพิวเตอร์ขนาดเล็ก สามารถตั้งไว้บนโต๊ะ (Desk-Top) หรือวางไว้บนตัก (Lap-Top) หรือแม้กระทั่งวางไว้ในฝ่ามือ (Note-Book) โดยมีราคาไม่แพง ขนาดและลักษณะการใช้งานที่ง่ายจึงเป็นที่นิยมแพร่หลายอย่างรวดเร็ว นิยมเรียกว่าคอมพิวเตอร์ส่วนบุคคล (PC : Personal Computer) จากความนิยมที่แพร่หลายอย่างรวดเร็ว ทำให้บริษัทผู้ผลิตต่างแข่งขันกันผลิตและพัฒนาไมโครคอมพิวเตอร์ เพื่อจะได้ใช้ประโยชน์ได้เต็มที่จากความสามารถของตัวเครื่อง

2.1.3 คำนิยามศัพท์ของระบบคอมพิวเตอร์ (Computer System)

ระบบคอมพิวเตอร์นั้นประกอบขึ้นด้วย ส่วนที่เป็นตัวเครื่องสามารถจับต้องได้ (Computer Hardware) และส่วนที่เป็นโปรแกรม (Computer Software) ซึ่งทำหน้าที่ร่วมกันในการประมวลผลข้อมูล ส่วนที่เป็นบุคลากร (Peopleware) และระบบเครือข่ายอินเตอร์เน็ต (Internet)

2.1.3.1 ฮาร์ดแวร์ (Hardware)

หมายถึง ตัวเครื่องคอมพิวเตอร์ที่บริษัทอุตสาหกรรมได้สร้างขึ้นรวมทั้งส่วนประกอบของคอมพิวเตอร์ ซึ่งเป็นส่วนที่เป็นอิเล็กทรอนิกส์, จักรกลไฟฟ้า, ทรานซิสเตอร์ มอเตอร์ และอื่น ๆ ที่ประกอบกันขึ้นเป็นเครื่องคอมพิวเตอร์ ซึ่งได้แก่

- **ส่วนนำข้อมูลเข้า** หรืออีกนัยหนึ่งคือ ส่วนรับข้อมูลจากมนุษย์สู่เครื่องคอมพิวเตอร์ ที่สำคัญและนิยมใช้ในปัจจุบัน ได้แก่

(1) แป้นพิมพ์ (Keyboard) มีไว้สำหรับให้ผู้ใช้ติดต่อกับคอมพิวเตอร์ ใส่ข้อมูลหรือคำสั่งเพื่อให้คอมพิวเตอร์ทำงานตามที่ต้องการ

(2) หน่วยขับจานบันทึก (Disk Drive) หมายถึงกลไกที่ใช้หมุนจานบันทึกให้ผ่านหัวอ่านหรือหัวบันทึก (Read/Write) ทำให้สามารถนำข้อมูลที่บันทึกอยู่ในจานบันทึกมาประมวลผลได้ หากต้องการจะบันทึกข้อมูลใหม่ลงไปก็สามารถบันทึกได้เช่นเดียวกัน

(3) เครื่องอ่านซีดีรอม (CD-ROM) ใช้สำหรับอ่านแผ่นซีดี-รอมอย่างเดียว เว้นแต่เครื่องอ่านและเขียน ซีดี (CD) สามารถทั้งอ่านและบันทึกข้อมูลลงในแผ่นซีดี (CD)

(4) เครื่องอ่านเลเซอร์ดิสก์ (Laser Disk) เหมือนกับซีดี-รอม แต่ใช้แสงเลเซอร์ (Laser) ในการอ่านและเขียนข้อมูล

(5) จอภาพ (Monitor) ส่วนใหญ่ใช้สำหรับแสดงผล เว้นแต่จอภาพแบบสัมผัส (Touch Screen) สามารถใช้รับข้อมูลได้โดยใช้ร่วมกับปากกาแสง (Light Pen) โดยใช้ปากกาแสงเขียนเป็นภาพหรือข้อความใด ๆ ก็ได้บนจอภาพ คอมพิวเตอร์จะรับเป็นข้อมูลแล้วนำไปเก็บและประมวลผลได้เช่นเดียวกับใช้แป้นพิมพ์หรือเครื่องชี้บนจอภาพ (Mouse)

(6) เครื่องชี้บนจอภาพ (Mouse) ใช้รับคำสั่งที่ใช้ในการควบคุมการทำงานของโปรแกรมและเครื่อง

(7) เครื่องกราดภาพ (Scanner) ใช้อ่านภาพหรือตัวอักษรลงในคอมพิวเตอร์ มีทั้งแบบอ่านภาพเป็นสี หรือขาว-ดำ มีทั้งแบบตั้งโต๊ะคล้ายเครื่องถ่ายเอกสารแต่เล็กกว่า อ่านได้พร้อมกันทั้งแผ่น (A4) หรือใหญ่กว่าเล็กน้อย ส่วนแบบมือถือเป็นเครื่องขนาดเล็ก ใช้มือถือแล้วลากไปตามเอกสาร โปรแกรมจะนำไปตัดต่อภาพเอง เครื่องสแกนเนอร์ได้พัฒนาจนสามารถเป็น OCR (Optical Character Reader) คือสามารถอ่านตัวอักษรลายมือที่ไม่หวัดมาก ซึ่งเครื่องอ่านเป็นรูปภาพ ให้กลายเป็นข้อมูลตัวอักษรโดยที่ไม่ต้องพิมพ์

(8) โมเด็ม (Modem : Modulator-Demodulator) เป็นอุปกรณ์สื่อสารข้อมูลชนิดหนึ่ง ซึ่งแปลงสัญญาณจากเครื่องคอมพิวเตอร์ให้เป็นสัญญาณที่ส่งผ่านไปตามสายโทรศัพท์ได้ และแปลงสัญญาณที่มาจากสายโทรศัพท์ให้กลับมาเป็นสัญญาณสำหรับเครื่องคอมพิวเตอร์

(9) อุปกรณ์ต่อพ่วง (Fax Peripheral) เป็นอุปกรณ์ที่ใช้กับเครื่องคอมพิวเตอร์ ใช้บัตรสอดและสามารถทำงานในรูปโทรสาร (Fax) ได้

(10) แผ่นวงจรระบบ Lan (Lan Card) เป็นแผงวงจรที่นำมาเสียบเพิ่มในเครื่องคอมพิวเตอร์ เพื่อทำหน้าที่เชื่อมโยงสัญญาณเครือข่ายในระบบ Lan (Local Area Network ข่ายงานบริเวณเฉพาะที่)

(11) อุปกรณ์แยกสัญญาณ HUB เป็นอุปกรณ์แยกสัญญาณเครือข่ายคล้ายชุมสายโทรศัพท์

(12) สายสัญญาณ ใช้เชื่อมโยงข้อมูลในระบบเครือข่าย มีหลายขนาดตามความเร็วตั้งแต่ สายโทรศัพท์, สายระบบ Lan, สาย Lease Line (สายเช่าสัญญาณ) ความเร็วเป็นไปตามวงเงินที่เช่า คือ 6, 9, 19.2, 64, 512, 2048 Kbps, สายเคเบิ้ลใต้น้ำ, สายใยแก้วนำแสง (Fiber Optic)

(13) เครื่องสำรองไฟฟ้า (UPS : Uninteruptable Power Supply) เป็นเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าให้คงที่ กรณีไฟฟ้าดับ ขัดข้อง เครื่องสำรองไฟฟ้าจะจ่ายไฟฟ้าสำรองให้ จึงมีเวลาพอที่จะรักษาข้อมูลและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้อง เป็นต้น

- **ส่วนประมวลผล** เป็นส่วนสำคัญที่สุดของระบบคอมพิวเตอร์ เปรียบเสมือนมันสมองของคอมพิวเตอร์ เพราะประกอบไปด้วยหน่วยความจำ หน่วยคำนวณและหน่วยควบคุม ส่วนนี้นิยมเรียกว่า ซีพียู (CPU : Central Processing Unit) หน่วยประมวลผลกลางมีส่วนประกอบที่สำคัญดังนี้

(1) ชิป (Chip) คือแผ่นวงจรรวม (Integrated Circuit หรือ IC) ที่มีขนาดเล็กมาก ส่วนมากจะใช้ซิลิคอน (Silicon) ซึ่งสามารถบรรจุองค์ประกอบหรือชิ้นส่วนอิเล็กทรอนิกส์ (ส่วนประกอบของชิปบางชนิดจะติดตั้งอย่างถาวร เรียกว่า รอมชิป (Rom Chip) หน่วยประมวลผลกลางเป็นที่บรรจุแผ่นวงจรรวม คือชิปซึ่งถือว่าเป็นสมองของคอมพิวเตอร์ และปฏิบัติตามคำสั่งของภาษาเครื่องซึ่งได้รับมาจากโปรแกรมคอมพิวเตอร์

(2) รอม (ROM : Read Only Memory) คือหน่วยความจำลักษณะหนึ่งที่ใช้สำหรับอ่านข้อมูลออกมาได้อย่างเดียวเท่านั้น จะบันทึกข้อมูลลงไปไม่ได้ หน่วยความจำส่วนนี้จะเติมคำสั่งและข้อมูลพื้นฐานที่คอมพิวเตอร์จะต้องใช้งานเอาไว้อย่างถาวร ไม่สามารถเปลี่ยนแปลงหรือลบทิ้งได้ แม้ปิดสวิตช์ที่เครื่องคอมพิวเตอร์ ข้อมูลในรอมจะไม่สูญหายไป

(3) แรม (RAM : Random Access Memory) คือหน่วยความจำที่อยู่ในเครื่องคอมพิวเตอร์ วัดขนาดข้อมูลกันเป็นกิโลไบต์ (Kilobyte), เมกะไบต์ (Megabyte) หรือกิกะไบต์ (Gigabyte) ทำงานได้รวดเร็วแบบเข้าถึงโดยสุ่มคือเข้าถึงหน่วยความจำทุกจุดได้โดยใช้เวลาในการเข้าถึงเท่ากันหมด ไม่ต้องตั้งต้นใหม่ทุกครั้งแล้วรอไปตามลำดับ RAM เป็นพื้นที่ที่จะนำข้อมูลโปรแกรมจากแผ่นดิสก์หรือฮาร์ดดิสก์มาเตรียมไว้ชั่วคราวเพื่อให้

CPU ใช้ในการประมวลผล เครื่องใดมี RAM มากเหมือนมีโต๊ะทำงานใหญ่ สามารถนำแฟ้มเอกสารและอุปกรณ์ต่าง ๆ มาวางบนโต๊ะได้ การทำงานย่อมสะดวกรวดเร็ว แต่ถ้าปิดเครื่องความจำบน RAM ก็จะหายไป โปรแกรมสำเร็จรูปปัจจุบันมักจะมีขนาดใหญ่และต้องการใช้เนื้อที่ในแรมมาก หลายโปรแกรมเจาะจงว่าจะต้องใช้กับคอมพิวเตอร์ที่มี RAM จำนวนมาก คอมพิวเตอร์ที่มี RAM ต่ำ อาจแก้ไขได้ด้วยวิธีการเพิ่ม RAM

- หน่วยความจำสำรอง (Storage) เป็นอุปกรณ์ที่ใช้เพื่อเก็บข้อมูลที่มีจำนวนมากไว้ เพื่อนำออกมาประมวลผลเมื่อต้องการ ที่สำคัญได้แก่

(1) จานบันทึก (Disk) หมายถึงอุปกรณ์เก็บข้อมูลมีลักษณะหลายชนิด ดังนี้

1.1 จานบันทึกอ่อน (Diskette) เป็นสื่อบันทึกข้อมูลที่นิยมใช้เนื่องจากพกพาไปใช้งานได้อย่างสะดวก Diskette เป็นจานแม่เหล็กแผ่นบาง ๆ แผ่นเดียวบรรจุอยู่ภายในซอง Diskette ที่ใช้กับไมโครคอมพิวเตอร์ มี 2 ขนาดคือ 5.25 x 5.25 นิ้วและ 3.5 x 3.5 นิ้ว ขนาด 3.5 x 3.5 นิ้ว นิยมใช้กันมากกว่าแบบแรกเพราะมีความจุข้อมูลได้สูงกว่าและเก็บรักษาได้ง่ายกว่า

1.2 จานบันทึกแข็ง (Hard Disk) จะบรรจุอยู่ในกล่องพร้อมกับหน่วยขับ (Drive) แล้วเก็บอยู่ภายในตัวเครื่อง หรืออาจจะติดอยู่ภายนอกก็ได้ สามารถเก็บข้อมูลได้จำนวนมากมีขนาดเป็นกิโลไบต์ (KB), เมกะไบต์ (MB), กิกะไบต์ (GB)

1.3 จานบันทึกอัดแน่น (CD : Compact Disk) เป็นสื่อที่ใช้บันทึกข้อมูลจะเป็นข้อความ ภาพ หรือเสียงก็ได้ รูปลักษณะทั่วไปเหมือนจาน CD ที่บรรจุเพลง มีเส้นผ่าศูนย์กลางขนาด 4.72 นิ้ว บรรจุข้อมูล 600 MB หรือประมาณ 400 เท่า ของจานบันทึกขนาด 3.5 นิ้ว นิยมใช้ในระบบเครือข่าย ทำให้สะดวกสำหรับผู้ใช้คอมพิวเตอร์ตามสาย On line

นอกจากนี้ยังมีจานบันทึกที่นำมาใช้กับคอมพิวเตอร์เครื่องใหญ่ (Mainframe) ที่เรียกว่า

- ชุดจานบันทึก (Disk Pack) ซึ่งจะมีแกนยึดติดกันตรงกลาง
- จานแสงหรือจานเลเซอร์ (Optical or Laser Disk)
- จานวีดีทัศน์ (Vedio Disk)

- จานบันทึกอัดแน่น (Compact Disk)

แผ่นดิสก์ Disk ที่ใช้ในปัจจุบันมีลักษณะเป็นจานแม่เหล็ก (Magnetic Disk) คือโลหะที่มีลักษณะเหมือนจาน เคลือบผิวด้วยไอออนออกไซด์ ทำให้เกิดกระแสแม่เหล็กบนผิวหน้าของจานแม่เหล็กจะมีสองขั้ว คือขั้วบวกและขั้วลบ สถานะสองขั้วนี้เองที่นำมาใช้แทนรหัสเลขฐานสอง (คือ 0 กับ 1) และทำให้บันทึกข้อมูลซึ่งแตกออกเป็นดิจิต (Digit) ได้อย่างง่ายดาย นับเป็นสื่อเก็บข้อมูลที่ได้รับความนิยมมากที่สุด ในปัจจุบันที่ใช้กับไมโครคอมพิวเตอร์ จานบันทึกเหล่านี้จะต้องนำมาจัดรูปแบบการบันทึก (Format) คือการกำหนดแทร็ก (Track) และเซ็กเตอร์ (Sector) ก่อนจึงจะนำไปใช้ได้ การจัดเก็บข้อมูลในดิสก์จะจัดแบ่งการเก็บข้อมูลออกเป็นเซ็กเตอร์และแทร็ก ใน 1 แทร็กประกอบด้วย 17 เซ็กเตอร์ ใน 1 เซ็กเตอร์ประกอบด้วย 256 อักขระ (Characters) ซึ่งในส่วนต่าง ๆ เหล่านี้สามารถจัดเก็บหรือซ่อนข้อมูลต่าง ๆ ได้มากมายแม้จะเป็น Disk ที่เสียหรือมีปัญหา ก็ยังสามารถกู้ข้อมูลได้โดยห้องทดลอง

- **ส่วนนำผลลัพท์ออก** เป็นเครื่องอุปกรณ์ที่ทำหน้าที่ติดต่อระหว่างเครื่องคอมพิวเตอร์กับมนุษย์ คือแสดงผลลัพท์ทางจอภาพ หรือเครื่องพิมพ์อัตโนมัติให้มนุษย์อ่านได้ โดยวิธีนำผลลัพท์จากส่วนประมวลผล ซึ่งเป็นรหัสภายในเครื่องแล้วแปลเป็นภาษาที่มนุษย์เข้าใจ เช่น ในประเทศไทยก็ออกแบบระบบให้แปลเป็นภาษาไทย แสดงออกมาทางจอภาพ หรือพิมพ์ออกทางเครื่องพิมพ์อัตโนมัติ ส่วนนำผลลัพท์ออกที่สำคัญคือ

(1) จอภาพ (Monitor) หมายถึง จอภาพของเครื่องคอมพิวเตอร์หรือเครื่องปลายทาง (Terminal) จอภาพนั้นมีหลายชนิด เช่น สีเดียว, หลายสี มีหลายขนาด จอภาพที่ดีจะต้องมีความถี่สูง ทำให้ได้ภาพที่นิ่งสนิท (Non-Interlaced) มีความคมชัดสูง (High Resolution) ขนาดมาตรฐานจะมีความละเอียด 1,024 คูณ 768 จุด

(2) เครื่องพิมพ์ (Printer) หมายถึง อุปกรณ์เครื่องพิมพ์ที่รับสัญญาณตรงจากเครื่องคอมพิวเตอร์ เพื่อพิมพ์งานออกมาเป็นข้อความและภาพลงบนกระดาษหรือวัตถุอื่นในประเภทเดียวกัน เครื่องพิมพ์ที่ใช้ในปัจจุบันมีหลายประเภท เช่น

2.1 แบบกระทบ (Impact Printer) เป็นเครื่องพิมพ์ชนิดที่พิมพ์ข้อความลงบนกระดาษ โดยใช้ม้อนตอกผ่านผ้าหมึกพิมพ์ลงบนกระดาษ ทำให้เกิดเป็นรูปตัวอักษรอักขระต่าง ๆ มีหลายชนิด เช่น

- เครื่องพิมพ์แบบจุด (Dot Matrix) เครื่องพิมพ์ที่มีหัวเข็มอยู่ภายในขณะทำงาน ใช้เข็มตอกออกมากระทบผ้าหมึกไปติดบนกระดาษ

- เครื่องพิมพ์แบบจานอักขระ (Daisy Wheel) เป็นเครื่องพิมพ์ที่ใช้แบบตัวอักษรจัดเรียงไว้บนแป้นพิมพ์ มีลักษณะเป็นจานกลมขณะทำงาน ตัวอักษรจะหมุนไปตรงกับจุดที่เคาะทำให้ตัวอักษรประทับที่ผ้าพิมพ์ไปติดบนกระดาษ

2.2 แบบไม่กระทบ (Non-Impact Printer) เป็นเครื่องพิมพ์ชนิดที่ไม่มีการกระทบตัวพิมพ์ลงบนผ้าหมึกแบบเครื่องพิมพ์แบบกระทบ

- เครื่องพิมพ์แบบฉีดหมึก (Ink Jet) ทำหน้าที่ฉีดหมึกออกเป็นตัวอักษร หรือภาพ

- เครื่องพิมพ์เลเซอร์ (Laser) เครื่องพิมพ์แบบที่ใช้ลำแสงเลเซอร์ในการสร้างภาพและถ่ายทอดลงสู่กระดาษด้วยวิธีการทางอิเล็กทรอนิกส์

2.1.3.2 ซอฟท์แวร์ (Software)

หมายถึง โปรแกรมคอมพิวเตอร์ (Program) ฐานข้อมูลเอกสารประกอบ และเอกสารอื่น ๆ เช่น คู่มือผู้ใช้, คู่มือติดตั้งโปรแกรม, คู่มือปฏิบัติการ, คู่มือการใช้เครื่องแผนผังวงจร เป็นต้น ซอฟท์แวร์ มีอยู่มากมายหลายประเภท เช่น

- ระบบปฏิบัติการซึ่งทำหน้าที่ควบคุมดูแลระบบคอมพิวเตอร์ทั้งระบบ

- ซอฟท์แวร์อรรถประโยชน์ซึ่งช่วยทำงานประจำปลีกย่อยต่าง ๆ ให้ผู้ใช้

- ตัวแปลภาษาซึ่งใช้ในการแปลโปรแกรมที่เขียนขึ้นด้วยภาษาคอมพิวเตอร์ระดับสูงให้เป็นภาษาเครื่องหรือภาษาระดับต่ำ

- ซอฟท์แวร์จัดการฐานข้อมูล ซึ่งใช้กำหนดลักษณะของบันทึกข้อมูลและค้นหาข้อมูล

- ซอฟท์แวร์จัดการระบบเครือข่าย ซึ่งใช้ในการควบคุมระบบเครือข่ายการสื่อสาร และควบคุมการประสานงานระหว่างอุปกรณ์ต่าง ๆ ในเครือข่าย

- ซอฟท์แวร์ประยุกต์ ซึ่งทำงานด้านต่าง ๆ ตามที่ผู้ใช้ต้องการ

การเขียนโปรแกรมเป็นการถ่ายทอดคำสั่งให้อยู่ในรูปแบบของภาษาที่คอมพิวเตอร์รับไปปฏิบัติได้ ภาษาเครื่องเป็นภาษาเดียวที่คอมพิวเตอร์เข้าใจและทำงานได้ ส่วนภาษาอื่น ๆ นั้น คอมพิวเตอร์ไม่เข้าใจและจำต้องแปลโปรแกรมนั้นจากภาษาที่ใช้เป็นภาษาเครื่องก่อน ภาษาสำหรับใช้เขียนโปรแกรมคอมพิวเตอร์ที่ช่วยให้เขียนคำสั่งโดยไม่ต้องรู้โครงสร้างและการทำงานภายในของคอมพิวเตอร์ เรียกว่า ภาษาระดับสูง (High-Level Language) ภาษาระดับสูงที่รู้จักกันดี ได้แก่ ภาษาเบสิก (BASIC), โคบอล (COBOL), ฟอร์แทรน (FORTRAN), ปาสคาล (PASCAL) ซี (C) การเขียนโปรแกรมอาจจะใช้ภาษาแอสเซมบลี (Assembly Language) หรือบางครั้งเรียกว่า ภาษาระดับต่ำ (Low-Level Language) ซึ่งคำสั่งจะตรงกับคำสั่งภาษาเครื่อง เมื่อเขียนโปรแกรมเป็นภาษาแอสเซมบลีแล้ว จะต้องใช้ตัวแปลภาษาแอสเซมบลีให้เป็นภาษาเครื่องก่อนจึงจะนำไปสั่งให้คอมพิวเตอร์ทำงานได้ การเขียนโปรแกรมภาษาแอสเซมบลีนี้ ผู้เขียนโปรแกรมจะต้องมีความรู้เกี่ยวกับโครงสร้างและการทำงานภายในเครื่องคอมพิวเตอร์เป็นอย่างดี ทำให้ไม่ค่อยมีผู้นิยมใช้ภาษานี้มากนัก ซอฟท์แวร์ที่เขียนโดยภาษาระดับต่ำหรือภาษาระดับสูงรวมเรียกว่า รหัสต้นฉบับ (Source Code) เพื่อให้คอมพิวเตอร์สามารถทำงานรับคำสั่งได้ รหัสต้นฉบับจะต้องถูกแปลเป็นภาษาเครื่องสำหรับใช้งานโดยหน่วยประมวลผลกลาง ซึ่งเรียกว่า Object Code

โปรแกรมคอมพิวเตอร์ ได้แก่ คำสั่งหรือชุดคำสั่งที่นำมาใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือให้ได้รับผลอย่างหนึ่งอย่างใด โปรแกรมอาจบรรจุไว้อย่างถาวรในเครื่องคอมพิวเตอร์ แผงวงจรรวม เทปแม่เหล็ก แผ่นดิสก์หรือบัตรเจาะรู (Punched Card) เป็นต้น โปรแกรมคอมพิวเตอร์ทั่วไปมี 2 ประเภทหลักคือ

(1) โปรแกรมควบคุม หรือโปรแกรมระบบปฏิบัติการ (Control or Operation System Program) โปรแกรมนี้เป็นชุดของโปรแกรมที่ทำหน้าที่ควบคุมดูแลและจัดการระบบคอมพิวเตอร์ทั้งระบบ เปรียบเสมือนผู้จัดการระบบที่อยู่กลางระหว่างผู้ใช้กับเครื่อง ช่วยให้ผู้ใช้ ใช้งานคอมพิวเตอร์ได้ง่ายขึ้น เช่น การบรรจุข้อมูล (Loading) การเก็บรักษาข้อมูล (Saving) การลบข้อมูล (Deleting) โปรแกรมควบคุมติดตั้งในเครื่องคอมพิวเตอร์เพื่อให้สามารถใช้โปรแกรมประยุกต์สั่งเครื่องทำงานตามต้องการต่อไป

(2) โปรแกรมประยุกต์ (Application Program) เป็นโปรแกรมที่ผู้ใช้คุ้นเคยมากที่สุด และโปรแกรมนี้ทำให้หน่วยประมวลผลกลาง (Microprecessor) ทำงานตามที่ต้องการ เช่น โปรแกรม Microsoft Word ทำให้คอมพิวเตอร์มีความสามารถในการพิมพ์และการนำรูปภาพมาจัดแต่งร่วมกับข้อความ โปรแกรม Pac Man ทำให้สามารถเล่นเกมส์ที่มีทั้งภาพและเสียงได้

การเขียนโปรแกรมเป็นการถ่ายทอดคำสั่งให้อยู่ในรูปแบบภาษาที่คอมพิวเตอร์รับไปปฏิบัติได้ ผู้เขียนโปรแกรมจะต้องวิเคราะห์ปัญหาหรืองานที่ต้องการใช้คอม-พิวเตอร์ จากนั้นจึงเรียงลำดับขั้นตอนที่คอมพิวเตอร์จะต้องคิดแล้วจึงเปลี่ยนขั้นตอนนั้นเป็นคำสั่งในภาษาที่ต้องการโดยต้องพิจารณาถึงความสามารถของฮาร์ดแวร์ที่จะนำโปรแกรมไปใช้ด้วย ลำดับของการทำงานอย่างใดอย่างหนึ่งที่เขียนเป็นขั้นตอนให้เข้าใจและทำตามได้สะดวก หรือลำดับการแก้ไขปัญหาด้านโปรแกรมเรียกว่าขั้นตอนวิธี (Algorithm) การพัฒนารูปแบบของโปรแกรมอาจจะต้องทำผังงาน (Flow Chart) ซึ่งเป็นผังที่แสดงการเคลื่อนที่ข้อมูลไปตลอดคำสั่งและเครื่องมือสำคัญที่ช่วยให้เข้าใจขั้นตอนการทำงานของโปรแกรมได้ชัดเจน

2.1.3.3 **พีเพิลแวร์ (Peopleware) บุคลากรทางคอมพิวเตอร์**

การใช้เครื่องคอมพิวเตอร์ในการประมวลผลนั้น จะต้องอาศัยบุคลากรหลายประเภทเข้าดำเนินการซึ่งจะมีระดับความรู้ ความเข้าใจและความชำนาญแตกต่างกันไป ดังจะกล่าวถึงบุคลากรประเภทต่าง ๆ ดังนี้ :-

(1) ผู้จัดการทั่วไป (General Manager) ตำแหน่งนี้มีชื่อเรียกเป็นหลายแบบ เช่น ผู้อำนวยการ, ผู้จัดการ, หัวหน้าฝ่าย, หัวหน้าแผนก ทั้งนี้ขึ้นอยู่กับปริมาณงานของหน่วยงานนั้น ๆ หรือความเหมาะสมในด้านอื่น ๆ อย่างไรก็ตามหัวหน้างานนั้นถือเป็นบุคคลที่สำคัญที่สุด มีหน้าที่รับผิดชอบงานทั้งหมด ซึ่งอาจเริ่มตั้งแต่การหาเครื่องคอมพิวเตอร์มาติดตั้งให้มีขนาดเหมาะสมกับงาน มีความรับผิดชอบดูแลบุคคลที่อยู่ภายใต้บังคับบัญชาในทุกระดับหน้าที่ ประสานงานระหว่างบุคคลในหน้าที่ต่าง ๆ ติดต่ออย่างใกล้ชิดกับนักวิชาการและหน่วยงานที่เกี่ยวข้อง

(2) นักวิเคราะห์ระบบ (System Analyst) หมายถึง ผู้มีหน้าที่ดูแลรับผิดชอบระบบงาน เริ่มตั้งแต่การวิเคราะห์และการออกแบบระบบงาน ระบบข้อมูล ตลอดจนผู้ประสานงานระหว่างผู้ใช้เครื่องกับหน่วยงานคอมพิวเตอร์จะต้องเป็นผู้มีความรู้ความสามารถเกี่ยว

กับระบบงานและโปรแกรมเป็นอย่างดี มีความรู้กว้างขวางในวงการต่าง ๆ โดยเฉพาะอย่างยิ่งด้านธุรกิจ เช่น บัญชี การตลาด การบริหาร เป็นต้น เพราะจะต้องใช้วิธีการเหล่านี้ในการวิเคราะห์ หรือการวางแผนรายงาน เพื่อให้บรรลุผลที่ดีกว่า นอกจากนั้นจะต้องเป็นผู้มีความคิดสร้างสรรค์และจะต้องรู้จักกำหนดขั้นตอนในการทำงานว่าขั้นตอนใดควรทำอย่างไร จัดเก็บข้อมูลไว้ในสื่อชนิดใด จัดพิมพ์อย่างไร การประมวลผลจะให้ระบบใดมีวิธีการอย่างไรที่จะให้เป็นไปตามระบบนั้น ๆ

(3) ผู้เขียนโปรแกรม (Programmer) หมายถึง ผู้ที่จะรับช่วงานจากนักวิเคราะห์ ระบบมาช่วยเขียนคำสั่งให้เครื่องทำงานอย่างเป็นขั้นตอนด้วยภาษาใดภาษาหนึ่งที่คอมพิวเตอร์จะสามารถนำไปแปลเป็นภาษาเครื่องได้ บุคคลผู้นี้จะต้องเป็นผู้ที่มีความรู้ในเรื่องกฎเกณฑ์ของภาษาคอมพิวเตอร์มาแล้วเป็นอย่างดี

(4) วิศวกรรมคอมพิวเตอร์ (Computer Engineer) เป็นผู้ที่จะต้องมีความรู้ทางด้านเทคนิคสูงและมีทักษะที่ได้รับการฝึกหัดมานานปี เพราะจะต้องรับผิดชอบระบบการทำงานของเครื่อง การบำรุงรักษา ระบบไฟและอุปกรณ์ต่าง ๆ เป็นต้น โดยปกติเครื่องคอมพิวเตอร์จะต้องได้รับการตรวจสอบเป็นครั้งคราว เพราะมิฉะนั้นจะก่อให้เกิดปัญหาเกิดความผิดพลาดในการประมวลผลการแก้ไขซ่อมบำรุงจะต้องทำได้ทันท่วงที เพื่อมิให้เสียเวลาการทำงานมากเกินไป

(5) เจ้าหน้าที่จัดการฐานข้อมูล (Data Base Administrator) ทำหน้าที่สร้างและควบคุมการใช้ฐานข้อมูลโดยการออกแบบลักษณะและวิธีจัดเก็บข้อมูลตามความประสงค์ของผู้ใช้ รวมทั้งวางข้อกำหนด ตลอดจนถึงระบบความปลอดภัยของฐานข้อมูล ดังนั้นจะต้องมีความรู้ในการออกแบบและการจัดการฐานข้อมูล รวมถึงโปรแกรมที่ใช้สำหรับจัดการฐานข้อมูลด้วย

(6) พนักงานควบคุมเครื่อง (Operator) คือผู้ที่จะบังคับและควบคุมดูแลเครื่องคอมพิวเตอร์ด้วยการกดปุ่มต่าง ๆ บนแผงหน้าปัด อันที่จริงเครื่องคอมพิวเตอร์สมัยใหม่มีวิวัฒนาการที่ก้าวหน้าไปมาก จนทำให้พนักงานควบคุมเครื่องเกือบจะไม่ต้องมีทักษะอย่างใดเป็นพิเศษ เพียงแต่คอยดูแลว่ามีสิ่งใดทำงานผิดปกติหรือไม่มีสิ่งใดขัดข้องหรือไม่ และถ้าจำเป็นอาจสามารถตรวจข้อผิดพลาดเล็ก ๆ น้อย ๆ และทำการแก้ไขได้

(7) ผู้ควบคุมการปฏิบัติการ (Operation Supervisor) จะเป็นผู้ดูแลทั่วไปภายในห้องคอมพิวเตอร์เปรียบเสมือนคนคุมงาน (Foreman) กล่าวคือจัดงานให้แต่ละคนทำ ไม่ก้าวก่ายกัน ควบคุมดูแลรักษาสื่อข้อมูล เช่น เทป จานบันทึก ให้อยู่ในสภาพที่จะใช้งานได้ดีทันที

(8) พนักงานเตรียมข้อมูล หมายถึง พนักงานที่มีหน้าที่ในการใช้รหัส และจัดเตรียมข้อมูลเหล่านี้ลงในสื่อข้อมูลชนิดต่าง ๆ เช่น เทป จานบันทึก ฯลฯ เพื่อให้พร้อมที่จะส่งเข้าเครื่องต่อไป พนักงานเหล่านี้จะต้องมีความชำนาญ เช่นเดียวกับพนักงานพิมพ์ดีด

2.1.3.4 ระบบเครือข่ายอินเตอร์เนต (Internet)

อินเตอร์เนต คือระบบเครือข่าย (Network) ที่เชื่อมโยงเครือข่ายมากมายและเชื่อมต่อกันทั่วโลก โดยมีมาตรฐานการรับส่งข้อมูลแบบเดียวกัน อินเตอร์เนตจึงเป็นแหล่งข้อมูลขนาดใหญ่ที่มีข้อมูลในทุก ๆ ด้าน ให้ผู้ที่สนใจเข้าไปค้นคว้าหามาใช้ได้อย่างสะดวกรวดเร็วและง่ายดาย (สิทธิชัย ประสานวงศ์, 2540 : 3) เครือข่ายอินเตอร์เนตเกิดขึ้นจากเจ้าหน้าที่สังกัดกระทรวงกลาโหมของประเทศสหรัฐอเมริกา ได้ใช้คอมพิวเตอร์จำนวน 4 เครื่องสร้างระบบเครือข่ายคอมพิวเตอร์ขึ้นมา เพื่อเป็นระบบเครือข่ายที่ไม่สามารถถูกทำลายได้ หากเป็นระบบที่ใช้แบบศูนย์กลางอย่างเดิมแล้ว อาจถูกทำลายระบบหรือโปรแกรมคอมพิวเตอร์ได้ง่าย ซึ่งจะก่อให้เกิดผลเสียหายต่อความมั่นคงของประเทศ

ความหมายของเครือข่ายอินเตอร์เนต คือการนำเอาเครือข่ายย่อย ๆ ของคอมพิวเตอร์เชื่อมต่อเข้าด้วยกัน โดยอาศัยการสื่อสารโทรคมนาคม เช่น โทรศัพท์ ซึ่งส่งผลให้ผู้ใช้คอมพิวเตอร์สามารถสื่อสารกันได้ง่าย เพียงสมัครเป็นสมาชิกจากผู้ให้บริการ (ISP) จะได้รหัสประจำตัว (ID Number) และเมื่อได้กำหนดรหัสผ่านแล้วสามารถเข้าสู่ระบบอินเตอร์เนต ทำให้สามารถทราบข้อมูลได้ทั่วโลก หรือใส่ข้อมูลแล้วก็จะทำให้ข้อมูลแพร่หลายไปได้เช่นเดียวกัน

การเจริญเติบโตของจำนวนผู้ใช้อินเตอร์เนตในด้านต่าง ๆ ไม่ว่าจะเป็นในด้านเศรษฐกิจ การเมือง หรือสังคม ส่งผลให้อาชญากรคอมพิวเตอร์อาศัยระบบอินเตอร์-เนตก่ออาชญากรรมได้ง่ายยิ่งขึ้น ใช้ข้อมูลในอินเตอร์เนตมาเอื้ออำนวยก่อให้เกิดประโยชน์ในด้านต่าง ๆ มากขึ้น เช่น มีการจัดตั้งมหาวิทยาลัยสำหรับผู้ที่สนใจจะลักลอบเข้าถึงระบบคอมพิวเตอร์

ของผู้อื่นขึ้นโดยผู้ที่ต้องการศึกษาเทคนิคและวิธีการลักลอบเข้าถึง สามารถเข้าไปลงทะเบียนเรียนทางอินเตอร์เนตได้ เป็นต้น

2.2 พื้นฐานทางด้านกฎหมายของต่างประเทศ

ปัจจุบันประเทศที่เจริญก้าวหน้าทางเทคโนโลยี มีกฎหมายเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ใช้เป็นการเฉพาะ โดยมีการจัดตั้งหน่วยงานสืบสวนสอบสวนและป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ ในประเทศสหรัฐอเมริกาและประเทศในภูมิภาคยุโรป เช่น เบลเยี่ยม ฟินแลนด์ ฝรั่งเศส เยอรมัน อิตาลี เนเธอร์แลนด์ สวีเดน และอังกฤษ เป็นต้น ส่วนในภูมิภาคเอเชียแปซิฟิค เช่น ออสเตรเลีย นิวซีแลนด์ ญี่ปุ่น ฮ่องกง สิงคโปร์และมาเลเซีย (ธรรมศักดิ์ วิชารยะ, 2540 : 36)

2.2.1 กฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ของประเทศสหรัฐอเมริกา

การกระทำผิดอาญาที่มีคอมพิวเตอร์เข้ามาเกี่ยวข้องนั้น เป็นปัญหาทวีความรุนแรงขึ้น โดยเฉพาะในประเทศสหรัฐอเมริกาที่เป็นต้นคิดของการใช้เครื่องคอมพิวเตอร์ ดังจะเห็นได้จากเหตุผลในการประกาศใช้กฎหมายอาชญากรรมคอมพิวเตอร์ของมลรัฐฟลอริด้า ซึ่งประกาศว่า

รัฐสภาได้ค้นพบและขอประกาศว่า

(1) การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์เป็นปัญหาที่กำลังก่อตัวเพิ่มขึ้นทั้งในภาครัฐบาลและภาคเอกชน

(2) การกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้ก่อให้เกิดความสูญเสียที่มีมูลค่ามหาศาลต่อสาธารณชน ซึ่งความเสียหายในเหตุการณ์แต่ละครั้งของการกระทำความผิดมีแนวโน้มที่จะสูงมากไปกว่าความเสียหายที่เกี่ยวข้องกับเหตุการณ์ในแต่ละครั้งของอาชญากรรมโจรผู้ดีอื่น ๆ

(3) โอกาสที่จะเกิดอาชญากรรมดังกล่าวต่อสถาบันการเงิน โครงการต่าง ๆ ของรัฐบาล เอกสารของทางราชการ รัฐวิสาหกิจอื่น ๆ โดยผ่านทางการนำข้อมูลเท็จเข้าไปในระบบคอมพิวเตอร์ การใช้เครื่องอำนวยความสะดวกทางคอมพิวเตอร์โดยไม่มีอำนาจ การแก้ไข

เปลี่ยนแปลงหรือทำลายข่าวสารหรือแฟ้มข้อมูลทางคอมพิวเตอร์ และการลักขโมยเอกสารทางการเงิน ข้อมูลและทรัพย์สินอื่น ๆ มีสูงมาก

(4) ในขณะที่รูปแบบต่าง ๆ ของการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์อาจถือได้ว่า เป็นเรื่องของความผิดอาญาที่ตั้งอยู่บนพื้นฐานของบทบัญญัติทางกฎหมายที่มีอยู่แล้วโดยทั่วไป แต่ก็นับว่าเป็นที่เรียกร้องกันและเป็นเรื่องที่เหมาะสม ที่จะพิจารณาว่าควรที่จะมีกฎหมายใหม่มาผนวกหรือเสริมเพิ่มเติม เพื่อที่จะห้ามการใช้เครื่องคอมพิวเตอร์ในทางที่ผิดรูปแบบต่าง ๆ

การกระทำผิดอาญาเกี่ยวกับคอมพิวเตอร์ อาจถูกดำเนินคดีได้โดยอาศัยบทบัญญัติของกฎหมายที่มีอยู่แล้วทั่ว ๆ ไป โดยไม่ต้องค้นหาลึกลงไปถึงเรื่องทางเทคโนโลยี แต่ก็มีการกระทำความผิดอีกเป็นจำนวนมากที่พอจะเรียกได้ว่าแตกต่างจากอาชญากรรมทั่วไป เมื่อเทียบกันในเรื่องของผู้กระทำผิด สภาพแวดล้อม รูปแบบของทรัพย์สินที่สูญเสีย รูปแบบของการกระทำมาตรฐานของการนับเวลาและสภาพทางภูมิศาสตร์ ซึ่งแสดงว่าการกระทำความผิดชนิดนี้มีลักษณะเฉพาะที่ต้องอาศัยความสามารถและการกระทำที่พิเศษแตกต่างจากเรื่องทั่ว ๆ ไป เครื่องคอมพิวเตอร์กำลังก่อให้เกิดอาชญากรรมใหม่ ๆ เหล่านี้ขึ้นในสังคมของเรา (Colin Tapper, 1987 : 5)

ในประเทศสหรัฐอเมริกา มีกฎหมายทั้งในระดับรัฐบาลกลางและระดับมลรัฐที่สำคัญ ได้แก่

(1) กฎหมายรัฐบาลกลางแห่งสหรัฐอเมริกา (Federal Legislation of the United States)

ได้มีการแก้ไขเพิ่มเติมบรรพที่ 18 แห่งประมวลกฎหมายของสหรัฐอเมริกา (Title 18 of The United States Code) โดยกฎหมายการคุ้มครองระบบคอมพิวเตอร์ ค.ศ.1979 (Federal Computer Systems Protection Act of 1979) ดังนี้

มาตรา 1028 การฉ้อฉลและการกระทำที่ผิดกฎหมายทางคอมพิวเตอร์

A. ผู้ใดเข้าถึง ก่อให้เกิดการเข้าถึง หรือพยายามเข้าถึงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ หรือส่วนหนึ่งส่วนใดของสิ่งดังกล่าว ซึ่งได้ปฏิบัติงานทั้งหมดหรือแต่บางส่วนให้แก่ธุรกิจการค้าระหว่างรัฐ หรือเป็นของหรืออยู่ภายใต้สัญญา

ของหรือร่วมกับสถาบันทางการเงินใด ๆ หรือกระทรวง ทบวง กรมหรือตัวแทนใด ๆ ของรัฐบาลแห่งสหรัฐอเมริกาหรือสถาบันที่มีอยู่ใด ๆ ซึ่งดำเนินการในธุรกิจการค้าระหว่างรัฐ หรือมีผลกระทบต่อธุรกิจการค้าระหว่างรัฐ โดยรู้อยู่แล้วและโดยจงใจไม่ว่าทางตรงหรือทางอ้อม ด้วยความประสงค์แห่ง

(1) การคิดหรือการวางแผนการหรือกลอุบายใด ๆ เพื่อที่จะหลอกลวง หรือ

(2) การได้ไปซึ่งเงิน ทรัพย์สินหรือบริการ สำหรับตนเองหรือผู้อื่นโดยวิธีของการปลอมแปลงหรือการฉ้อโกง หรือการเป็นตัวแทนหรือการให้สัญญา

ต้องระวางโทษปรับไม่เกินสองเท่าครึ่งของความผิดฐานฉ้อโกงหรือลักทรัพย์ หรือจำคุกไม่เกินสิบห้าปีหรือทั้งจำทั้งปรับ

B. ผู้ใดเข้าถึง แก้ไขเปลี่ยนแปลง ทำให้เสียหาย ทำลายหรือพยายามทำให้เสียหายหรือทำลายเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ ดังที่ได้ระบุไว้ในอนุมาตรา (A) หรือคอมพิวเตอร์ซอฟท์แวร์ โปรแกรมหรือข้อมูลใด ๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ โดยเจตนาและโดยปราศจากอำนาจไม่ว่าทางตรงหรือทางอ้อม ต้องระวางโทษปรับไม่เกิน 50,000 เหรียญสหรัฐ หรือจำคุกไม่เกินสิบห้าปี หรือทั้งจำทั้งปรับ

C. คำนิยาม

(1) "เข้าถึง" (Access) หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากหรืออีกนัยหนึ่ง เอาประโยชน์ใด ๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์มาใช้

(2) "คอมพิวเตอร์" (Computer) หมายถึง เครื่องมือประดิษฐ์ทางอิเล็กทรอนิกส์ชนิดหนึ่งซึ่งปฏิบัติงานเกี่ยวกับทางตรรกวิทยา การคำนวณ และความจำโดยอาศัยการยักย้ายถ่ายเทของแรงกระตุ้นทางอิเล็กทรอนิกส์หรือทางแม่เหล็ก และรวมถึงเครื่องมืออำนวยความสะดวกทั้งหลายเกี่ยวกับการนำข้อมูลเข้า การนำข้อมูลออก การประมวลผล การเก็บรักษาข้อมูลซอฟท์แวร์หรือการสื่อสารซึ่งเชื่อมโยงกับหรือเกี่ยวพันกับเครื่องมือประดิษฐ์ดังกล่าว ภายใต้ระบบหรือข่ายงานอันหนึ่ง

(3) "ระบบคอมพิวเตอร์" (Computer System) หมายถึงชุดอุปกรณ์ทางคอมพิวเตอร์ เครื่องมือประดิษฐ์ทั้งหลายและซอฟท์แวร์ที่เกี่ยวข้องสัมพันธ์กัน ทั้งที่ได้เชื่อมโยงกันหรือไม่ได้เชื่อมโยงกัน

(4) "ข่ายงานคอมพิวเตอร์" (Computer Network) หมายถึงการติดต่อเชื่อมโยงกันภายในของระบบการสื่อสารกับเครื่องคอมพิวเตอร์ โดยผ่านสถานีรับส่งทางไกลหลายแห่งหรือหน่วยงานอันซับซ้อนที่ประกอบด้วยเครื่องคอมพิวเตอร์ตั้งแต่สองเครื่องขึ้นไปซึ่งเชื่อมโยงภายในเข้าด้วยกัน

(5) "ทรัพย์สิน" (Property) รวมถึง (แต่ไม่ได้จำกัดเท่านี้) เอกสารทางการเงิน ข่าวสาร ตลอดจนข้อมูลที่ได้ประมวลผลขึ้นหรือได้ผลิตขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์และคอมพิวเตอร์ซอฟท์แวร์กับโปรแกรมคอมพิวเตอร์ที่อยู่ในรูปแบบ ซึ่งทั้งมนุษย์และเครื่องจักรกลต่างก็สามารถที่จะอ่านเข้าใจได้ รวมทั้งวัตถุมีรูปร่างหรือไม่มีรูปร่างซึ่งอาจมีราคาได้อื่น ๆ

(6) "บริการ" (Services) รวมถึง (แต่ไม่ได้จำกัดเพียงเท่านี้) เวลาของการทำงานของเครื่องคอมพิวเตอร์ การประมวลผลข้อมูลและงานเก็บรักษาข้อมูล

(7) "เอกสารทางการเงิน" (Financial Instrument) หมายถึง เช็ค ดร๊าฟท์ ธนาณัติ สมุดเงินฝากธนาคาร หนังสือเลตเตอร์ออฟเครดิต ตั๋วแลกเงิน บัตรเครดิต หรือพันธบัตรใด ๆ หรือเอกสารที่ใช้แทนการประมวลผลทางอิเลกทรอนิกส์ใด ๆ

(8) "โปรแกรมคอมพิวเตอร์" (Computer Program) หมายถึงคำสั่งหรือรายการหรือชุดของคำสั่ง หรือรายการที่อยู่ในรูปแบบอันเป็นที่ยอมรับได้ของเครื่องคอมพิวเตอร์ (ใช้งานได้กับเครื่องคอมพิวเตอร์) ซึ่งทำให้หน่วยงานของระบบคอมพิวเตอร์ตามที่ได้ออกแบบขึ้นสามารถผลิต ผลผลิตที่เหมาะสมออกมาได้

(9) "คอมพิวเตอร์ซอฟท์แวร์" (Computer Software) หมายถึงชุดของโปรแกรมคอมพิวเตอร์ ระเบียบการและเอกสารที่เกี่ยวข้องกับการทำงานของระบบคอมพิวเตอร์

"ความผิดฐานเข้าถึง" ตามมาตรา 1028 เป็นฐานความผิดชนิดหนึ่ง ซึ่งกฎหมายบัญญัติเป็นพิเศษว่า เมื่อมีการเข้าถึง...เกิดขึ้น ผู้กระทำจะต้องมีความผิดตามมาตรานั้น ๆ ซึ่งเป็นการบัญญัติขึ้นเพื่อแก้ไขปัญหาข้อขัดข้องของกฎหมายลักทรัพย์โดยตรง

ส่วน "การเข้าถึง" ทางคอมพิวเตอร์อาจก่อให้เกิดการกระทำที่มิชอบขึ้นได้ในรูปแบบต่าง ๆ กัน การกระทำที่มิชอบเหล่านี้มีลักษณะเช่นเดียวกับความผิดฐานลักทรัพย์ ความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์ในกฎหมายอาญา แต่มีความแตกต่างกันในเรื่องขององค์ประกอบของความผิดบางประการ ซึ่งทำให้ไม่สามารถนำบทบัญญัติของกฎหมายในเรื่องความผิดฐานลักทรัพย์ ความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์มาบังคับใช้กับการกระทำที่ก่อให้เกิดความเสียหายที่เกิดขึ้นได้

ในส่วนของการกระทำในความผิดฐานลักทรัพย์นั้น กฎหมายที่มีอยู่แล้วในเรื่องลักทรัพย์ได้ประสบกับปัญหาข้อขัดข้องในการนำมาบังคับใช้กับความผิดที่เกิดขึ้นกับเทคโนโลยีสมัยใหม่นี้ โดยเหตุที่ความผิดฐานลักทรัพย์นั้น ส่วนใหญ่จะเป็นเรื่องที่เกี่ยวกับทรัพย์ที่จับต้องได้และทรัพย์ที่จับต้องไม่ได้ในบางกรณี เพราะฉะนั้นการ "เอาไป" จึงถือว่าเป็นสาระสำคัญของความผิดฐานนี้ องค์ประกอบเกี่ยวกับการ "เอาไป" นี้ได้ก่อให้เกิดปัญหาขึ้นในเมื่อมันได้เข้าไปเกี่ยวข้องกับคอมพิวเตอร์ เพราะการเอาไปในกรณีนี้อาจจะมิได้มีการจับต้องหรือพาไปตามความเป็นจริงเลยก็ได้ (วีรพงษ์ บุญโญภาส, 2531 : 103) ดังนั้นกฎหมายของสหรัฐอเมริกาในปัจจุบันจึงได้บัญญัติกฎหมายอาญาในความผิดเกี่ยวกับคอมพิวเตอร์ในส่วนของความผิดดังกล่าวเป็น "ความผิดฐานเข้าถึง (Access) ขึ้นต่างหากจากความผิดฐานลักทรัพย์ เพื่อที่จะสามารถนำมาใช้บังคับกับการกระทำที่ก่อให้เกิดความเสียหายอันมีลักษณะของการลักขโมยนี้ขึ้นโดยเฉพาะ ในขณะเดียวกันก็ได้บัญญัติให้การกระทำที่มิชอบในทำนองปลอมเอกสารและทำให้เสียทรัพย์เป็น" ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)" และ "ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) ซึ่งจะได้นำมากล่าวต่อไป

ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) หมายถึง การแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ คอมพิวเตอร์ซอฟท์แวร์ โปรแกรมหรือข้อมูลใด ๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์

ในลักษณะของการแก้ไขเปลี่ยนแปลงนั้น บางลักษณะก็จะต้องอาศัยการเข้าถึงทางคอมพิวเตอร์ด้วย ดังที่ได้กล่าวมาแล้ว แต่ในบางลักษณะก็อาจจะเป็นการแก้ไขเปลี่ยนแปลงที่ไม่ต้องอาศัยการเข้าถึงใด ๆ อันเป็นการแก้ไขเปลี่ยนแปลงแก่วัตถุที่เป็นรูปธรรมโดยตรงและเนื่องจากรูปธรรมนี้เป็นทรัพย์สินทางเทคโนโลยีชนิดหนึ่ง การกระทำนั้นจึงอาจก่อให้เกิดความเสียหายได้ค่อนข้างสูง เมื่อเทียบกับการแก้ไขเปลี่ยนแปลงในทรัพย์สินที่เป็นประดิษฐ์กรรมธรรมดาอย่างอื่น ๆ กฎหมายอาญาในความผิดเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกา จึงได้บัญญัติให้เป็นความผิดชนิดหนึ่ง ความผิดฐานแก้ไขเปลี่ยนแปลงนี้ต้องเป็นการกระทำโดยเจตนา และเป็นการกระทำโดยปราศจากอำนาจเพราะถ้าเป็นการกระทำที่มีอำนาจในการแก้ไขเปลี่ยนแปลงก็ย่อมไม่มีความผิดในทางอาญาตามหลักกฎหมายทั่วไป การแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์มีส่วนเกี่ยวข้องในแง่ของการกระทำ ซึ่งเป็นปัญหาเกี่ยวกับความผิดฐานปลอมเอกสารอยู่ด้วย ความผิดฐานปลอมเอกสารเกี่ยวกับคอมพิวเตอร์ซอฟท์แวร์ โปรแกรมคอมพิวเตอร์หรือข้อมูลต่าง ๆ นั้นมีปัญหาข้อขัดข้องในการตีความหมายของคำว่า "เอกสาร" จะครอบคลุมถึงสิ่งต่าง ๆ ดังกล่าวหรือไม่ กฎหมายของสหรัฐอเมริกาจึงได้แก้ไขปัญหาด้วยการบัญญัติให้การกระทำดังที่กล่าวมาเป็นความผิดฐาน "แก้ไขเปลี่ยนแปลง" โดยไม่จำต้องมีองค์ประกอบดังเช่นความผิดฐาน "ปลอมเอกสาร" ที่ได้ใช้อยู่เดิม

ส่วนการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์นั้น ย่อมไม่มีปัญหาในเรื่องของการปลอมเอกสารแต่อย่างใด เพราะไม่มีส่วนเกี่ยวข้องกับคำว่า "เอกสาร" อยู่เลย ส่วนสาเหตุที่บัญญัติไว้ให้เป็นความผิดพิเศษออกไปก็เพื่อคุ้มครองผลิตผลทางเทคโนโลยีนั้นเอง

ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) หมายถึงการทำให้เสียหายหรือทำลายเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ คอมพิวเตอร์ซอฟท์แวร์ โปรแกรมหรือข้อมูลใด ๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ และเช่นเดียวกับลักษณะของการแก้ไขเปลี่ยนแปลง บางลักษณะก็จะต้องอาศัยการเข้าถึงทางคอมพิวเตอร์ด้วย บางลักษณะก็เป็นการทำให้เสียหายหรือทำลายที่ไม่ต้องอาศัยการเข้าถึงอันเป็นการเสียหายหรือทำลายโดยตรง และด้วยเหตุผลเดียวกับการแก้ไขเปลี่ยนแปลง ความเสียหายที่เกิดขึ้นจากการกระทำค่อนข้างสูง และสิ่งที่เสียหายเป็น

ผลิตผลทางเทคโนโลยีชนิดหนึ่ง กฎหมายอาญาเกี่ยวกับความผิดทางคอมพิวเตอร์ ในสหรัฐอเมริกาจึงถือเป็นเหตุผลหนึ่งที่บัญญัติให้เป็นความผิดต่างหาก แยกออกจากความผิดฐานทำให้เสียทรัพย์ธรรมดา (ภานุ รังสีสหัส, 2533 : 121)

(2) **กฎหมายในระดับรัฐบาลกลาง** ซึ่งถูกนำมาใช้บังคับกับอาชญากรรมคอมพิวเตอร์ไม่ว่าจะเป็นการใช้โดยตรงหรือโดยอ้อม กฎหมายที่เกี่ยวข้องมากที่สุดจะเป็นกฎหมายที่เกี่ยวกับกรณีดังต่อไปนี้ (David Icove, 1995 : 73)

- กฎหมายว่าด้วยการค้าและการพาณิชย์ มาตรา 1644 การฉ้อโกงโดยใช้เครดิตการ์ด (15 USC Commerce and Trade, Chapter 41, Section 1644)

- กฎหมายว่าด้วยลิขสิทธิ์ (17 USC Copyrights)

- กฎหมายอาญาและวิธีพิจารณาความอาญา (18 USC Crimes and Criminal Procedure) มาตรา 81 การลอบวางเพลิงคอมพิวเตอร์และอุปกรณ์, มาตรา 641 การยักยอกหรือลักทรัพย์ซึ่งเงิน ทรัพย์สินหรือบันทึกของสาธารณะ, มาตรา 793 การสูญเสียซึ่งการปกป้องข้อมูลข่าวสาร, มาตรา 1029 การฉ้อโกงโดยใช้อุปกรณ์เข้าถึง, มาตรา 1030 การฉ้อโกงโดยการใช้คอมพิวเตอร์, มาตรา 1343 การฉ้อโกงโดยใช้สายโทรเลข คลื่นวิทยุหรือโทรทัศน์, มาตรา 2155 การก่อวินาศกรรมต่อคอมพิวเตอร์หรือข้อมูลข่าวสาร, มาตรา 2314 การลักทรัพย์สินที่เกี่ยวข้องกับคอมพิวเตอร์, มาตรา 2511 การขัดขวางหรือเปิดเผยระบบสื่อสารโทรคมนาคม, มาตรา 2522 ให้อำนาจเจ้าพนักงานในการบังคับใช้กฎหมายเกี่ยวกับระบบสื่อสารโทรคมนาคมโดยได้รับอนุญาตจากศาล, มาตรา 3121 การใช้อุปกรณ์ดักฟัง อุปกรณ์ติดตามและอุปกรณ์บันทึกหมายเลข (Pen Register) โดยได้รับอนุญาตจากศาล, มาตรา 2000aa การตรวจค้นและยึดพยานหลักฐานในการสืบสวนดำเนินคดีจะต้องได้รับอนุญาตจากศาล (David Icove, 1995 : 74-78)

(3) **กฎหมายในระดับมลรัฐของประเทศสหรัฐอเมริกา** ในระดับมลรัฐต่างก็มีการบัญญัติกฎหมายเฉพาะออกมาโดยมุ่งตรงต่ออาชญากรรมคอมพิวเตอร์ กฎหมายส่วนใหญ่นั้นคล้ายคลึงหรือเลียนแบบมาจากกฎหมายในระดับรัฐบาลกลางหรือกฎหมายของรัฐที่ประสบกับปัญหาอาชญากรรมคอมพิวเตอร์มากที่สุด เช่น รัฐแคลิฟอร์เนีย เป็นต้น

2.2.2 กฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ของประเทศอังกฤษ

อังกฤษเป็นประเทศที่ใช้และพัฒนาเทคโนโลยีทางคอมพิวเตอร์ เช่นเดียวกับประเทศสหรัฐอเมริกา จึงได้มีการพัฒนากฎหมายขึ้นมาบังคับใช้กับเทคโนโลยีทางคอมพิวเตอร์ ทั้งในทางแพ่งและทางอาญา โดยอังกฤษได้ออกกฎหมายเพื่อที่จะรับฟังเอกสารจากคอมพิวเตอร์ โดยถือว่าเป็นข้อยกเว้นของพยานบอกเล่า คือ พระราชบัญญัติพยานทางแพ่ง ค.ศ.1968 (Civil Evidence Act 1968), พระราชบัญญัติพยานทางอาญา ค.ศ.1965 (Criminal Evidence Act 1965) และในปี ค.ศ.1984 อังกฤษได้บัญญัติกฎหมายใหม่คือ พระราชบัญญัติตำรวจและพยานทางอาญา ค.ศ.1984 เพื่อสร้างเงื่อนไขในการรับฟังเอกสารจากคอมพิวเตอร์ให้รัดกุมขึ้นกว่ากฎหมายเดิม

ต่อมาเมื่อมีการกระทำผิดทางอาญา โดยใช้คอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้องมูลค่าความเสียหายที่เกิดขึ้นมีจำนวนมาก ประเทศอังกฤษจึงได้บัญญัติกฎหมายขึ้นมาควบคุมอาชญากรรมคอมพิวเตอร์ขึ้นบังคับใช้เมื่อ 29 สิงหาคม ค.ศ.1990 คือพระราชบัญญัติการใช้คอมพิวเตอร์ในทางที่ผิด ค.ศ.1990 (Computer Misuse Act 1990) โดยมีเหตุผลในการประกาศใช้ว่า "พระราชบัญญัติฉบับนี้เป็นบทบัญญัติเพื่อคุ้มครองสำหรับการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์และอุปกรณ์ในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการแก้ไขเปลี่ยนแปลงที่เกี่ยวข้องกับผลประโยชน์ที่มิชอบ" ซึ่งมีเนื้อหาสาระที่สำคัญของกฎหมาย ดังนี้คือ

มาตรา 1 ความผิดฐานเข้าถึงคอมพิวเตอร์และส่วนประกอบของคอมพิวเตอร์โดยไม่ได้รับอนุญาต

(1) บุคคลใดก็ตามย่อมมีความผิด ถ้า

a. บุคคลนั้นได้ทำการให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใด ๆ โดยเจตนาที่จะเข้าถึงสิ่งที่ปกป้องคุ้มครองไม่ให้เข้าสู่ระบบหรือได้ผ่านสิ่งปกป้องเช่นว่านั้นเข้าไปยังโปรแกรมใด ๆ หรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใด ๆ

b. บุคคลนั้นเจตนาที่จะเข้าถึงสิ่งที่ปกป้องคุ้มครองระบบโดยปราศจากอำนาจและ

c. บุคคลนั้นได้รู้อยู่ในขณะนั้นว่าตนเป็นต้นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานอันปราศจากอำนาจนั้น

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำต่อ

a. โปรแกรมพิเศษหรือข้อมูลพิเศษเฉพาะเจาะจงใด ๆ

b. โปรแกรมหรือข้อมูลเฉพาะชนิดใดชนิดหนึ่ง หรือ

c. โปรแกรมหรือข้อมูลที่ถูกเก็บไว้เฉพาะในคอมพิวเตอร์ใด ๆ

(3) บุคคลใดกระทำความผิดตามมาตรานี้ต้องระวางโทษ...

มาตรา 2 การเข้าถึงโดยไม่ได้รับอนุญาต หมายถึง มีเจตนาที่จะกระทำการหรือให้ความสะดวกหรือส่งเสริมในการกระทำความผิด ดังนี้

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ถ้าหากว่าตนได้กระทำความผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการเข้าถึงโดยไม่มีอำนาจเป็นความผิด)

a. ได้กระทำผิดในสิ่งที่มาตรานี้บังคับใช้ หรือ

b. ให้ความสะดวกในการกระทำผิด (ไม่ว่าโดยตนเองหรือโดยบุคคลใด ๆ) และความผิดที่ตนจงใจกระทำผิดหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำผิด เช่นเดียวกันกับผู้กระทำผิดที่ตนช่วย

(2) มาตรานี้บังคับใช้กับความผิดของบุคคลซึ่งมีอายุตั้งแต่ 21 ปีขึ้นไป

(3) เพื่อวัตถุประสงค์ของมาตรานี้ไม่ว่าการกระทำความผิดของผู้กระทำผิดที่อยู่ระยะไกลจะได้กระทำลงในโอกาสที่ไม่มีอำนาจในการเข้าถึงระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้ถึงว่าจะมีข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำผิดที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) ผู้กระทำผิดตามมาตรานี้ต้องระวางโทษ

มาตรา 3 ความผิดฐานแก้ไขเปลี่ยนแปลง คอมพิวเตอร์และส่วนประกอบโดยไม่ได้รับอนุญาต

(1) บุคคลใดก็ตามย่อมมีความผิด ถ้า

a. ผู้นั้นได้กระทำการใด ๆ อันเป็นการก่อให้เกิดการแก้ไขเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ใด ๆ และ

b. จะต้องกระทำการโดยเจตนาและจำเป็นต้องได้รู้ถึงการกระทำนั้น

(2) ความมุ่งหมายโดยเจตนาตาม อนุ 1 ข้างต้น หมายถึง เจตนาที่จะก่อให้เกิดการแก้ไขเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ใด ๆ และได้กระทำโดย

a. ทำให้เสียไปซึ่งระบบปฏิบัติการของคอมพิวเตอร์ใด ๆ

b. ป้องกันหรือขัดขวางการเข้าถึงเพื่อที่จะยึดข้อมูลหรือโปรแกรมคอมพิวเตอร์ใด ๆ ในเครื่องคอมพิวเตอร์

c. ทำให้เสียไปซึ่งระบบปฏิบัติการของโปรแกรมคอมพิวเตอร์นั้น หรือความน่าเชื่อถือของข้อมูลนั้น ๆ

(3) โดยเจตนาไม่จำเป็นที่จะต้องตรงกับ

a. คอมพิวเตอร์ใด ๆ โดยเฉพาะ

b. ข้อมูลหรือโปรแกรมเฉพาะหรือข้อมูล หรือโปรแกรมชนิดใดชนิดหนึ่งโดยเฉพาะ

c. การแก้ไขเปลี่ยนแปลงใด ๆ โดยเฉพาะหรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) ความมุ่งหมายของอนุ (1) b. จำเป็นต้องรู้ถึงการกระทำนั้น หมายถึงการได้รู้ว่าในการแก้ไขเปลี่ยนแปลงใด ๆ ผู้นั้นได้เจตนาก่อให้เกิดขึ้นโดยที่ไม่ได้รับอนุญาต

(5) ความมุ่งหมายของส่วนประกอบคอมพิวเตอร์ตามมาตรานี้ ไม่ว่าจะเป็นการแก้ไขโดยไม่ได้รับอนุญาตหรือเจตนากระทำต่อคอมพิวเตอร์ และส่วนประกอบตาม อนุ (2) หรือเป็นเจตนาที่กระทำอย่างถาวรหรือเพียงชั่วคราวก็ตาม

(6) การแก้ไขเปลี่ยนแปลงสิ่งซึ่งบรรจุอยู่ในคอมพิวเตอร์ จะได้รับการคุ้มครองตามความมุ่งหมายของกฎหมายชดเชยความเสียหายจากอาชญากรรม ค.ศ.1971 ถ้าการแก้ไขเปลี่ยนแปลงนั้นมีผลกระทบโดยตรงต่อคอมพิวเตอร์ สื่อบันทึกของคอมพิวเตอร์และทำให้เสียไปตามลักษณะเงื่อนไขทางกายภาพหรือทางวัตถุ

(7) บุคคลใดกระทำความผิดตามมาตรานี้ต้องระวางโทษ

กฎหมาย Computer Misuse Act 1990 ของประเทศอังกฤษในมาตรา 1 เป็นการบัญญัติพื้นฐานที่ใช้กับความผิดฐานเข้าถึงโดยไม่ได้รับอนุญาต มีสาระที่สำคัญในส่วนของการกระทำคือผู้กระทำผิดจะต้องกระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลการทำงานใด ๆ โดยผู้กระทำจะต้องรับผิดนั้นไม่ว่าผู้กระทำจะประสบผลสำเร็จในการเข้าสู่ระบบประมวลผลเข้าสู่โปรแกรมหรือข้อมูลหรือไม่ถือว่าเป็นความผิดสำเร็จแล้ว ส่วนความผิดในมาตรา 2 บังคับใช้กับกรณีกระทำการหรือให้ความสะดวกหรือส่งเสริมในการกระทำความผิดตามมาตรา 1 ซึ่งเป็นการควบคุมเครื่องจากระยะไกล เช่น การลักลอบเข้าถึงระบบโดยใช้เครื่องระยะไกลและใช้บังคับกับบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป โทษตามมาตรา 2 จะมีโทษสูงกว่ามาตรา 1 และในมาตรา 3 เป็นบทบัญญัติความผิดฐานแก้ไขเปลี่ยนแปลงคอมพิวเตอร์และส่วนประกอบ อันเป็นฐานความผิดชนิดหนึ่งบังคับใช้กับความผิดที่เกี่ยวข้องกับคอมพิวเตอร์

2.2.3 เจตนาในการกระทำความผิด

ในการกำหนดโทษสำหรับความผิดทางอาญาโดยทั่วไปจะต้องมีการแสดงออกถึงเจตนาในการกระทำความผิดทางอาญาด้วย ซึ่งนับว่าเป็นองค์ประกอบภายในของความรับผิดทางอาญาในเรื่องนั้น ๆ เจตนาที่จะกระทำความผิด ได้มีการบัญญัติไว้ในตัวบทกฎหมายอาญาของทุกประเทศทั่วโลก สำหรับการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์นั้น ก็เป็นความผิดทางอาญาที่ต้องการเจตนาดังเช่นความผิดอาญาอื่น ๆ โดยทั่วไปอันเป็น "เจตนาธรรมดา" ที่จะกระทำการอันเป็นความผิดนั้น ๆ และในขณะเดียวกันความผิดทางอาญาที่เกี่ยวกับคอมพิวเตอร์ในบางกรณีก็อาจต้องการ "เจตนาพิเศษ" ในการกระทำผิดนั้น ๆ ด้วย ตัวอย่างเช่น กฎหมายในเรื่องการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ของมลรัฐแคลิฟอร์เนีย สหรัฐอเมริกา บัญญัติว่า "จำเลยจะต้องเข้าถึงระบบคอมพิวเตอร์" "เพื่อจุดประสงค์ของการวางแผนหรือกลอุบายใด ๆ เพื่อที่จะข่มขู่หรือหลอกลวง" หรือได้ประโยชน์จากการบริการ "โดยเจตนาทุจริตและหลอกลวง" ซึ่งถ้าผู้กระทำความผิดขาดเจตนาดังกล่าวก็ไม่อาจมีการลงโทษทางอาญาเกิดขึ้นได้ แม้ว่าผู้กระทำผิดยังอาจถูกดำเนินคดีทางแพ่งในข้อหาฐานละเมิดได้ก็ตาม

2.3 คำนิยามศัพท์ของอาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์มีความหมายกว้างขวาง นักวิชาการให้คำนิยามไว้ตามวัตถุประสงค์ของการศึกษาในแต่ละกรณี องค์การสหประชาชาติยอมรับว่าไม่สามารถบัญญัตินิยามศัพท์ให้ยอมรับเป็นสากลได้ ซึ่งในทางปฏิบัติจำแนกออกเป็น 2 ส่วนคือ

ส่วนที่ 1 อาชญากรรมดั้งเดิมซึ่งโดยทั่วไปมีกฎหมายระบุฐานความผิดและบทลงโทษไว้อยู่แล้ว เช่น การโจรกรรม การฉ้อโกง การปลอมแปลงและการก่อกวน ซึ่งมีกฎหมายหลักบัญญัติความผิดและบทลงโทษไว้

ส่วนที่ 2 การฝ่าฝืนกฎหรือข้อห้ามและพฤติกรรมเบี่ยงเบนต่าง ๆ ในการใช้คอมพิวเตอร์ยังไม่มีกฎหมายบัญญัติไว้เป็นความผิด

คู่มืออาชญากรรมคอมพิวเตอร์ ของกระทรวงยุติธรรมสหรัฐอเมริกา ให้ความหมายอาชญากรรมคอมพิวเตอร์ไว้ว่า

"การกระทำผิดกฎหมายอาญาที่ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์ ในการก่ออาชญากรรม การสืบสวนจับกุมและการดำเนินคดีในชั้นสอบสวนและการพิจารณาคดีในชั้นศาล (David Carter, 1996 : 3-3)

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

(1) อาชญากรรมที่เกิดขึ้นใหม่อันเป็นผลสืบเนื่องมาจากการใช้คอมพิวเตอร์ในสังคมอย่างแพร่หลาย เช่น การบุกรุกเข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัทธุรกิจที่เชื่อมโยงผ่านเครือข่ายโทรคมนาคม

(2) อาชญากรรมแบบดั้งเดิมที่แปรสภาพไป เนื่องมาจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ ซึ่งในการสืบสวนคดีประเภทนี้จำต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ และคุ้นเคยกับอุตสาหกรรมเทคโนโลยีขั้นสูง (Kenneth Rosenblatt, 1995 : 1-2)

ศาสตราจารย์ ดร.เดวิด คาร์เตอร์ (David L.Carter) และ ดร.แอนดรา แคทซ์ (Andra J. Katz) นักวิชาการจากมหาวิทยาลัยมิชิแกนสเตท สหรัฐอเมริกา ซึ่งเป็นนักวิชาการที่ศึกษาวิจัยเรื่องนี้ให้นิยามศัพท์ของอาชญากรรมคอมพิวเตอร์ไว้ว่า

(1) การกระทำใด ๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และทำให้ผู้กระทำได้รับผลตอบแทน

(2) การกระทำผิดกฎหมายใด ๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์มาประกอบในการสืบสวนติดตามจับกุม

และให้ความหมายการกระทำที่ผิดกฎระเบียบเกี่ยวกับการใช้คอมพิวเตอร์ (Computer Malfeasance) หมายถึง

"การกระทำใด ๆ ที่เกี่ยวกับการใช้ การเข้าถึงข้อมูล โดยที่ผู้กระทำไม่ได้รับอนุญาต แม้ไม่ถึงกับเป็นการกระทำที่ผิดกฎหมาย แต่ก็เป็นการกระทำที่ผิดระเบียบกฎเกณฑ์ของการใช้คอมพิวเตอร์นั้น ๆ" (David Carter, 1996 : 3-3)

ศาสตราจารย์ ดร.ดอน บาร์กเกอร์ (Don Parker) อาจารย์แห่งมหาวิทยาลัยสแตนฟอร์ด สหรัฐอเมริกา อธิบายความหมายของอาชญากรรมคอมพิวเตอร์ว่า

"คอมพิวเตอร์เข้ามามีส่วนสำคัญในการประกอบอาชญากรรมทั่วไป ซึ่งรวมถึงการฉ้อโกง ลักทรัพย์ ยักยอกทรัพย์ การรับสินบน วินาศกรรม จารกรรม รีดเอาทรัพย์และลักพาตัวเพื่อเรียกค่าไถ่"

มร.จอห์น เทเบอร์ (John Taber) นักเขียนโปรแกรมระบบคอมพิวเตอร์ของบริษัท IBM อธิบายถึงความหมายของ อาชญากรรมคอมพิวเตอร์ว่า

"เป็นการกระทำอภินิหารที่ไม่น่าเชื่อ เพราะเหตุว่า สภาพที่อยู่เหนือความเข้าใจของมนุษย์และเทคโนโลยีคอมพิวเตอร์ นำพาไปสู่การประกอบอาชญากรรมได้ แม้การบังคับจากระยะไกลด้วยเครื่องคอมพิวเตอร์

ดังนั้น เมื่อมีการกระทำผิดใดเกิดขึ้นและเกี่ยวข้องกับคอมพิวเตอร์ องค์ประกอบหลายส่วนของการกระทำความผิดที่ยากต่อการทำความเข้าใจ ไม่เฉพาะต่อผู้คนทั่วไปเท่านั้น แต่ยังสร้างความสับสนแก่พนักงานเจ้าหน้าที่ในกระบวนการยุติธรรมที่จะดำเนินคดีกับผู้กระทำผิดอีกด้วย"

แม้ว่าจะมีการอธิบายความหมายของอาชญากรรมคอมพิวเตอร์ไว้ โดยนักวิชาการหลายคนที่แตกต่างกันออกไป แต่พอสรุปเพื่อการทำความเข้าใจความหมายได้ว่า

อาชญากรรมคอมพิวเตอร์ (Computer Crime) คือ การใช้เครื่องคอมพิวเตอร์หรือใช้เทคโนโลยีที่มีเป้าหมายของการกระทำต่อเครื่องคอมพิวเตอร์ หรือเป็นเครื่องมือในการกระทำความผิดที่ฝ่าฝืนต่อกฎหมายเกี่ยวกับการกระทำผิดอาญาจำพวก ลักทรัพย์ ทุจริต ฉ้อโกงหรือยักยอกทรัพย์ บริการหรือข้อมูล แยกกล่าวได้เป็น 2 พวก ดังนี้

(1) ลักทรัพย์หรือละเมิดต่อฮาร์ดแวร์ (Hardware), โปรแกรมที่อยู่ในเครื่อง (Firm Ware), และซอฟท์แวร์ (Software) โดยถือว่าเครื่องคอมพิวเตอร์เป็นเป้าหมายของการกระทำต่อ (Computer as the Victims of Crime)

(2) การลักทรัพย์, วินาศกรรม, จารกรรม, ทุจริตฉ้อโกง หรือยักยอกทรัพย์ที่มีการใช้เครื่องคอมพิวเตอร์ เป็นเครื่องมืออำนวยความสะดวกในการกระทำผิด (Computer as the Facilitators of Crime)

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ว่า คำนิยามของคำว่า อาชญากรรมคอมพิวเตอร์นั้นมีหลายแนวทางและส่วนใหญ่มักจะไม่ให้คำนิยามไว้อย่างชัดเจน อย่างไรก็ดีสามารถแบ่งแยกคำนิยามได้ดังต่อไปนี้

- คำนิยามที่มีความหมายอย่างแคบ คือให้คำว่าอาชญากรรมทางคอมพิวเตอร์ รวมถึงเฉพาะความผิดที่เกิดขึ้นกับข้อมูลภายในคอมพิวเตอร์เท่านั้น

- คำนิยามที่ใช้ความรู้ทางคอมพิวเตอร์เป็นเกณฑ์ กล่าวคือครอบคลุมเฉพาะความผิดที่เกิดขึ้น ไม่ว่าจะในเครื่องคอมพิวเตอร์หรือกับเครื่องคอมพิวเตอร์เอง และความผิดดังกล่าวผู้กระทำความผิดต้องใช้ความรู้ความสามารถทางคอมพิวเตอร์เป็นพิเศษ

- คำนิยามที่ให้ความหมายอย่างกว้างคือ ครอบคลุมถึงการกระทำความผิดทุกอย่างที่มีคอมพิวเตอร์เป็นส่วนประกอบ

การให้คำนิยามหรือคำจำกัดความนั้นพบว่ามีข้อจำกัดดังนี้ คือ

- การให้คำนิยามเป็นการอธิบายถึงพฤติกรรมของบุคคล มิใช่เป็นการประกอบอาชญากรรมโดยแท้

- หลายครั้งไม่สามารถนำข้อกฎหมายมาปรับใช้เพื่อลงโทษผู้กระทำได้โดยตรง อย่างเช่นที่ใช้กับคดีอาญาทั่วไป เช่น คดีลักทรัพย์ คดีฉ้อโกง เป็นต้น

- เป็นการกระทำเกี่ยวเนื่องกับเขตอำนาจการดำเนินคดี เพราะการกระทำเกี่ยวเนื่องกับคนทั่วโลก บางครั้งการกระทำที่ถือว่าเป็นความผิดในประเทศหนึ่ง แต่อาจไม่เป็นความผิดในอีกประเทศหนึ่ง

- หลายครั้งเป็นการยากที่จะพิสูจน์ว่ามีอาชญากรรมเกิดขึ้นจริง เนื่องจากไม่มีหลักฐานที่จะพิสูจน์ความผิด ไม่มีพยานบุคคลยืนยันการกระทำนั้น บางครั้งไม่ส่งผลกระทบต่อเจ้าของคอมพิวเตอร์โดยตรง เพียงแต่เป็นการละเมิดกฎเกณฑ์บางอย่างเท่านั้น ส่งผลให้การให้คำนิยามและคำจำกัดความหมายอาชญากรรมคอมพิวเตอร์ยังไม่เป็นที่สรุปได้แน่ชัด

2.4 ประเภทและลักษณะของอาชญากรรมและอาชญากรคอมพิวเตอร์

2.4.1 การแบ่งประเภทอาชญากรรมคอมพิวเตอร์ของ ดร.เดวิด คาร์เตอร์ และ ดร.แอนดรา แคทซ์

ศาตราจารย์ ดร.เดวิด คาร์เตอร์ (David Carter) และ ดร.แอนดรา แคทซ์ (Andra Katz) ซึ่งเป็นนักอาชญาวิทยาที่ศึกษาวิจัยเรื่องนี้ ได้แบ่งอาชญากรรมคอมพิวเตอร์ไว้เป็น 6 ประเภท ได้แก่

(1) การปฏิบัติการต่อคอมพิวเตอร์ ซึ่งเป็นเป้าหมายของอาชญากรรมโดยตรง (The Computer is the Target) เพื่อให้ได้มาถึงข้อมูลคอมพิวเตอร์หรือเพื่อทำความเสียหายให้กับเครื่อง โปรแกรมหรือแฟ้มข้อมูลคอมพิวเตอร์ต่าง ๆ อาทิเช่น

- การโจรกรรมทรัพย์สินทางปัญญา
- การโจรกรรมข้อมูลการตลาด
- การฉ้อฐานข้อมูลในแฟ้มคอมพิวเตอร์
- การก่อวินาศกรรมต่อทรัพย์สินทางปัญญา
- การก่อวินาศกรรมต่อโปรแกรมระบบปฏิบัติการหรือแฟ้มข้อมูลคอมพิวเตอร์
- การบุกรุกฐานข้อมูลทะเบียนของทางราชการ

- การลักลอบเข้าไปในระบบคอมพิวเตอร์ เพื่อความท้าทายหรือความอยากรู้อยากเห็นอันเป็นการละเมิดต่อการเป็นส่วนตัว

(2) อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด (The Computer is an Instrumentality of a Crime) ใช้การประมวลผลของเครื่องคอมพิวเตอร์ให้ความสะดวกแก่การประกอบอาชญากรรม เช่น

- การปลอมแปลงบัตรบริการเงินด่วนและเลขบัญชี
- การลักลอบโอนเงินจากการปัดเศษตัวเลขในการคำนวณดอกเบี้ยธนาคารหรือแลกเปลี่ยนสกุลเงิน
- การปลอมแปลงบัตรเครดิต
- การฉ้อโกงโดยใช้การทำรายการบนเครื่องคอมพิวเตอร์
- การฉ้อโกงทางด้านการสื่อสารโทรคมนาคม

(3) อาชญากรรมอื่น ๆ ที่มีส่วนเกี่ยวข้องกับคอมพิวเตอร์ (The Computer is Incidental to Other Crimes) คือคอมพิวเตอร์ไม่ใช่สิ่งจำเป็นสำหรับการประกอบอาชญากรรม แต่ว่าคอมพิวเตอร์เป็นส่วนประกอบในการกระทำผิด เช่น

- การฟอกเงิน
- การลักลอบโอนเงิน
- การเผยแพร่ภาพลามกอนาจาร
- คดีฆาตกรรม
- การพนันบุคเมคกิ้ง
- การลักพาตัว เรียกค่าไถ่ เป็นต้น

(4) อาชญากรรมอันเป็นผลมาจากการใช้คอมพิวเตอร์อย่างแพร่หลายทั่วไป (Crime which is Associated with the Prevalence of Computer) เช่น

- การลอกเลียนหรือปลอมแปลงโปรแกรมคอมพิวเตอร์
- การละเมิดลิขสิทธิ์ของโปรแกรมคอมพิวเตอร์
- การปลอมแปลงอุปกรณ์
- การค้าอุปกรณ์และโปรแกรมคอมพิวเตอร์ในตลาดมืด

(5) การข่มขู่ผ่านคอมพิวเตอร์ (Technological Coercion Via Computer) เช่น

- การใช้เอกสารจากคอมพิวเตอร์เป็นหลักฐานในการข่มขู่
- การใช้คอมพิวเตอร์ในการเข้าถึงและเผยแพร่คำขู่เข็ญ

(6) การรบกวนเครือข่ายคอมพิวเตอร์ (Networking Malfeasance) เช่น

- การก่อกวนทางเพศ
- การก่อกวน ไล่ล่า ติดตาม
- การหมิ่นประมาทบุคคลหรือองค์กรผ่านทางเครือข่ายคอมพิวเตอร์
- การล่อลวงเยาวชนไปเพื่อการอนาจาร

2.4.2 การแบ่งประเภทอาชญากรรมคอมพิวเตอร์ของสำนักงานเลขาธิการองค์กรตำรวจสากล

สำนักงานเลขาธิการองค์กรตำรวจสากลจำแนกประเภทอาชญากรรมคอมพิวเตอร์เป็น 6 ประเภท ดังนี้

(1) การลักลอบผ่านเข้าและการสกัดข้อมูล (Unauthorized Access and Interception) ได้แก่

- การลักลอบผ่านเข้าไปในระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต
- การสกัดข้อมูลของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยใช้วิธีการทางเทคนิคโดยไม่มีสิทธิ
- การลักลอบใช้งานระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์

(2) การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Alteration of Computer Data) ได้แก่ การลักลอบใส่โปรแกรม Logic Bomb, Trojan Horse, Virus หรือ Worm เข้าไปเปลี่ยนแปลงข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์

(3) คดีฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-Related Fraud) ได้แก่ การฉ้อโกงและโจรกรรมเงินสดจากเครื่องฝากถอนเงินอัตโนมัติ (ATM), การปลอมแปลง

โดยใช้เครื่องคอมพิวเตอร์ เช่น การปลอมแปลงรหัสลับเฉพาะตัวในเครื่องโทรศัพท์มือถือ, การปลอมแปลงบัตรเครดิต, บัตรโทรศัพท์, การใช้คอมพิวเตอร์ในการปลอมแปลงเอกสารสำคัญต่าง ๆ, การปลอมแปลงเงินตรา ตั๋วเงินต่าง ๆ, การปลอมแปลงเครื่องเล่นเกม การฉ้อโกงด้วยการแก้ไขข้อมูลคอมพิวเตอร์ การฉ้อโกงและการโจรกรรมที่เกี่ยวข้องกับการชำระเงินหรือจุดจำหน่ายสินค้า และการลักลอบใช้บริการการสื่อสารคมนาคม

(4) การทำซ้ำโปรแกรมคอมพิวเตอร์และลอกเลียนแบบสินค้า (Semi-Conductor) ที่ได้รับการคุ้มครองลิขสิทธิ์ (Unauthorized Reproduction)

(5) การก่อวินาศกรรมระบบ ข้อมูลและโปรแกรมคอมพิวเตอร์ (Computer Sabotage)

(6) อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์อื่น ๆ (Other Computer Related Crime)

- การโจรกรรมข้อมูลลับทางการค้าเพื่อทำให้เสียหายทางเศรษฐกิจหรือได้เปรียบทางการค้า

- การใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ในการเก็บหรือขนถ่ายสินค้าผิดกฎหมาย

- การใช้ BBS (ซึ่งเป็นโปรแกรมที่ทำหน้าที่เก็บรายการ หัวข้อหรือข้อมูล) ในการบันทึก การเปลี่ยนและแจกจ่ายสิ่งของที่เกี่ยวข้องกับการกระทำผิด

2.4.3 การแบ่งประเภทอาชญากรรมคอมพิวเตอร์ขององค์การสหประชาชาติ

องค์การสหประชาชาติจำแนกอาชญากรรมคอมพิวเตอร์ ไว้เป็น 5 ประเภท ได้แก่

(1) การฉ้อโกงโดยใช้คอมพิวเตอร์ (Fraud by Computer Manipulation)

(2) การปลอมแปลงโดยใช้คอมพิวเตอร์ (Computer Forgery)

(3) การทำลายหรือแก้ไขเปลี่ยนแปลงข้อมูลหรือโปรแกรมคอมพิวเตอร์ (Damage to or Modification of Computer Data or Programs)

(4) การลักลอบเข้าไปในระบบเครือข่ายคอมพิวเตอร์และการลักลอบใช้บริการ (Unauthorized Access to Computer Systems and Service)

(5) การลอกเลียนแบบหรือทำซ้ำโปรแกรมคอมพิวเตอร์ที่ได้รับการคุ้มครองลิขสิทธิ์ (Unauthorized Reproduction of Legally Protected Computer Program)

2.4.4 การแบ่งประเภทอาชญากรรมคอมพิวเตอร์ของเดวิท ไอคอป, คาร์ล ซีเกอร์ และวิลเลียม วันสโตร์

เดวิท ไอคอป (David Icove), คาร์ล ซีเกอร์ (Karl Seger) และวิลเลียม วันสโตร์ (William Vonstorch) ผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ได้จำแนกเป้าหมายในการสู่รูจมของอาชญากรรมคอมพิวเตอร์ไว้ในหนังสือเรื่อง Computer Crime : A Crimefighter's Handbook ไว้เป็น 6 ลักษณะ ได้แก่ (David Icove, 1995 : 5)

(1) การสู่รูจมคอมพิวเตอร์ทางทหารและการข่าวกรองโดยหน่วยก่อวินาศกรรม

คอมพิวเตอร์ทางการทหารและข่าวกรอง ส่วนใหญ่จะเป็นพวกจารชน ในยุคโลกาภิวัฒน์ประเทศมหาอำนาจต่าง ๆ จะนำเทคโนโลยีสมัยใหม่เก็บข้อมูลข่าวสารสนเทศซึ่งถือว่าเป็นความลับของชาติไว้ในคอมพิวเตอร์ เช่น การกำหนดตำแหน่งดาวเทียมกองทัพอากาศ เพื่อการวางกองกำลังทหารทั่วโลก ขณะที่จารชนทราบดีว่าคอมพิวเตอร์อยู่ที่ใดที่นั่นจะมีข้อมูลความลับยิ่งนานไปการจารกรรมก็เสมือนกับกีฬาการลอบเข้าไปในระบบคอมพิวเตอร์

เมื่อเดือนมกราคม ค.ศ.1990 พนักงานบริษัท Silicon Valley 3 คนถูกจับกุมดำเนินคดีในความผิดฐานบุกรุกเข้าไปในระบบคอมพิวเตอร์ของรัฐบาลสหรัฐฯ ซึ่งเก็บความลับของชาติ เกี่ยวกับการฝึกซ้อมรบของการทหาร แผนการบินทหาร รายงานการสืบสวนสอบสวนของตำรวจ เอฟบีไอ. เกี่ยวกับประธานาธิบดี เฟอร์ดินัน มาร์กอส รวมทั้งความลับทางการทหารอื่น ๆ

(2) การสู่รูจมคอมพิวเตอร์ธุรกิจโดยคู่แข่งการค้า

คอมพิวเตอร์องค์กรธุรกิจต่าง ๆ อาจตกเป็นเป้าหมายของบริษัทคู่แข่งโดยเฉพาะเมื่อหมดยุคสงครามเย็น แล้วก้าวสู่ยุคสงครามเศรษฐกิจที่แผ่ขยายไปทั่วโลก มีการแข่งขันทางเศรษฐกิจระหว่างประเทศ ปรากฏว่าส่งผลนำไปสู่การเกิดสงครามจารกรรมทาง

อุตสาหกรรม แม้ว่าในทางเปิดเผยจะมีสัมพันธภาพกันแน่นแฟ้น แต่ในทางเศรษฐกิจเป็นศัตรูกัน เช่น คดี บริษัทเครื่องบิน โบอิ้ง กล่าวหาบริษัทแอร์บัสของฝรั่งเศสว่าลอบดักฟังการสนทนาโทรศัพท์ของพนักงานบริษัทโบอิ้งในโรงแรมแห่งหนึ่ง เรื่องการจำหน่ายที่นั่งของสายการบิน เพื่อเอาความลับของบริษัทไป

(3) การสู่โจมคอมพิวเตอร์การเงินและการธนาคารโดยอาชญากรมืออาชีพ

ธนาคารและสถาบันทางการเงินอื่น ๆ มักตกเป็นเป้าหมายของกลุ่มอาชญากรอาชีพ โดยในยุคโลกาภิวัฒน์เงินมักจะถูกนำไปพิมพ์เป็นตัวเลขปรากฏบนจอคอมพิวเตอร์หรือบนรายงานทางบัญชีธนาคาร การนำฝากเช็คหรือถอนเงินสดด้วยเช็คสามารถทำได้โดยทางอิเล็กทรอนิกส์ การชำระเงินค่าสาธารณูปโภคต่าง ๆ ด้วยระบบอิเล็กทรอนิกส์ การหักชำระหนี้บัญชีกระแสรายวันด้วยระบบอิเล็กทรอนิกส์ จึงเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่จะมีการลักทรัพย์สินหรือการทุจริต ฉ้อโกงทางอิเล็กทรอนิกส์ เช่นกัน

อาชญากรคอมพิวเตอร์ มักพุ่งเป้าหมายไปยังคอมพิวเตอร์ของธนาคารสถาบันการเงิน ดังตัวอย่างของคดีที่เกิดขึ้นแล้วในสหรัฐอเมริกา เช่น เมื่อต้นปี ค.ศ.1988 กลุ่มอาชญากรคอมพิวเตอร์จำนวน 7 คนวางแผนเพื่อทำการลักลอบโอนเงินของ First National Bank of Chicago โดยกลุ่มคนร้ายพยายามโอนเงินทาง With Transfer ออกจากบัญชีเงินฝากของ

1. Merrill Lynch and Company จำนวน 23.57 ล้านเหรียญสหรัฐฯ
2. United Airlines จำนวน 25 ล้านเหรียญสหรัฐฯ
3. Brown-Forman Corporation จำนวน 19.75 ล้านเหรียญสหรัฐฯ

เพื่อโอนไปเข้าบัญชีของพรรคพวกตนที่ไปเปิดบัญชีรอรับการโอนไว้ที่ธนาคาร New York แล้วจากนั้นพยายามโอนต่อไปยังธนาคารที่ 2 ในกรุงเวียนนา โดยมีการอนุมัติการโอนเช่นว่านั้นทางโทรศัพท์ และจากนั้นธนาคารที่โอนเงินทำการโทรศัพท์เพื่อตรวจสอบยืนยันการโอนเงินข้างต้น การโทรศัพท์ตรวจสอบดังกล่าวสามารถนำไปสู่แหล่งที่กบดานและจับกุมคนร้าย หากว่ากลุ่มคนร้ายมีความฉลาดมากกว่านี้ หรือทำการเร็วขึ้นอีกหน่อย เงินทั้งหมด 70 ล้านเหรียญสหรัฐฯ คงอันตรธานไปด้วย

การประทุษร้ายต่อสถาบันการเงิน มักจะเป็นบุคคลภายในสถาบันการเงินนั้นเอง โดยอาศัยเหตุที่ตนเป็นผู้มีความรู้ ความสามารถ ดังอีกคดีหนึ่งคือในปี ค.ศ.1994 วิศวกรสลับสาย (Switch Technician) ถูกเจ้าหน้าที่ตำรวจจับกุมดำเนินคดี เนื่องจากลักลอบเอาข้อมูลบัตรเครดิตหลายพันหมายเลขออกไปจำหน่ายให้กับกลุ่มคนร้าย ยังผลทำให้เกิดความเสียหายเป็นเงินรวมประมาณ 50 ล้านเหรียญสหรัฐฯ

เมื่อเดือน กุมภาพันธ์ ค.ศ.1989 มีคดีการทุจริตฉ้อโกงค่าโทรศัพท์ซึ่งถือว่าเป็นอาชญากรรมคอมพิวเตอร์ เกิดขึ้นและนำเป็นห่วงสำหรับอุตสาหกรรมโทรคมนาคม นักโทษ 15 คนซึ่งต้องโทษอยู่ในเรือนจำเมโทร ในตำบลเดวิดสัน เมืองแนชวิล มลรัฐเทนเนสซี่ ลักลอบเข้าไปในบัญชีโทรศัพท์ผู้อื่นแล้วใช้โทรศัพท์ทางไกล เพียงช่วงหนึ่งวันหยุดสุดสัปดาห์เกิดความเสียหาย 2,000 เหรียญสหรัฐฯ โดยนักโทษที่ลักลอบเข้าไปในระบบคอมพิวเตอร์ได้ทำการลักเอารหัสลับของลูกค้าออกมาจำหน่ายให้นักโทษอื่นในราคา 5 เหรียญสหรัฐฯ เพื่อนำไปใช้หรือนำเอาออกให้เช่าใช้โทรศัพท์ในอัตราครั้งละ 1.25 เหรียญสหรัฐฯ

(4) การจู่โจมคอมพิวเตอร์หน่วยงานของรัฐบาลและของบริษัท สาธารณูปโภคเพื่อการก่อการร้าย

คอมพิวเตอร์ของหน่วยงานราชการและบริษัทสาธารณูปโภคต่าง ๆ มักตกเป็นเป้าหมายของกลุ่มผู้ก่อการร้าย (Terrorists)

(5) การจู่โจมของบริษัททั่วไปซึ่งตกเป็นเป้าหมายแก่พนักงานหรืออดีตพนักงานในทำนองเดียวกัน คอมพิวเตอร์ของมหาวิทยาลัยตกเป็นเป้าหมายแก่นักเรียนหรือนักศึกษาในเครื่องแบบ

คอมพิวเตอร์ของบริษัท ห้างร้านที่มักเป็นเป้าหมายของการกระทำของพนักงาน ลูกจ้าง หรืออดีตพนักงานลูกจ้าง ในขณะที่คอมพิวเตอร์ของมหาวิทยาลัยมักเป็นเป้าหมายการกระทำของนิสิต นักศึกษาหรืออดีตนิสิต นักศึกษาสถาบันนั้น ๆ

(6) การจู่โจมคอมพิวเตอร์ขององค์กรต่าง ๆ ซึ่งตกเป็นเป้าหมายของอาชญากรคอมพิวเตอร์ ซึ่งในบางครั้งอาชญากรคอมพิวเตอร์ จะเข้าไปในระบบเพื่อแลกเปลี่ยนความรู้และในบางครั้งอาจจะกระทำการโดยได้รับการว่าจ้าง

คอมพิวเตอร์ขององค์กรหน่วยงานที่มักตกเป็นเป้าหมายของพวกอาชญากร แม้ว่าบางครั้งพวกเหล่านี้อาจลักลอบเข้าไปในระบบคอมพิวเตอร์เพื่อทดลองภูมิปัญญา แต่ในขณะที่พวกมืออาชีพจะรับจ้างเพื่อลักลอบเข้าไปในระบบคอมพิวเตอร์ของผู้อื่น

2.4.5 **อาชญากรคอมพิวเตอร์** (Computer Criminals)

การประกอบอาชญากรรมอะไรก็ตามต้องถือว่าเป็นความผิด และในโลกนี้เกือบทุก ๆ คนต่างก็เคยทำผิดอะไรบ้างไม่มากก็น้อย ตั้งใจบ้างไม่ตั้งใจบ้าง ฉะนั้นอาชญากรคอมพิวเตอร์ก็มักจะเป็นคนธรรมดา ๆ ไม่ผิดแผกแตกต่างไปจากคนอื่น ๆ นอกจากว่าเขาจะเป็นคนที่มีปัญหาจะต้องแก้และเขาคิดหาวิธีแก้แตกต่างไปจากคนอื่น คือใช้คอมพิวเตอร์ช่วยแก้ในการโกง อาชญากรคอมพิวเตอร์มักจะเป็นผู้ได้รับความไว้วางใจ ฉะนั้นจึงถือโอกาสใช้ความไว้วางใจนั้นให้เป็นประโยชน์ในการแก้ปัญหา ศาสตราจารย์ โดนัลด์ เครสซีย์ (Donald Cressey) จากมหาวิทยาลัยแคลิฟอร์เนีย (University of California at Santa Barbara) ได้สัมภาษณ์อาชญากรในอเมริกาเป็นจำนวนมาก และสรุปว่าอาชญากรคอมพิวเตอร์จะคิดว่า เขายืมเงินไปเพียงชั่วคราวและคิดว่าการกระทำของเขาไม่ได้เป็นความผิดเพราะไม่ได้ขโมยและเมื่อ "ขอยืม" บ่อย ๆ เข้าก็ติดเป็นนิสัย สันดาน กลายเป็นอาชญากรไปโดยไม่ได้ตั้งใจ อาชญากรประเภทอื่นอาจจะเป็นชายมากกว่าหญิง ทางด้านคอมพิวเตอร์ในตอนแรก ๆ จะมีชายมากกว่าหญิง แต่สมัยปัจจุบันมีผู้หญิงมากขึ้น ส่วนมากผู้หญิงจะเป็นผู้สนับสนุนมากกว่าที่จะเป็นตัวการ ผู้หญิงมักจะเป็นพนักงานเตรียมข้อมูลหรือพนักงานควบคุมข้อมูลออก เช่น พนักงานเตรียมข้อมูลหญิงในศูนย์คอม-พิวเตอร์ ตำรวจจราจรพบว่าไม่มีการตรวจสอบย้อนหลังสำหรับใบสั่งความผิดทางจราจร คือเมื่อส่งข้อมูลจากใบสั่งเข้าเครื่องคอมพิวเตอร์แล้วจะไม่มีการกลับไปดูที่ต้นฉบับใบสั่งอีก ติดตามเฉพาะข้อมูลที่อยู่ในคอมพิวเตอร์เท่านั้น ฉะนั้นพนักงานหญิงเหล่านั้นเริ่มคดโกงโดยการไม่ใส่ข้อมูลใบสั่งที่ตนเองได้รับเข้าเครื่องคอมพิวเตอร์ช่วยญาติพี่น้อง ต่อไปก็ช่วยเพื่อนจนในที่สุดถูกจับได้ เพราะช่วยหลายคนเกินไป อาชญากรคอมพิวเตอร์ในอเมริกาส่วนมากเป็นคนหนุ่มสาว อายุระหว่าง 18-30 ปี ประมาณว่าร้อยละ 20 ของอาชญากรคอมพิวเตอร์ยังอยู่ในวัยเรียนมหาวิทยาลัย เท่าที่ผ่านมาอาชญากรคอมพิวเตอร์ส่วนมากเป็นนักคอมพิวเตอร์หรือผู้ที่มีความรู้ความสามารถ มีสิทธิหน้าที่ต้องใช้คอมพิวเตอร์ อาชญากรอาชีพมักจะไม่มีความรู้ด้านคอมพิวเตอร์ พอที่จะประกอบ

อาชญากรรม ฉะนั้นจะต้องสร้างระบบการป้องกันอาชญากรรมคอมพิวเตอร์ขึ้นโดยถือหลักว่าอาชญากรมีความรู้ด้านคอมพิวเตอร์เท่า ๆ กับนักคอมพิวเตอร์ที่ออกแบบระบบป้องกัน

เหตุจูงใจ (Motives) ในการประกอบอาชญากรรมคอมพิวเตอร์ บรรดาอาชญากรทั้งหลายมักจะมีเหตุจูงใจในทำนองเดียวกัน คือการประกอบอาชญากรรมเป็นการท้าทายและเป็นการเล่นเกม (Challenge and Game Playing) อาชญากรบางคนคิดว่าการประกอบอาชญากรรมคอมพิวเตอร์ไม่ได้เป็นการกระทำผิด แต่เป็นเรื่องที่คนทั่วไปก็มักจะกระทำกัน ซึ่งเป็นการกระทำแบบที่เรียกว่า Vending Machine Syndrom คือ ถ้าเราไปพบเงิน 2-3 เหรียญใน Vending Machine หรือในโทรศัพท์สาธารณะก็จะเก็บเงินนั้นไว้โดยไม่พยายามสืบหาเจ้าของ ดร.สแตนเลย์ วินเกอร์ (Dr. Stanley Winkler) จากบริษัท IBM ได้ทดลองเรื่องนี้ในประเทศต่าง ๆ คือในระหว่างที่รอเครื่องบินตามท่าอากาศยาน ท่านจะไปที่ตู้โทรศัพท์สาธารณะและโทรบอกพนักงานรับโทรศัพท์ (Operator) ว่าเก็บเงินได้ 2-3 เหรียญ ในตู้โทรศัพท์จะให้คืนให้ที่ไหน พนักงานรับโทรศัพท์ทุกแห่งจะบอกว่าไม่ต้องส่งคืนที่ใดทั้งนั้น ถ้าพิจารณาในแง่นี้ ทุกคนที่เก็บเงินจากตู้โทรศัพท์สาธารณะมาใช้ในการโทรศัพท์หรือเก็บไว้เฉย ๆ ก็เป็นอาชญากรทั้งนั้น แต่ข้อแตกต่างระหว่างผู้ที่เก็บเงินจากตู้โทรศัพท์กับอาชญากรคอมพิวเตอร์ก็คือจำนวนเงินที่อาชญากรคอมพิวเตอร์เก็บมาโดยใช้คอมพิวเตอร์นั้นมักจะเป็นจำนวนมาก โดยที่ผู้ประกอบอาชญากรรมถือว่าตนเล่นเกมชนะคอมพิวเตอร์จึงได้เงินนั้นมา ในวงการคอมพิวเตอร์มักจะถือกันว่าการทดลองสั่งให้คอมพิวเตอร์ทำอะไรที่ไม่มีในตำราเป็นการเล่นเกมชนิดหนึ่ง ดังจะสังเกตได้ว่านักศึกษาคอมพิวเตอร์จะแข่งขันกันว่า ใครจะมีความสามารถมากกว่ากันในการสั่งให้เครื่องคอมพิวเตอร์ทำอะไรที่เครื่องไม่ควรจะทำ เมื่อทำเล่น ๆ ตอนเป็นนักศึกษาได้พอจบไปทำงานก็อาจจะลองทำเอาเงินได้

ข้อแตกต่างระหว่างอาชญากรคอมพิวเตอร์และอาชญากรอื่น ๆ คือ อาชญากรคอมพิวเตอร์มักจะกลัวถูกจับได้และลักษณะการกระทำจะสมรู้ร่วมคิดกันหลายคน การกลัวถูกจับได้มักจะไม่ใช่เรื่องน่ากลัวสำหรับอาชญากรอาชีพ แต่กลับต้องการให้มีข่าวลงหนังสือพิมพ์เพื่อจะได้รู้อ้วดกับอาชญากรด้วยกันว่าเป็นฝีมือของตนเอง แต่อาชญากรคอมพิวเตอร์มักจะเป็นมือสมัครเล่นเป็นผู้มีงานการทำเป็นหลักฐาน ถ้าถูกจับได้ก็จะอับอายขายหน้าเสียชื่อเสียง

จากแฟ้มอาชญากรรมคอมพิวเตอร์ในประเทศสหรัฐอเมริกา กรณีส่วนมากจะเป็นการสมรู้ร่วมคิดกันหลายคน โดยเฉพาะอย่างยิ่งในกรณีการยักยอกทรัพย์ที่เกินสองแสนบาทขึ้น

ไป ถ้าเป็นการกระทำโดยไม่ใช้คอมพิวเตอร์ ผู้กระทำผิดมักจะกระทำด้วยตนเองถึงประมาณ 90% แต่ถ้าเป็นการกระทำโดยใช้คอมพิวเตอร์จะมีการร่วมมือกันถึง 50% โดยทั่ว ๆ ไปแล้ว นักโปรแกรม (Programmer) และพนักงานปฏิบัติการห้องคอมพิวเตอร์ (Computer Room Operator) มักจะไม่ร่วมมือกันประกอบอาชญากรรม จากประวัติ 175 กรณี มีการร่วมมือกันระหว่างนักโปรแกรมกับนักปฏิบัติการเพียง 4 กรณี ทั้งนี้เป็นเพราะนักโปรแกรมกับพนักงานปฏิบัติการมักจะไม่ถูกกัน นักโปรแกรมมักจะเรียกร้องให้พนักงานปฏิบัติการแสดงความรู้ความสามารถมากขึ้นให้สามารถตัดสินใจทำงานเองได้มากขึ้น แต่พนักงานปฏิบัติการมักจะมีการศึกษาและการฝึกอบรมต่ำกว่า จึงพยายามเรียกร้องให้นักโปรแกรมเขียนคำสั่งให้ชัดเจนทุกขั้นตอน ยิ่งกว่านั้นถ้านักโปรแกรมคิดจะประกอบอาชญากรรมคอมพิวเตอร์เขาก็จะทำได้โดยไม่ต้องให้พนักงานปฏิบัติการช่วยในทำนองเดียวกัน ถ้าพนักงานปฏิบัติการคิดจะคดโกงเขาก็จะไม่ไปปรึกษานักโปรแกรม ส่วนใหญ่จะปรึกษากับพนักงานปฏิบัติการด้วยกันเอง

การจำแนกอาชญากรคอมพิวเตอร์ อาจแยกออกตามประเภทและลักษณะการกระทำผิดของบุคคลได้ดังนี้คือ

(1) พวกมือใหม่ (Novice) บุคคลที่จัดอยู่ในกลุ่มนี้มักเป็นผู้ที่พึ่งมาทำการศึกษาหาความรู้ในด้านเทคโนโลยีคอมพิวเตอร์ เข้าใจและเข้าถึงวิธีการใช้และสมรรถนะของเครื่องคอมพิวเตอร์ว่าอยู่จุดใด จึงทำให้เกิดประสบการณ์จากการทดลองใช้เครื่องคอมพิวเตอร์ การทดลองทำรายการครั้งแล้วครั้งเล่าจนเกิดความชำนาญขึ้นมา เท่าที่ปรากฏในอดีตบุคคลในกลุ่มนี้ยังไม่เคยถูกเจ้าหน้าที่จับกุมมาสอบสวนดำเนินคดี อันเนื่องมาจากการกระทำผิดเกี่ยวกับคอม-พิวเตอร์มาก่อนเลย เพราะพวกนี้เมื่อทำผิดครั้งเดียวแล้วก็จะหลบหน้าหายไปไม่ไปสร้างความเสียหายแก่ผู้เป็นเจ้าของระบบอีก

บางครั้งลักษณะของอาชญากรแบบนี้เป็นพวกต้องการทราบหรือต้องการเข้าถึงข้อมูล บุคคลเหล่านี้รู้รหัสผ่านเพื่อเข้าไปยังฐานข้อมูลนั้นและมีเป็นจำนวนมากที่เป็นลูกจ้างหรือพนักงานของหน่วยงานนั้น ๆ เอง ซึ่งบุคคลประเภทนี้มิได้เป็นอาชญากรโดยแท้จริงเพียงแต่ใช้โอกาสในตำแหน่งหน้าที่ที่มีอยู่เข้าไปดำเนินการกับข้อมูลคอมพิวเตอร์

(2) พวกกวนประสาท (Deranged Person) คนจำพวกนี้มักมีความผิดปกติอยู่ในตัวเองชอบทำในสิ่งที่รุนแรงมีอาการทางประสาทและที่ต้องระวังคือ เป็นพวกที่เป็นอันตราย

ต่อวงการคอมพิวเตอร์ที่เดียวแต่หากพูดถึงขีดความสามารถของพวกนี้แล้ว มือยังไม่ถึงขั้นที่จะเจาะระบบป้องกันที่มีรหัสป้องกันเพื่อเข้าไปทำอันตรายต่อแฟ้มข้อมูล ที่น่าเป็นห่วงคือทำอันตรายต่อระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ซึ่งยิ่งเสียหายหนัก บุคคลพวกนี้มักเน้นสร้างความเสียหายต่อเครื่องคอมพิวเตอร์และบุคลากรผู้ใช้เครื่อง

(3) พวกองค์กรอาชญากรรม (Organized Crime) กลุ่มบุคคลพวกนี้เป็นสมาชิกขององค์กรอาชญากรรมที่มีเจตนาในการประกอบอาชญากรรม เช่น การลักลอบค้ายาเสพติด บ่อนการพนัน การฆ่ากรรโชก การค้าประเวณี ฯลฯ จึงนำเอาเครื่องคอมพิวเตอร์ของตนเองมาใช้เป็นเครื่องอำนวยความสะดวกเพื่อเก็บข้อมูลเสมือนหนึ่งว่าเป็นหน่วยงานธุรกิจ หน่วยงานหนึ่ง และใช้คอมพิวเตอร์เป็นเครื่องมือ หรืออุปกรณ์ในการกระทำผิดที่มุ่งกระทำต่อองค์กรอื่น ๆ ที่ใช้เครื่องคอมพิวเตอร์เป็นอุปกรณ์หลักในการทำงานปกติ บางครั้งอาจลักลอบเข้าไปดูข้อมูลในการสืบสวนสอบสวนของเจ้าหน้าที่ผู้รักษากฎหมายที่ทำการสืบสวนสะกดรอยความเคลื่อนไหวของกลุ่มองค์กรอาชญากรรมตนเอง

(4) พวกคนร้ายอาชีพ (Career Criminals) บุคคลประเภทนี้มักเป็นการรวมตัวกันของผู้ที่เคยถูกจับกุมหรือถูกดำเนินคดีในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์มาก่อน แต่จะมีขนาดกลุ่มเล็ก ๆ พวกนี้ชอบหาเงินในทางที่ใช้ความรู้ทางคอมพิวเตอร์ไปลอกเลียนแบบงานของผู้อื่นเพื่อขายเอาเงินเข้ากระเป๋าตนเอง

(5) พวกหัวรุนแรง (Ideologues) บุคคลประเภทนี้มีมูลเหตุจูงใจในการกระทำผิดอาชญากรรมคอมพิวเตอร์ โดยมีความเชื่อในแนวความคิดว่าจะต้องเข้าไปสร้างพฤติกรรมที่ก่อให้เกิดความเสียหายหรือทำลายเพื่อเป็นการประกาศตน

(6) พวกแหกด่านลองดี/พวกทำลาย (Hacker/Cracker) สำหรับบุคคลประเภทนี้มีพฤติกรรมที่ชอบลักลอบเจาะด่านป้องกัน (Security) ที่มีการตั้งรหัสผ่าน (Password) เพื่อเข้าไปใช้ระบบคอมพิวเตอร์หรือดูแฟ้มข้อมูลของบุคคลอื่น ซึ่งอาจแยกอธิบายถึงลักษณะของพฤติกรรมของ Hacker/Cracker ได้ดังนี้

ลักษณะของ Hacker/Cracker

- เป็นผู้ที่มีความฉลาด เรียนรู้เร็ว
- เป็นผู้ที่มีความหยิ่ง ทรนงว่าตนเองเหนือผู้อื่น

- เป็นผู้ที่ชอบหาความบันเทิงในชีวิตด้วยคอมพิวเตอร์และใช้ในทางที่ผิด
- เป็นชายมากกว่าหญิง
- เป็นผู้ชอบแสดงความสามารถ
- เป็นนักสะสมข้อมูล

Hacker/Cracker จัดเป็นบุคคลที่มีความรู้และความชำนาญเป็นเลิศในอันที่จะลักลอบเข้าไปในระบบคอมพิวเตอร์ หรือแฟ้มข้อมูลคอมพิวเตอร์ของผู้อื่น แต่วัตถุประสงค์ของ Hacker/Cracker แตกต่างกันคือ

พวกแหกด่านลองดี (Hacker) เป็นบุคคลผู้มีความรู้และความชำนาญทางด้านคอมพิวเตอร์ ชอบลักลอบเข้าไปในระบบคอมพิวเตอร์ของผู้อื่น โดยเฉพาะระบบคอมพิวเตอร์ที่มีการตั้งรหัสผ่าน (Password) แล้วก็จะให้คำแนะนำในการตั้งระบบการป้องกันให้ดีกว่าที่เป็นอยู่

พวกทำลาย (Cracker) ก็จัดเป็นบุคคลที่มีความรู้ความชำนาญเป็นเลิศในการที่จะลักลอบเข้าไปในระบบคอมพิวเตอร์หรือแฟ้มข้อมูลของผู้อื่น แต่กลุ่มนี้มีวัตถุประสงค์เพื่อเข้าไปทำลายก่อให้เกิดความเสียหายด้วยการลบแฟ้มข้อมูลทำให้เครื่องคอมพิวเตอร์เสียทำงานไม่ได้ หรือรบกวนการทำงานของระบบคอมพิวเตอร์

เกี่ยวกับพฤติกรรมของ Hacker/Cracker ครั้งหนึ่ง ศาสตราจารย์โดโรธี เดนนิ่ง (Professor Dorothy Denning of Georgetown University) ได้มีความเห็นในเอกสารการวิจัยของตนเองในปี ค.ศ.1990 ว่า Hacker เป็นพวกเรียนรู้ นักสำรวจที่ชอบช่วยเหลือมากกว่าทำลาย สมควรที่จะทำงานใกล้ชิดด้วย แต่ในที่สุดในปี 1995 ก็ได้ลงความเห็นใหม่ว่า Hacker เป็นพวกที่มีความพอใจที่ได้ดูถูกความผู้อื่น พวกนี้รู้ว่าผิดก็ยังกระทำจึงไม่ควรให้พวก Hacker มาร่วมงานด้วย

(7) พวก Snooping หรือ พวก Cyber-Voyeurism จัดเป็นพวกมีความรู้เรื่องระบบคอมพิวเตอร์เป็นอย่างดี และมีความสามารถเข้าถึงฐานข้อมูลต่าง ๆ โดยหลีกเลี่ยงและผ่านรหัสลับ (Password) เช่นเดียวกัน Hacker/Cracker แต่พวก Snooping นี้มีวัตถุประสงค์เพียงแค่เข้าถึงและตรวจดูว่าในฐานข้อมูลหรือระบบคอมพิวเตอร์ต่าง ๆ นั้นมีอะไรอยู่บ้าง หากมีข้อมูลหรือโปรแกรมที่น่าสนใจก็จะคัดลอก (Copy) เอามาไว้เป็นของตนเอง

2.5 คดีอาชญากรรมคอมพิวเตอร์ในต่างประเทศและในประเทศไทย

2.5.1 ตัวอย่างอาชญากรรมคอมพิวเตอร์จากการรวบรวมของมหาวิทยาลัยมิชิแกน-สเตท ประเทศสหรัฐอเมริกา

จากเอกสารประกอบการสัมมนา เรื่องสภาพปัญหาและแนวโน้มอาชญากรรมคอมพิวเตอร์ได้ ยกตัวอย่างคดีอาชญากรรมคอมพิวเตอร์ในประเทศสหรัฐอเมริกา โดย Case Studies เป็นเรื่องที่เกิดขึ้นจากรายงานข่าวทางหน้าหนังสือพิมพ์ และเป็นเรื่องที่เกิดจากประสบการณ์ของผู้ฝึกอบรม ซึ่งได้เข้ามามีส่วนร่วมดำเนินการสืบสวนสอบสวน เพื่อจับกุมผู้กระทำผิดมาลงโทษ ได้แก่ (David Carter, 1996 : 4-11)

- **พวกอาชญากรรมเกี่ยวกับเด็ก** มีเด็กอายุ 14 ปี ในรัฐฟลอริด้า ได้มีเพศสัมพันธ์กับผู้ใหญ่ ซึ่งเธอพบในการสื่อสารโดยอินเตอร์เนต หรือคดีอาจเกิดขึ้นโดยการติดต่อกันในอินเตอร์เนต โดยผู้กระทำผิดพยายามสร้างความเชื่อ ความไว้วางใจ เพื่อนำไปสู่ความผิดทางเพศหรือการลักพาตัวและการสนทนาโดยคอมพิวเตอร์ได้แพร่หลายมากขึ้น โดยเด็กไม่ได้ทราบถึงอันตรายที่เกิดขึ้น ผลดังกล่าวทำให้เด็กถูกล่อลวงไปในการกระทำผิดมากขึ้น

- **สิ่งลามกเด็ก** ปรากฏว่าอินเตอร์เนตสามารถเป็นสื่อในการกระจายรูปภาพดังกล่าวไปได้ตามสาย และสามารถมีผู้รับได้มากมายเพราะสามารถทำได้เร็ว ง่าย ถูกและหลากหลาย เคยมีตัวอย่างเจ้าหน้าที่ศุลกากรของสหรัฐ สามารถจับผู้กระทำความผิดเกี่ยวกับการเผยแพร่รูปภาพลามกเด็กในอินเตอร์เน็ตได้จำนวนมาก

- **สื่อลามกอนาจาร** ในสหรัฐอเมริกา มีการค้าภาพลามกอนาจารโดยสามารถพัฒนาและแพร่ขยาย ด้วยการหลบเลี่ยงกฎหมายที่มีอยู่ไปได้

- **อาชญากรรมทางเพศ** การที่สามารถติดต่อสื่อสารได้อย่างกว้างขวางทำให้เป็นการง่ายในการก่ออาชญากรรม เพราะเจอเหยื่อได้ง่าย มีตัวอย่างในสหรัฐอเมริกาที่รัฐรอริกอน มีชายอายุ 19 ปี ถูกตัดสินจำคุก 30 วัน และถูกทำทัณฑ์บนไว้ 5 ปี สำหรับการกระทำผิดทางเพศกับเด็กหญิงอายุ 14 ปี ที่รู้จักกันบนอินเตอร์เนต จากการวิจัยในสหรัฐทำให้ทราบว่ามีการเพิ่มขึ้นของการเผยแพร่ภาพลามก และความผิดทางเพศมากขึ้น

- **การข่มขู่หรือทำให้เสียหาย** มีการกระทำผิดในลักษณะนี้โดยแพร่หลายในสหรัฐ ด้วยการใช้อี-เมล (Electronic Mail) มีคดีตัวอย่างที่มหาวิทยาลัยมิชิแกน นักศึกษาชายถูกจำคุกในข้อหาข่มขู่ เนื่องจากการใช้อี-เมล เพราะการสร้างรูปภาพลงในระบบเชื่อมตรง (on line) คอมพิวเตอร์เกี่ยวกับผู้หญิงซึ่งถูกข่มขืนและทรมานโดยใช้ชื่อเพื่อนเป็นผู้หญิงคนนั้น

- **การก่อกวนหรือรังควาน** เป็นที่กล่าวกันว่าการใช้ภาษาลามกในคอมพิวเตอร์หรือรูปภาพโดยผ่าน On Line เพิ่มมากขึ้นตลอดมา แต่ในอนาคต เมื่อคอมพิวเตอร์สามารถทำให้เราใช้ได้เสมือนทำด้วยตนเอง อาชญากรรมประเภทนี้ก็จะยิ่งมากขึ้น เพราะเทคโนโลยีเข้ามามีบทบาทในชีวิตของคนเรามากขึ้น นั่นหมายถึงย่อมมีทั้งสิ่งที่ดีและไม่ดีเกิดขึ้นในการพัฒนาเทคโนโลยี

- **การทำร้าย** คนเรายิ่งพัฒนาความคิดในการก่อกวน ข่มขู่เท่าไหร่ คอมพิวเตอร์ก็สามารถสนองความประสงค์ของผู้คิดได้เสมอ และการที่อี-เมล สามารถทำงานได้อย่างรวดเร็ว ทำให้การใช้ถ้อยคำแม้มีจำนวนมากก็สามารถส่งไปยังเป้าหมายได้อย่างรวดเร็ว บางกรณีผู้ที่ตกเป็นผู้เสียหายในเรื่องนี้เกิดขึ้นจากการลงชื่อเป็นสมาชิกใช้บริการอินเตอร์เน็ต มีตัวอย่างคดีหนึ่งที่พวก Hacker ได้เจาะเข้าไปในองค์การโทรศัพท์ และแก้ข้อมูลของโทรศัพท์ประจำบ้านให้กลายเป็นโทรศัพท์สาธารณะ ซึ่งทุกครั้งเจ้าของบ้านจะใช้ จะมีเสียงบอกให้หยอดเหรียญทุกครั้ง

- **การฉ้อโกงและฆาตกรรม** ปัจจุบันค่อนข้างง่ายที่จะทำอาชญากรรมเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ โดยผ่านข้อมูลในคอมพิวเตอร์ และมีคดีฆาตกรรมหนึ่งในเท็กซัส ซึ่งมีผู้แก้ไขข้อมูลเกี่ยวกับการรักษาคนป่วย ทำให้คนไข้นั้นตาย โดยผู้กระทำหวังเงินประกันชีวิต และมีคดีฆาตกรรมอีกคดีหนึ่ง โดยมีหญิงจากมารีแลนด์พบถูกฆ่าตายอยู่หลังบ้านของชายคนหนึ่งใน North Carolina อันสืบเนื่องมาจากการติดต่อแบบชู้สาวกันทางอี-เมล โดยฝ่ายชายบรรยายถึงวิธีการที่จะทรมานเธอ และฆ่าเธอหลังจากมีสัมพันธ์กัน ซึ่งการค้นพบศพหญิงนั้นเนื่องจากข้อความที่หญิงแจ้งแก่สามีเธอ และเนื้อหาในอี-เมล ที่ยึดได้จากคอมพิวเตอร์ผู้ชาย

- **การไล่ล่าหรือไล่ตาม** (Cyber - Stalking) เป็นคดีที่มิชิแกนชายอายุ 32 ปี ถูกลงโทษในการใช้อี-เมล ไล่ตามผู้หญิงที่เจอกันโดยบริการหาคู่ ซึ่งกรณีดังกล่าวเกิดขึ้นในหลายพื้นที่ในสหรัฐ ที่เกี่ยวกับการติดตามตัวของบุคคลอื่น

- **อั้งยี่ในเมือง** มีอินเตอร์เนตช่องหนึ่งที่เป็นจุดติดต่อของพวกสมาชิกแก๊งค์ระหว่างประเทศ เรียกว่า "Glock 3" และภาษาที่ใช้หยาบคาย รุนแรง และใช้อินเตอร์เนตเป็นอุปกรณ์ต่อต้านศัตรู

Glock 3 มีไว้สำหรับให้ข้อมูลเป้าหมายและข่าวสาร ข้อมูลที่ติดต่อกับแก๊งค์อื่น ใช้แจ้งวิธีการกระทำผิด ใช้เข้าร่วมกระทำความผิดเป็นการร่วมกันใช้ข้อมูลเกี่ยวกับการทำงานของแก๊งค์ติดต่อกันโดยใช้อี-เมล ช่องดังกล่าว ยังช่วยสนับสนุนให้สมาชิกของแก๊งค์ก่อกวน ผู้ที่ไม่เห็นด้วยหรือดูถูกกลุ่มตนทาง อี-เมล

- **พวกกบฏหรือพวกก่อกวน** ผู้ใช้คอมพิวเตอร์สามารถหาวิธีเข้าไปในระบบคอมพิวเตอร์จากโค้ดลับต่าง ๆ จนถึงขนาดสามารถควบคุมจรวดในระยะไกลได้ บางกลุ่มเพื่อเป็นการยุแหย่เจ้าหน้าที่ของรัฐ โดยใส่ข้อมูลเพื่อแจ้งให้ผู้อ่านทราบถึงวิธีการฆ่าตัวตาย วิธีการช่วยตัวเอง วิธีการที่นักเรียนจะระเบิดห้องน้ำ หรือเข้าไปในโรงเรียนเวลากลางคืนเพื่อเผาโรงเรียน มีข้อมูลหลากหลายในวิธีการที่จะก่อกวนหรือทำลายโดยใช้อินเตอร์เนต

- **พวกก่อการร้าย** จากพยานหลักฐานในคดีในสหรัฐพบว่า พวกก่อการร้ายชอบใช้อินเตอร์เนต เป็นเครื่องมือในการแลกเปลี่ยนข้อมูล เพราะปลอดภัยกว่า หลากหลายกว่า แผนของพวกก่อการร้ายในการส่งผ่านอินเตอร์เนต ทำได้ในระยะเวลาสั้นรวดเร็วและจับได้ยาก

- **ช่องโจร** มักใช้คอมพิวเตอร์ในการสั่งการทำงาน เพราะไม่ปรากฏแหล่งที่มา การสั่งการหรือให้ข้อมูลการทำงานทำได้รวดเร็ว การติดต่อสื่อสารได้ทั่วโลก ข้อมูลไม่คลาดเคลื่อน และจับได้ยาก การทำงานของช่องโจร หรือองค์กรอาชญากรรมโดยผ่านอี-เมล อินเตอร์เนตถือเป็นทางที่ดีที่สุดในการส่งข้อมูล พวกช่องโจรมักใช้คอมพิวเตอร์ในการเก็บข้อมูลการกระทำผิด ฟอกเงิน ควบคุมเครื่องมือที่ใช้ในการกระทำผิด การกระทำความผิดอาจประกอบด้วย การทำลายระบบของผู้ที่รู้การทำงานของแก๊งค์มากเกินไป การทำลายผู้ที่หักหลังองค์การ

- **พวกคลั่งลัทธิหรือเหยียดหยามเผ่าพันธุ์** จากการสำรวจของสมาคมชาวยิวพบว่าพวกต่อต้านเผ่าพันธุ์หรือลัทธิ ได้กระจายข้อมูลบนเครือข่าย (Networks) ในยุโรปทางตะวันตกและสหรัฐอเมริกา Neo-Nazis ได้จัดตั้ง Inter Network ใช้ Mailboxes ส่งข้อมูลไปให้นักศึกษาใน 70 ประเทศ

2.5.2 ตัวอย่างอาชญากรรมคอมพิวเตอร์ของ โรเบิร์ต สไนเดอร์

โรเบิร์ต สไนเดอร์ (Robert Synder) นักสืบตำรวจโคลัมบัส มลรัฐโอไฮโอ และที่ปรึกษา บริษัท AT&T และ MCI ด้านอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งเป็นวิทยากรในการฝึกอบรมและสัมมนาได้ยกผลตัวอย่างคดีอาชญากรรมคอมพิวเตอร์ ที่เกิดจากประสบการณ์ของตนเอง ได้เข้ามามีส่วนร่วมดำเนินการสืบสวนสอบสวนเพื่อจับกุมผู้กระทำผิดมาลงโทษ

คดีตัวอย่าง (Case Studies) เหล่านี้เป็นเรื่องที่เกิดจากประสบการณ์ของ โรเบิร์ต สไนเดอร์ ซึ่งได้เข้าไปมีส่วนร่วมดำเนินการสืบสวนสอบสวน เพื่อจับกุมตัวผู้กระทำความผิดมาลงโทษ ส่วนใหญ่ของพวกกระทำความผิดนี้คือพวกอาชญากร ซึ่งมีความรู้ความชำนาญในด้านคอมพิวเตอร์และอาศัยช่องว่างของพัฒนาการเทคโนโลยีเป็นเครื่องมือในการทำงาน โดยปกติกลุ่มบุคคลประเภทนี้บางส่วนเป็นผู้ที่ไม่ประสบผลสำเร็จในการทำงานขององค์กรทั่ว ๆ ไป ทำให้เกิดพฤติกรรมบางประการ ซึ่งมีแนวโน้มที่เป็นอาชญากรรมคอมพิวเตอร์

- การเจาะข้อมูลใน Voice Mail Box เมื่อสามารถทราบถึงเลขที่บัตรเครดิต ชื่อผู้ถือบัตร และวันหมดอายุของบัตรเครดิตแล้วนำข้อมูลดังกล่าวมาใช้กระทำความผิด เช่น การสั่งซื้อของทาง Mail Order ซึ่งส่วนใหญ่ที่อยู่ปลายทางนั้นเมื่อตรวจสอบแล้วจะไม่มีผู้อาศัยอยู่ หรืออาจจะเป็นตู้รับฝากไปรษณีย์ภัณฑ์ นอกจากนี้แล้วกลุ่มผู้ค้ายาเสพติดยังใช้ Voice Mail Box เป็นช่องทางในการติดต่อสื่อสาร นัดหมายการส่งของ การโอนเงิน และสั่งการต่าง ๆ เนื่องจากจะมีความปลอดภัยมากกว่าที่จะใช้โทรศัพท์ติดต่อด้วยกันโดยตรง ซึ่งเมื่อกระทำการเสร็จสิ้นแล้วก็อาจจะเปลี่ยน Voice Mail Box ไปในที่อื่น ๆ อีก ทำให้ยากในการติดตามสืบสวนหาข่าว

- ลูกจ้างบริษัทแห่งหนึ่งไม่พอใจบริษัทที่จ้างอยู่ ต้องการลาออกไปอยู่อีกบริษัทหนึ่ง จึงได้ลบข้อมูลซอฟท์แวร์ที่เขาเขียนขึ้นให้กับบริษัทนี้ทิ้งไปและได้บรรจุ (Load) ข้อมูลดังกล่าวเก็บไว้ที่ตัวเอง

ในการจับกุมผู้ต้องหานั้นยากมาก เพราะหลักฐานต่าง ๆ ได้ถูกทำลายไปแล้ว แต่จุดอ่อนของพวกอาชญากรคือ ชอบโอ้อวดในสิ่งที่ตนเองได้ทำไปว่าคนอื่น ๆ ไม่สามารถกระทำได้ ในกรณีนี้จึงต้องให้เขารับสารภาพว่าได้กระทำการอย่างไรไป เพื่อนำคำรับสารภาพนั้นมาใช้เป็นหลักฐานในการลงโทษ โดยอาจจะต่อรองให้มีการลงโทษน้อยกว่า

ซึ่งแสดงให้เห็นว่า หลักฐานข้อมูลต่าง ๆ ในคดีอาชญากรรมคอมพิวเตอร์นั้น สามารถสูญหาย หรือเปลี่ยนแปลงได้อย่างรวดเร็ว แต่ก็สามารถติดตามหรือใช้เทคโนโลยีในการสืบหาพยานหลักฐานได้อยู่ ถ้าหากรู้วิธีการสืบพยานหลักฐานที่ถูกวิธี

- ในสหรัฐอเมริกา บริษัทสามารถจ้างลูกจ้างชั่วคราวมาทำงานแทนลูกจ้างได้ ในกรณีที่ลูกจ้างอาจจะลาพักผ่อน หรือลาป่วย ซึ่งสามารถลาได้นาน ในธนาคารแห่งหนึ่งได้ว่าจ้างลูกจ้างชั่วคราวมาทำงานแทนลูกจ้างประจำซึ่งขอลากิจ ลูกจ้างชั่วคราวคนนั้นมีความเชี่ยวชาญในด้านคอมพิวเตอร์อย่างมาก และได้แอบเข้าไปใช้ข้อมูลเกี่ยวกับบัตรเครดิตของธนาคารโดยที่นายจ้างไม่รู้ เมื่อครบกำหนดการจ้างงาน ผู้บริหารต้องการให้จ้างไว้เป็นลูกจ้างประจำ เนื่องจากมีประสิทธิภาพในการทำงานสูงแต่ได้รับการปฏิเสธ ทำให้เกิดความสงสัยขึ้นจึงได้ตรวจสอบประวัติบุคคลแล้วปรากฏว่า มีประวัติการก่อคดีต่าง ๆ มาแล้วถึง 5 คดี เช่น ฉ้อโกง ปลอมแปลง ดังนั้นจึงต้องการเป็นลูกจ้างชั่วคราวเพราะไม่มีการตรวจสอบประวัติก่อนทำงาน

- พนักงานฝ่ายบริการลูกค้า (Teller) ของธนาคารแห่งหนึ่งมีการโกงค่าธรรมเนียมในการโอนเงิน (Wire Fee) ของบัญชีผู้อื่นใส่บัญชีของตัวเองโดยอาศัยเวลาช่วงพักกลางวัน เหตุที่จับได้นั้นเนื่องจากการตรวจสอบรายงาน พบว่ามีการโอนเงินถึง 3 ครั้งในวันเดียวกัน จึงได้รู้ว่ามีการโกงเกิดขึ้น

- บริษัทผู้ผลิตสินค้ารายหนึ่งได้เขียนซอฟท์แวร์เพื่อใช้ในการควบคุมการทำงานของหุ่นยนต์ในโรงงาน โดยได้บรรจุอยู่ในเมนเฟรม (Main Frame) ของบริษัทซึ่งได้เชื่อมตรง (On Line) 32 ประเทศ ต่อมามีพวกอาชญากรสามารถเจาะเข้าไปในเมนเฟรม ได้ทำให้การทำงานนั้นผิดปกติไป จากการสืบทราบพบว่าเป็น Netherland Hacker วิธีการแก้ไขที่บริษัทจะทำให้คือ

1. ปิดการติดต่อสื่อสารทั้งหมด

2. ปิดระบบของโรงงานผลิต ซึ่งจะทำให้เสียหายมีมูลค่าถึง 200,000 ดอลล่าร์สหรัฐ

การสืบหาข้อมูลนี้จะทำได้ลำบากเนื่องจากจะต้องเดินทางไปเก็บข้อมูลเองทุกจุด เพราะใช้การติดต่อสื่อสาร (Telecomunication) ไม่ได้เนื่องจากจะทำให้พวกอาชญากรรู้ตัวว่ากำลังจะถูกตามอยู่

- ที่เมืองโคลัมบัส รัฐโอไฮโอ มีบริษัทร้องเรียนว่ามีการใช้โทรศัพท์ของบริษัทโทรไปที่สาธารณรัฐประชาชนจีน เป็นมูลค่าถึง 100,000 ดอลล่าร์สหรัฐ หลังจากการสืบสวนนับว่าเป็นการใช้โทรศัพท์มือถือผ่านศูนย์ใน New York ในที่สุดก็สามารถจับกุมตัวได้ที่ Maryland

การฉ้อโกงโทรศัพท์นี้มักจะใช้โทรศัพท์มือถือมากกว่าโทรศัพท์ใช้สาย เนื่องจากการติดตามนั้น โทรศัพท์ใช้สายง่ายกว่าโทรศัพท์มือถือ หากโทรศัพท์มือถือนั้นสงสัยว่าจะถูกติดตามก็สามารถปิดเครื่องแล้วไปใช้หมายเลขอื่นต่อไป

- ปัญหาการเข้าไปใช้โทรศัพท์ของผู้อื่นโทรไปกระทำความผิด เช่น การโทรเข้าสายฉุกเฉิน 911 (ของสหรัฐอเมริกา ส่วนประเทศไทยใช้ 191) เพื่อแกล้งแจ้งเหตุด่วนเหตุร้าย หรือโทรเข้าไปพูดวิตถารกับผู้รับผู้อื่น หรือให้ต่อผ่านไปยังที่อื่นโดยไม่เสียค่าโทรศัพท์ และอีกตัวอย่างหนึ่งคือ นาย A ได้เข้าไปใช้ข้อมูลระบบโทรศัพท์ของ Dr.Smith สั่งโอนเงินเข้าบัญชีโดยอ้างว่าให้ส่งเงินให้ลูกชาย 2,000 ดอลล่าร์สหรัฐ เมื่อธนาคารได้รับคำสั่งจึงได้ตรวจสอบ (Double Check) กลับมา และสายก็กลับมายังนาย A ว่ายืนยันคำสั่งดังกล่าว ธนาคารจึงสั่งจ่ายเงินให้กับนาย A ไป หรือบริษัทโทรศัพท์ท้องถิ่นของมลรัฐโอไฮโอ จะถูกพวกอาชญากรเข้าไปทำให้ระบบเสียหายบ่อย ๆ เช่น การโทรศัพท์ฟรีหรืออื่น ๆ แต่มักจะไม่ได้ความร่วมมือจากบริษัทโทรศัพท์ท้องถิ่นรายอื่น ๆ เนื่องจากผลของการกระทำนั้น ไม่ได้เกิดขึ้นกับบริษัทของเขาทำให้ยากในการรวบรวมข้อมูลเมื่อติดตามสืบสวน

- มีการใช้ระบบการสื่อสารในการลอบวางระเบิด และใช้ระบบการสื่อสารสั่งการจุดระเบิด หรือมีการลอกเลียนพฤติกรรมต่าง ๆ โดยการเปิดคอมพิวเตอร์ดู วิธีการในการวางระเบิดแล้วกระทำตาม จึงถือว่าเป็นอันตรายอย่างยิ่ง

- เป็นลักษณะการกระทำผิดโดยใช้คอมพิวเตอร์เข้าไปแทรกในสัญญาณความถี่ของทางราชการและนำไปใช้ในทางทุจริต

2.5.3 ตัวอย่างอาชญากรรมคอมพิวเตอร์จากการสัมมนาทางวิชาการของ ดร.ศรีศักดิ์ จามรมาน และ ดร.กนกวรรณ ว่องวัฒนสิน

จากเอกสารประกอบการสัมมนาทางวิชาการ เรื่อง "เทคโนโลยีการป้องกันอาชญากรรมทางธุรกิจสมัยใหม่" ศาสตราจารย์ ดร.ศรีศักดิ์ จามรมาน และ ดร.กนกวรรณ

ว่องวัฒนสิน ได้ยกคดีอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นกรณีศึกษาตัวอย่างและเป็นคดีที่น่าสนใจดังนี้

(1) นักเรียนระดับเตรียมอุดมใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิดได้เงินยี่สิบล้านบาท

คดีนี้เกิดขึ้นเมื่อปี พ.ศ.2511 ที่แคลิฟอร์เนีย อาชญากรในขณะนั้นเป็นนักเรียนในระดับเตรียมอุดมที่แฮมมิงตัน ไฮสคูล (Hamilton High School) ชื่อเจอร์รี่ นีล (Jerry Neal) เป็นคนหัวดี ขยันขันแข็ง มีพรสวรรค์ในด้านอิเล็กทรอนิกส์ อายุเพียง 19 ปี ก็ตั้งบริษัทเล็ก ๆ ขึ้นมาขายสิ่งประดิษฐ์ ด้านอิเล็กทรอนิกส์เล็ก ๆ น้อย ๆ

ทุก ๆ วันเจอรรี่เดินไปโรงเรียนผ่านโกดังเก็บของ ของบริษัท Pacific Telephone and Telegraph Company ที่กองขยะของโกดังนั้นเจอร์รี่พบขยะต่าง ๆ น่าสนใจมากมาย เช่น เครื่องมือชำรุดที่บริษัททิ้ง แต่เจอร์รี่เอาไปแกะชิ้นส่วนทำอย่างอื่นขายได้ นอกจากเครื่องมือต่าง ๆ แล้ว เจอร์รี่ก็เก็บเอกสารต่าง ๆ ของบริษัทมาด้วย เช่น แผนการปฏิบัติงานของบริษัท, โปรแกรมคอมพิวเตอร์ที่ใช้กับระบบ, โครงสร้างของการจัดการบริษัท, บันทึกติดต่อภายในบริษัทแม้กระทั่งงบประมาณของบริษัท ซึ่งคอมพิวเตอร์ได้พิมพ์ออกมา เมื่อเจอร์รี่เข้ามหาวิทยาลัยมีประสบการณ์ด้านขโมยเวลาโทรศัพท์ทางไกลเพิ่มเติมจากเพื่อน ๆ เจอร์รี่ก็เริ่มกระทำผิดโดยไปประมูลรถยู้ใช้แล้วของบริษัท ซึ่งยังมีตราติดอยู่ ซื้อกุญแจจากพนักงานบริษัทที่ลาออก ต่อมาในเดือนมิถุนายน 2514 เจอร์รี่ก็ทดลองขโมยครั้งแรกโดยใช้เครื่องปลายทางของตนเองติดต่อกับคอมพิวเตอร์ของบริษัท สั่งเครื่องโทรศัพท์และอุปกรณ์ราคาหกแสนบาทให้ไปส่งที่โกดังย่อย พอเช้ามืดเจอร์รี่ก็ไปเอาสินค้าที่สั่งมาเซ็นรับของและส่งใบเซ็นรับของกลับไปทางไปรษณีย์ กิจการของเจอร์รี่ขยายเพิ่มมากขึ้น จึงตัดสินใจเล่าให้เพื่อนฟังและว่าจ้างให้เพื่อนมาเป็นคนขับรถ ต่อมาเพื่อนขอเพิ่มค่าจ้าง เจอร์รี่ไม่ยอม เพื่อนจึงไปแจ้งให้บริษัททราบ บริษัทส่งนักสืบสะกดรอยตามจนจับได้ แต่เจอร์รี่ปฏิบัติการอย่างดีมากจนบริษัทเองหาข้อมูลไม่ได้ว่าเจอร์รี่ขโมยอะไรไปบ้าง ในที่สุดโดยการต่อรองกันเจอร์รี่ยอมรับว่าของราคาเพียงหนึ่งแสนบาท และถูกตัดสินจำคุก 40 วัน พอออกจากคุก เจอร์รี่ตั้งบริษัทใหม่ รับปรึกษาและจัดวางระบบป้องกันอาชญากรรมคอมพิวเตอร์

(2) การฉ้อโกงสี่หมื่นล้านบาทที่บริษัทประกันภัย

คดีเกิดขึ้นที่ประเทศสหรัฐอเมริกา เจ้าหน้าที่จับกุมได้เมื่อ พ.ศ.2516 หลังจากที่ได้ดำเนินการโกงมาถึง 10 ปี บริษัทที่เกิดเรื่องชื่อ The Equity Funding

Corporation of America (EFCA) ที่ Los Angeles, California บริษัทนี้เริ่มมาจากบริษัทหลักทรัพย์และประกันภัยเล็ก ๆ สองบริษัท มีผู้บริหารเป็นคนหนุ่มอายุเฉลี่ยเพียง 33 ปี มีความตั้งใจที่จะทำให้บริษัทของตนเป็นบริษัทการเงินที่ใหญ่ที่สุด ขยายกิจการเร็วที่สุด มีชื่อเสียงมากที่สุด แต่วิธีที่ทำให้บรรลุวัตถุประสงค์นั้นไม่ถูกต้อง คือกลายเป็นวิธีฉ้อโกงโดยใช้คอมพิวเตอร์ช่วยวิธีการโกงก็คือ ใช้คอมพิวเตอร์สร้างกรมธรรม์ปลอมขึ้นมา

ผลประโยชน์จากการตั้งกรมธรรม์ปลอมขึ้นนี้มีหลายประการ เช่นทำให้รายได้ปลอมของบริษัทสูงขึ้น กำไรปลอมสูงขึ้น จำนวนลูกค้าปลอมสูงขึ้น ทำให้ราคาหุ้นของบริษัทในตลาดหลักทรัพย์สูงขึ้น ผู้จัดการสามารถตั้งเงินเดือนและรายได้ต่าง ๆ สูงขึ้น มีการจ่ายค่านายหน้าสูงขึ้น มีการเบิกค่ารับรองและค่าเดินทางสูงขึ้น เป็นต้น นอกจากนั้นบริษัทยังได้เอาหุ้นของบริษัทไปใช้ในการซื้อกิจการต่าง ๆ ทั้งในประเทศ ต่างประเทศมากมายรวมแล้วในที่สุดมีบริษัทในเครือเกือบร้อยบริษัท เอากรมธรรม์ทั้งจริงและปลอมไปใช้เป็นหลักประกันในการกู้เงินหรือขายต่อให้กับบริษัทประกันภัยอื่น เป็นต้น

เจ้าหน้าที่ตรวจสอบจากภายนอกก็ตรวจสอบไม่พบอะไรน่าสงสัย ในปี 2515 บริษัทตรวจสอบบัญชี Seidman and Seidman มาตรวจสอบทาง EFCA พิมพ์รายละเอียดกรรมธรรม์ให้โดยระบุหมายเลขและจำนวนเงินและอื่น ๆ ยกเว้นชื่อและที่อยู่ผู้เอาประกันภัย โดยระบุให้แต่ละคนจะมีเลขประจำตัว 5 ตำแหน่ง ซึ่งเจ้าหน้าที่ของ EFCA จะเขียนโปรแกรมสั่งให้คอมพิวเตอร์คิดเลขจริง 2 ตัวแรกออก แล้วใส่เลขปลอมลงไป ฉะนั้นถ้ามีกรมธรรม์อยู่ 20,000 ฉบับ ก็สามารถให้คอมพิวเตอร์สร้างเลขปลอมขึ้นเป็นแสนฉบับได้ ผู้ตรวจสอบใช้วิธีสุ่มตัวอย่างเลือกหมายเลข 2,000 ฉบับแล้วขอให้คอมพิวเตอร์พิมพ์ชื่อและที่อยู่ให้ เพื่อส่งให้ผู้เอาประกันภัยยืนยัน EFCA ก็สั่งคอมพิวเตอร์ให้ไปเลือกชื่อและที่อยู่ที่มีตัวจริงหรือใส่ชื่อที่อยู่ของผู้ทุจริตและญาติพี่น้องเข้าไป แล้วขอให้เขาช่วยยืนยันให้

การใช้คอมพิวเตอร์ช่วยในการฉ้อโกงอีกแง่หนึ่ง ก็คือเป็นข้ออ้างในการทำลายต้นฉบับเอกสาร นั่นคือเมื่อเอาข้อมูลเข้าไปในการ์ดในแถบแม่เหล็กแล้ว ก็ทำลายหลักฐานต้นฉบับทั้งหมด โดยอ้างว่ามีอยู่ในคอมพิวเตอร์แล้วไม่ต้องเก็บต้นฉบับให้เปลืองที่ เมื่อถึงเวลาตรวจสอบ ผู้ตรวจสอบก็ต้องขอความร่วมมือจากพนักงานคอมพิวเตอร์ ซึ่งจะเขียนโปรแกรมสั่งเครื่องอย่างไรก็ได้ เพราะผู้ตรวจสอบสมัยนั้นไม่มีความรู้เรื่องคอมพิวเตอร์ การฉ้อโกงนี้ถูกจับได้

โดยมีพนักงานของบริษัทระดับผู้ช่วยประธานบริหารถูกให้ออกจากงาน จึงไปแจ้งความให้เจ้าหน้าที่มาตรวจสอบ จนในที่สุดได้หลักฐานเพียงพอที่จะดำเนินคดีได้

2.5.4 คดีอาชญากรรมคอมพิวเตอร์ในประเทศไทย

เนื่องจากประเทศไทยมิได้เป็นประเทศผู้นำในการผลิต การจำหน่ายและการใช้เทคโนโลยีคอมพิวเตอร์ เป็นแต่เพียงประเทศผู้ตามในการใช้เทคโนโลยีด้านนี้เท่านั้น ดังนั้น ผู้มีความรู้เชี่ยวชาญในด้านเทคโนโลยีคอมพิวเตอร์จึงมีน้อย เช่นเดียวกับการเกิดอาชญากรรมคอมพิวเตอร์ยังมีไม่มากนัก จากเอกสารงานวิจัยที่ นายนันทชัย เพียรสนอง นำเสนอต่อวิทยาลัยการยุติธรรมกระทรวงยุติธรรมในหลักสูตร "ผู้บริหารกระบวนการยุติธรรมระดับสูง (บ.ย.ส.)" พ.ศ.2539 ได้รวบรวมข่าวคราวการเกิดอาชญากรรมคอมพิวเตอร์ในประเทศไทยไว้ดังนี้

(1) การทุจริตด้านบัตรบริการฝากถอนเงินอัตโนมัติ (ATM)

การให้บริการฝากถอนเงินอัตโนมัติ (Automatic Teller Machine หรือ ATM) ของธนาคารพาณิชย์ต่าง ๆ ซึ่งก่อให้เกิดความสะดวกสบายแก่ลูกค้าของธนาคารเป็นอย่างมาก เพราะผู้ต้องการถอนเงินเพียงแต่ไปกดเอาจากเครื่อง ATM เท่านั้นโดยไม่ต้องไปติดต่อเสมียนธนาคารที่หน้าเคาเตอร์ของธนาคารที่ตนมีบัญชีเงินฝากอยู่ การให้บริการชนิดนี้ได้ปรากฏเป็นข่าวทางหน้าหนังสือพิมพ์เมื่อประมาณ 8 ถึง 10 ปีที่ผ่านมาว่า ผู้ใช้บัตร ATM บางคนไม่ได้ไปกดเอาเงินจากเครื่อง ATM เลย แต่บัญชีถูกหักเงินไปหรือบางคนกด ATM แล้วไม่มีเงินออกมา แต่บัญชีมีรายการถอนเงินออกไปแล้ว สาเหตุมักเกิดจากมีคนร้ายใช้วิธีการต่าง ๆ ในการลักลอบเอาเงินของเจ้าของบัตรไป เช่น ในกรณีแรก ผู้ใช้บัตรไม่ได้ไปกดเอาเงินจากเครื่อง ATM เลย แต่บัญชีถูกหักไปแล้วนั้น มักจะเกิดจากคนใกล้ชิดขโมยเอาบัตร ATM ไปเบิกเอาเงินออกมา หรือในกรณีหลัง ผู้ใช้บัตร ATM กด ATM แล้วไม่มีเงินไหลออกมานั้น ก็อาจเป็นกรณีที่คนร้ายใช้หมากฝรั่งหรือของแข็ง เช่น ไม้จิ้มฟันไปอุดไว้ที่ช่องใส่เงิน เมื่อผู้ใช้บัตรกดเครื่อง ATM แล้วเงินก็จะค้างอยู่ในเครื่องไม่ไหลออกมา เพราะติดหมากฝรั่งหรือของแข็งที่ปิดไว้ และบัตร ATM ก็จะไม่คืนออกมาด้วย เนื่องจากเครื่องทำงานไม่ครบวงจร จากนั้นคนร้ายจะเข้าไปพูดกับผู้ใช้บัตรว่าเครื่องเสียให้ลองกดซ้ำอีก เมื่อเหยื่อหลงเชื่อทำตามเงินก็ยังไม่ไหลออกมา แต่รหัสบัตรจะถูกแอบดูและจำเอาไว้ โดยเจ้าของบัตรไม่ทราบ จึงเดินออกไปจากตู้ ATM เพื่อไปแจ้งแก่ธนาคาร

จากนั้นคนร้ายก็จะมาแกะเอาหมากฝรั่งหรือของแข็งออก แล้วจะได้ทั้งบัตรและเงินที่ค้างอยู่ รวมทั้งนำบัตรไปเบิกเงินได้อีก (มติชน, 19 ต.ค. 2539 : 1)

(2) การทุจริตด้านบัตรเครดิต

ในปัจจุบันบัตรเครดิตเป็นที่นิยมใช้กันอย่างกว้างขวาง และเพิ่มจำนวนขึ้นอย่างรวดเร็วทุกปี และมีข่าวทุจริตเกี่ยวกับการใช้บัตรชนิดนี้เกิดขึ้นบ่อย ๆ เช่น เมื่อประมาณกลางปี พ.ศ.2539 มีข่าวว่ารองผู้ว่าการธนาคารแห่งประเทศไทย ถูกคนร้ายปลอมแปลงบัตรเครดิตไปใช้ที่ประเทศมาเลเซีย เป็นมูลค่ากว่า 400,500 บาท และยิ่งการใช้บัตรเครดิตมีการขยายตัวมากขึ้น ปัญหาเกี่ยวกับการทุจริตบัตรเครดิตก็ยิ่งเพิ่มมากขึ้นเป็นเงาตามตัว จากรายงานการวิจัยของบริษัท ศูนย์วิจัยกสิกรไทย จำกัด ปีที่ 2 ฉบับที่ 273 วันที่ 23 สิงหาคม 2539 เรื่อง "ทุจริตบัตรเครดิต : ปัญหาที่ต้องเร่งแก้ไข" ได้รายงานว่า การทุจริตบัตรเครดิตเกิดจากกรณีดังต่อไปนี้

- เกิดจากผู้ถือบัตรเองมีเจตนากระทำการทุจริต โดยการปลอมแปลงเอกสาร หลักฐานในการสมัครและเมื่อได้รับการอนุมัติให้เป็นผู้ถือบัตรแล้ว ก็นำไปใช้จ่ายจนเกิดความเสียหายต่อธนาคารผู้ออกบัตร หรืออาจจะมีกรณีแจ้งหายแล้วนำไปใช้ต่อเอง

- เกิดจากการกระทำของคนร้าย โดยเจ้าของบัตรไม่ทราบ จนกระทั่งมีใบเรียกเก็บหนี้แจ้งมาว่ามีการใช้จ่ายด้วยบัตรเครดิตเกิดขึ้น ซึ่งกรณีนี้สามารถเกิดขึ้นได้โดย เกิดจากบัตรหาย เพราะลืมทิ้งไว้ในร้านค้า ลืมกระเป๋าทิ้งไว้ในห้องน้ำ ทำบัตรหล่นหายโดยไม่รู้ตัว หรือเกิดจากบัตรถูกขโมยโดยบุคคลใกล้ชิดนำไปใช้ ถูกล้วงหรือถูกกรีดกระเป๋า ถูกขโมยจากห้องพักหรือตู้เก็บของ (Locker), หรือเกิดจากบัตรที่ส่งไปจากธนาคารไม่ถึงผู้รับโดยเจ้าหน้าที่ธนาคารทุจริต เจ้าหน้าที่เอกสารทุจริตหรือเจ้าหน้าที่ไปรษณีย์ทุจริต เป็นต้น

จากรายงานสถิติของกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ (ศสก.) พบว่าในปี พ.ศ.2538 มีคดีทุจริตเกี่ยวกับบัตรเครดิตเกิดขึ้น 76 คดี จับผู้ต้องหาได้ 68 คน และมีมูลค่าความเสียหายทั้งสิ้น 49.46 ล้านบาท

รูปแบบการทุจริต

- โดยการขโมยบัตรของเจ้าของบัตรไปใช้โดยตรง

- โดยการปลอมของร้านค้าที่รับบัตรโดยเจตนาทุจริต ลอกเลียนจากรหัส

ตัวเลขตามใบรายการที่ลูกค้าใช้บริการ ไปทำตัวนูนลงบนบัตรพลาสติกเปล่า จากนั้นร้านค้าจะรูดบัตรและปลอมลายเซ็นของเจ้าของบัตร แล้วนำใบรายการไปขึ้นเงินจากธนาคาร

- เป็นการปลอมแปลงบัตรของกลุ่มมิจฉาชีพ หรือร้านค้า โดยการนำบัตรที่หมดอายุแล้วไปผ่านความร้อนเพื่อรีดรหัสตัวเลขบนบัตรออกแล้วพิมพ์รหัสตัวเลขนูนขึ้นใหม่ให้เหมือนกับบัตรของเจ้าของบัตรรายอื่นที่ยังไม่หมดอายุ แล้วนำไปใช้รับบริการกับร้านค้า

- การปลอมแปลงลายเซ็นโดยพนักงานรับจ่ายเงินของร้านค้าและห้างที่รับบัตรเครดิตจ่ายแทนเงินสด ทำการรูดสลิปบัตรไว้หลาย ๆ ใบ

- การใช้บัตรเครดิตผ่านเครือข่ายอินเตอร์เนต ทำให้คนร้ายที่สามารถเข้าถึงระบบ สามารถทราบรหัสในบัตร ชื่อเจ้าของบัตรแล้วนำข้อมูลไปใช้ทำบัตรปลอมขึ้นใหม่ได้

(3) การทำลายเครื่องฝากถอนเงินอัตโนมัติ (ATM)

นับได้ว่าเป็นการกระทำอาชญากรรมที่เกี่ยวกับเครื่องคอมพิวเตอร์โดยตรง เพราะเครื่อง ATM ก็เป็นเครื่องคอมพิวเตอร์อย่างหนึ่ง เช่น เมื่อวันที่ 28 ธันวาคม 2539 มีคนร้ายขับรถจักรยานยนต์หย่อนระเบิดใส่ตู้ ATM ของธนาคารกรุงศรีอยุธยา ซึ่งตั้งอยู่ที่หน้าโรงงานบริษัท ชัมมิต พุตแวร์ แอนด์ ชีท จำกัด ตำบลบางโฉลง อำเภอบางพลี จังหวัดสมุทรปราการ แรงระเบิดทำให้ตู้ ATM พังยับเยิน แต่คนร้ายไม่สามารถเอาเงินไปได้ เพราะยามรักษาการณ์ของบริษัทเข้าไปขัดขวางไว้ได้ทัน (ไทยรัฐ, 29 ธ.ค.2539 : 1) และเมื่อวันที่ 26 มีนาคม 2541 เวลาประมาณ 02.00 น. มีคนร้ายลอบเข้าไปในธนาคารกสิกรไทย สาขาบางเมฆขาว ถนนสุขุมวิท ตำบลท้ายบ้าน อำเภอเมือง จังหวัดสมุทรปราการ ใช้แก๊สตัดแผ่นเหล็กทางด้านหลังตู้ ATM ได้เงินไปประมาณ 700,000 บาท และขณะหลบหนีทำเงินสดตกกระจายเกลื่อนตามรายทาง ที่หลบหนีเก็บได้ทั้งหมด 145,800 บาท (ไทยรัฐ, 27 มี.ค. 2541 : 1)

(4) การขโมยแผงวงจรรวมหรือไอซี (Integrated Circuit)

กรณีที่เป็นข่าวใหญ่ลงในหน้าหนังสือพิมพ์ ได้เกิดขึ้นแล้ว 3 ครั้ง ครั้งแรกเมื่อวันที่ 13 กุมภาพันธ์ 2538 ได้มีคนร้ายร่วมกันปล้น บริษัท รอกิไทย จำกัด ถนนโรจนะ ตำบลคานหาม อำเภออุทัย จังหวัดพระนครศรีอยุธยา ได้แผงวงจรรวมหรือไอซีไปเป็นจำนวนมาก คิดเป็นมูลค่าประมาณ 50 ล้านบาท ครั้งที่ 2 เมื่อวันที่ 10 ธันวาคม 2539 รถบรรทุก 6 ล้อคันหนึ่งรับจ้างขนส่งแผงวงจรรวมหรือไอซี จำนวน 40 กล่อง มูลค่าประมาณ 10 ล้านบาท จากบริษัท

เอเอ็มดี (ไทยแลนด์) จำกัด ถนนแจ้งวัฒนะไปยังคาร์โก สนามบินดอนเมือง เมื่อรถแล่นมาถึงหน้าสนามบินดอนเมือง มีคนร้ายประมาณ 10 คน ใช้ปืนเป็นอาวุธปล้นทั้งรถบรรทุกและแผงวงจรรวมหรือไอซีไปได้ แต่ต่อมาเจ้าหน้าที่ตำรวจสามารถสืบสวนติดตามจับกุมคนร้ายได้ทั้งหมดและยึดของกลางคืนมาได้ ผลการสืบสวนสอบสวนได้ความว่า แผงวงจรรวมหรือไอซีจะถูกส่งต่อไปยังประเทศสิงค์โปร์ เพื่อนำไปประกอบเป็นเครื่องคอมพิวเตอร์ต่อไป (ธรรมรัฐ, 26 ธ.ค. 2539 : 11) การชโมยเครื่องคอมพิวเตอร์ โดยเมื่อวันที่ 24 มีนาคม 2541 มีคนร้าย 2 คนลอบเข้าไปในบริษัท อายิโนะโมะโต๊ะ จำกัด สาขาธนบุรี แล้วลักเอาคอมพิวเตอร์ขนาด Note Book จำนวน 8 เครื่องไป แต่ต่อมาถูกจับได้พร้อมของกลาง (ไทยรัฐ, 7 เม.ย. 2541 : 19)

(5) การ**จูนโทรศัพท์มือถือ**

ในรอบปี พ.ศ.2539 ที่ผ่านมามีข่าวใหญ่เกี่ยวกับผู้ใช้โทรศัพท์มือถือถูกลักลอบเอาเบอร์โทรศัพท์ไปใช้หลายราย ทั้งโทรศัพท์ภายในประเทศและโทรศัพท์ทางไกลไปต่างประเทศ บางรายมียอดใช้ภายในเวลา 5 วัน รวม 292 ชั่วโมง เป็นเงินค่าโทรศัพท์ 700,000 บาทเศษ

การจูนโทรศัพท์มือถือสามารถกระทำได้ 3 ลักษณะคือ

- ร้านค้าให้บริการแก่ลูกค้าที่มารับบริการจูนเลขหมายของตนเอง กรณีต้องการเปลี่ยนเครื่องใหม่เนื่องจากเครื่องเก่าชำรุดหรือล้าสมัยโดยใช้เครื่องลูกข่ายนอกระบบ

- การแอบจูนจากลูกค้าที่นำเครื่องลูกข่ายไปซ่อมหรือตรวจเช็คกับร้านค้าย่อย

- การแอบจูนโดยอาศัยเครื่องดักสัญญาณเพื่อดักคลื่นโทรศัพท์ของผู้ใช้ที่เปิดใช้อยู่และนำไปจูนเครื่องใหม่ให้แก่ลูกค้ารายอื่น ๆ ต่อไป ระบบโทรศัพท์ที่ถูกจูนมากที่สุดคือระบบแอนะล็อก (Analog) เพราะเป็นระบบที่ไม่ยุ่งยาก และเครื่องโทรศัพท์ชนิดนี้มีการลักลอบนำเข้ามาจากต่างประเทศมาก (เดลินิวส์, 2 ม.ค. 2540 : 8) การกระทำลักษณะนี้ศาลฎีกาได้มีคำวินิจฉัย เป็นบรรทัดฐานว่าเป็นการรับส่งวิทยุคมนาคม โดยอาศัยคลื่นสัญญาณโทรศัพท์ของผู้อื่นโดยไม่ได้รับอนุญาต หรืออีกนัยหนึ่งเป็นการแย่งใช้คลื่นสัญญาณโทรศัพท์ของผู้อื่นโดยไม่มีสิทธิ เป็นความผิดตามพระราชบัญญัติวิทยุคมนาคม พ.ศ.2498 มาตรา 6 ประกอบมาตรา 23 แต่ไม่มีความผิดฐานลักทรัพย์ (ฎีกาที่ 5354/2539)

(6) การพ่วงสายโทรศัพท์ตามบ้าน

ได้มีข่าวปรากฏอยู่เสมอ ๆ ว่าโทรศัพท์ตามบ้าน ซึ่งให้บริการโดยองค์การ-โทรศัพท์แห่งประเทศไทย เจ้าของเลขหมายจะได้รับใบแจ้งหนี้ค่าโทรศัพท์ที่สูงกว่าความจริงมาก ซึ่งองค์การโทรศัพท์แห่งประเทศไทยมีหน่วยงานที่รับผิดชอบในการตรวจสอบว่ามีการผิดพลาดในการคิดค่าบริการหรือไม่ หรือตรวจสอบได้ว่ามีผู้แอบพ่วงใช้สายโทรศัพท์หรือไม่ ในกรณีที่มีการคิดค่าบริการเกินกว่าความเป็นจริงโดยเจตนา หรือมีการแอบพ่วงใช้สายโทรศัพท์ก็นับว่าเป็นอาชญา-กรรมอย่างหนึ่ง

(7) การละเมิดลิขสิทธิ์โปรแกรม

โดยมีการคัดลอก (Copy) โปรแกรมต้นฉบับออกจำหน่าย หรือแจกจ่ายให้ผู้อื่นนำไปใช้โดยผิดพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 เช่น คดีแดงที่ 432/41 ระหว่างพนักงานอัยการ โจทก์ นายอรัญ ชมภูพันธ์ จำเลย ศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลางพิพากษาว่าจำเลยละเมิดลิขสิทธิ์ของบริษัท ไมโครซอฟท์ คอร์ปอเรชั่น จำกัด และบริษัท อโกเบ ซิสเต็มส์ อินคอร์ปอเรเรส์ จำกัด โดยการนำแผ่นซีดีที่บันทึกโปรแกรมคอมพิวเตอร์ของทั้งสองบริษัทมาทำซ้ำออกขายต่อสาธารณชน โดยไม่ได้รับอนุญาตจากทั้งสองบริษัท ผิดตามพระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 มาตรา 31, 70 วรรคสอง ให้จำคุก 1 ปี และปรับ 200,000 บาท โทษจำคุกรอการลงโทษ 2 ปี ให้ของกลางตกเป็นของเจ้าของลิขสิทธิ์ และจ่ายเงินค่าปรับกึ่งหนึ่งแก่ผู้เสียหายซึ่งเป็นเจ้าของลิขสิทธิ์ (มติชน, 4 เม.ย. 2541 : 8)

(8) การขโมยข้อมูลและการแก้ไขข้อมูล

เป็นการเข้าถึงฐานข้อมูลแล้วคัดลอก (Copy) เอาข้อมูลไปหรือเข้าถึงข้อมูลแล้วเปลี่ยนแปลงแก้ไขข้อมูลในหน่วยความจำ เช่น

(1) เมื่อวันที่ 5 พฤษภาคม 2541 ผู้จัดการบริษัท เช้าท์ อีสวู๊ดส์ จำกัด จังหวัดระยอง แจ้งตำรวจว่าข้อมูลลับในเครื่องคอมพิวเตอร์ถูกขโมยไป ต่อมาตำรวจจับพนักงานรักษาความปลอดภัยของบริษัทคนหนึ่ง ได้รับสารภาพว่าเป็นผู้คัดลอก (Copy) ข้อมูล ชื่อลูกค้าชาวต่างประเทศ บัญชีรายรับรายจ่ายของบริษัทไป คนร้ายรายนี้จบ ปวช. สาขาอิเล็กทรอนิกส์ เคยถูกจับข้อหาขับรถประมาท ถูกส่งตัวมายังสถานพินิจฝึกการใช้เครื่องคอมพิวเตอร์จนชำนาญในระหว่างถูกควบคุม (มติชน, 6 พ.ค.2541 : 1)

(2) เมื่อวันที่ 9 กุมภาพันธ์ 2542 นายวัฒนา คงคาประเสริฐ ผู้จัดการธนาคารนครหลวงไทย สาขาพระราม 4 นำตัวพนักงานคนหนึ่งในสาขา เข้าแจ้งความต่อตำรวจในข้อหาลักเงินของธนาคาร พฤติการณ์คือ เมื่อลูกค้านำเงินมาฝาก เมื่อรับเงินและพิมพ์รายการฝากเงินลงในสมุดคู่ฝากแล้วคืนสมุดให้ลูกค้าไป จากนั้นก็ลบรายการออกจากคอมพิวเตอร์ของธนาคารแล้วเอาเงินไป ต่อมาเมื่อลูกค้ามาถอนเงินก็รีบเข้าประกบแล้วลงรายการในสมุดคู่ฝากของลูกค้า จากนั้นลบข้อมูลออกจากคอมพิวเตอร์ แต่นำเงินของตนเองจ่ายให้ไปแทนได้เงินไปกว่า 2,000,000 บาท เพราะทำหลายราย ถูกจับได้เนื่องจากพนักงานคนนี้ลาป่วย พนักงานคนอื่นทำงานแทน จึงพบเหตุความผิด เหตุเกิด สน.ทองหล่อ (ไทยรัฐ, 11 ก.พ. 2542 : 19)

(9) อาชญากรรมบนเครือข่ายอินเตอร์เน็ต

นับแต่เครือข่ายอินเตอร์เน็ตได้เปิดบริการในเชิงพาณิชย์ขึ้นในประเทศไทย นับตั้งแต่ประมาณปี พ.ศ.2537 เป็นต้นมา การใช้อินเตอร์เน็ตในด้านไม่ดีหรือในด้านลบในประเทศไทยก็สามารถกระทำได้เช่นเดียวกันกับในประเทศสหรัฐอเมริกา ซึ่งเป็นต้นกำเนิด บรรดาเวบไซต์ (Web Sites) ต่าง ๆ ก็สามารถถูกเปิดดูได้จากเครื่องคอมพิวเตอร์ในประเทศไทยที่เชื่อมต่อกับเครือข่ายอินเตอร์เน็ต และอาชญากรรมที่เกิดขึ้นเกี่ยวกับประเทศไทยหรือในประเทศไทยก็เริ่มมีข่าวเกิดขึ้นแล้ว เช่น

- การตัดต่อภาพ เอาภาพใบหน้าดาราสาวของไทย ไปติดต่อกับภาพเปลือยของหญิงสาวคนอื่น ให้ดูเสมือนว่า ดาราคนไทยถ่ายภาพเปลือย แล้วแพร่ภาพไปในเวบไซต์ (Web Site) เช่น ดาราสาวชื่อ นิโคล เทริโอ ถูกตัดต่อภาพเปลือยแล้วแพร่ภาพทางเครือข่ายอินเตอร์เน็ต (เดลินิวส์, 1 พ.ค. 2541 : 1)

- การเล่นการพนัน ไม่ว่าจะเป็นแบล็กแจ็ก โป๊กเกอร์ รูเล็ต สล็อตแมชีน หวยล็อตโต รโดยผู้เล่นสามารถลงทะเบียนเชื่อมตรง (On-Line) ผ่านทางไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ไปยังเจ้าของบ่อน ทางบ่อนจะตอบรับกลับมาแจ้งรหัสผ่านให้เข้าไปเลือกเล่นการพนันชนิดต่าง ๆ ได้ตามต้องการ แต่ผู้เล่นจะต้องมีบัตรเครดิตชนิดสากล เช่น บัตรวีซ่า (Visa), บัตรมาสเตอร์ (Master Card) และจะต้องแจ้งรหัสบัตรเครดิตนั้น ๆ เวบไซต์ชนิดนี้เพิ่งจะเริ่มต้นมีการให้บริการ และกำลังขยายตัวมากขึ้นโดยสามารถให้บริการได้ตลอด 24 ชั่วโมง (ไทยรัฐ, 31 ม.ค. 2540 : 1)

- เมื่อระหว่างเดือนธันวาคม 2540 ถึงเดือนมกราคม 2541 มีบริษัทเถื่อนส่ง E-Mail จากประเทศไทยผ่านเครือข่าย Internet ไปยังผู้รับในหลายประเทศทั่วโลก เสนอจัดส่งเด็กหญิงอายุระหว่าง 15-17 ปี ไปให้บริการทางเพศได้ทั่วโลก โดยจ่ายเงินเพียง 3,000-8,000 เหรียญสหรัฐ เป็นการค้าประเวณีทางเครือข่ายอินเตอร์เนต (ไทยรัฐ, 10 เม.ย. 2541 : 1)

- การส่งไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) กล่าวหาบุคคลอื่นให้เสียหาย โดยเมื่อวันที่ 11 มี.ค.2541) มีผู้แอบส่งข้อความทาง E-Mail จากประเทศไทยผ่านเครือข่ายอินเตอร์เนตไปยังผู้รับทั่วโลกว่า นักการเมืองในประเทศไทยกำลังใช้อิทธิพลทางการเมืองบีบบังคับผู้บริหารในธนาคารแห่งประเทศไทย ให้ลาออกและให้มีการเปลี่ยนแปลงโครงสร้างการบริหารงานภายในองค์กรเสียใหม่ (มติชน, 12 มี.ค. 2541 : 1)

- การทำลายภาพพจน์ของประเทศ และการคว่ำบาตรทางอินเตอร์เนต (Internet Boycott) รวมทั้งลัทธิเหยียดผิว (Racism)

ได้มีการสร้างโฮมเพจ Don't! Buy! Thai! และมีการประกาศขายเสื้อดังกล่าวในราคา 10 เหรียญสหรัฐและคิดค่าส่ง 3 เหรียญ ซึ่งพวกอาชญากรได้อ้างว่าไม่ได้กำไรจากการขายเสื้อดังกล่าว แต่ต้องการคว่ำบาตรประเทศไทยว่าเป็นประเทศที่มีการค้าประเวณีเด็กเป็นอุตสาหกรรมหลักมากที่สุด ถึงประมาณ 2 แสนคน โดยที่รัฐบาลไทยไม่มีความพยายามที่จะแก้ไขปัญหาอย่างจริงจัง แต่ในทางตรงข้ามประเทศไทยมีรายได้จากการนี้ถึง 2 พันล้านเหรียญต่อปี อาชญากรเหล่านี้เรียกคนไทยว่าเป็น "ซาตาน" เป็นพวกขายลูกกิน และเชิญชวนให้เลิกซื้อสินค้าไทย เพื่อคว่ำบาตรทางเศรษฐกิจ ซึ่งพิจารณาให้ดีแล้วปรากฏว่ามีหลายสิ่งที่น่าเคลือบแคลงสงสัยอยู่ เพราะโฮมเพจนี้มีธุรกิจเข้ามาเกี่ยวข้อง เช่น การที่แอนดริว วาเชส (Andrew Vachss) ผู้ก่อตั้ง Don't! Buy! Thai! เป็นผู้เขียนโครงเรื่องให้กับหนังสือการ์ตูนชุด มนุษย์ค้างคาว ตอน The Ultimate Evil (ซึ่งอาจแปลเป็นไทยได้ว่า "สุดยอดแห่งความชั่วร้าย") ถึงแม้ว่าชื่อประเทศในเรื่องจะเป็น "อุดรคาย" แต่มีการระบุไว้ชัดเจนที่ท้ายเรื่องว่า เป็นสิ่งชั่วร้ายที่สุดในเรื่องดังกล่าวเป็นเรื่องจริง พร้อมสิ่งตีพิมพ์บทความ 12 หน้าโจมตีประเทศไทยเอาไว้

นอกจากนี้ Don't! Buy! Thai! ยังได้เชิญชวนให้ชาวเน็ตปกป้องเด็กและร่วมสนับสนุนการคว่ำบาตรด้วยการดาวน์โหลดรูปสัญลักษณ์ "สุนัขใส่เสื้อ" ไปไว้บนโฮมเพจส่วนตัว จนมีคนจำนวนมากคล้อยตาม ทั้ง ๆ ที่หลาย ๆ คนไม่เคยมาเมืองไทย จึงเป็นการกระทำอาชญากรรมที่มีลักษณะของการเหยียดหยามชนชาติอื่น และเชื่อว่าชนชาติของตนเองดีที่สุด ที่เรียกว่า "Racism" รวมอยู่ในกรณีนี้ด้วย

ดังนั้น จึงเป็นที่แน่นอนว่า อาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นโดยอาศัยเครือข่ายอินเตอร์เนตในประเทศสหรัฐอเมริกาเป็นอย่างไร ก็สามารถเกิดขึ้นได้ ในประเทศไทยจึงจำเป็นที่จะต้องศึกษาและหาทางป้องกันความเสียหายที่จะเกิดขึ้น