บทที่ 3

การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์

ก่อนที่จะกล่าวถึงการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ซึ่งถือกันว่าเป็นอาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง จะขอกล่าวถึงขอบเขตของอาชญากรรมคอมพิวเตอร์เสียก่อน โดยนักกฎหมายบางท่านเห็นว่าขอบเขตของอาชญากรรมคอมพิวเตอร์จำต้องมีการใช้คอมพิวเตอร์ในการกระทำความผิด (Computer Abuse) กล่าวคือผลสำเร็จของการกระทำต้องอาศัยความรู้ในเชิงเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญ การใช้คอมพิวเตอร์ในการกระทำความผิดสามารถแบ่งได้อย่างกว้างๆ ออกเป็น 3 ชนิดด้วยกัน คือ

1. เป็นการใช้คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือของการกระทำความผิด (Instrument) เช่น ใช้คอมพิวเตอร์เพื่อที่จะกระทำความผิดฐานฉ้อโกง ลักทรัพย์ หรือยักยอกทรัพย์ โดยมีเจตนาที่จะได้ไปซึ่งประโยชน์อันเกี่ยวกับการเงิน การค้า ทรัพย์สินหรือบริการ

2. เป็นการกระทำต่อตัวเครื่องคอมพิวเตอร์ อาจเรียกได้ว่าเป็นเรื่องของคอมพิวเตอร์ในฐานะที่เป็นวัตถุเป้าหมายของการกระทำความผิด (Object) เช่น การลักขโมยเครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ การทำลายหรือการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ หรือสิ่งที่บรรจุอยู่ภายในเครื่องคอมพิวเตอร์ เช่น ข้อมูล หรือโปรแกรม

3. การใช้คอมพิวเตอร์ในฐานะสัญลักษณ์ (Symbol) ความผิดทางอาญาซึ่งกระทำผ่านคอมพิวเตอร์บางอย่าง ที่ยังไม่ได้บัญญัติให้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด แต่เป็นเพียงแค่สัญลักษณ์ ความผิดเหล่านี้อาศัยความลึกลับซับซ้อนของคอมพิวเตอร์เป็นวิธีเพื่อการฉ้อโกง ตัวอย่างในกรณีนี้ เช่นเรื่องของการให้บริการนัดหมาย (Date) ซึ่งอ้างว่าจะใช้คอมพิวเตอร์เป็นเครื่องมือช่วยในการนัดหมาย แต่ความจริงกลับไม่มีหรือไม่ใช้คอมพิวเตอร์กระทำการติดต่อจัดคู่ดังกล่าวอย่างแท้จริง มีเพียงสมุดคู่มือหรือให้พนักงานที่มีตำแหน่งเป็นเพียงแค่เสมียนที่ไม่ได้รับการฝึกฝนมาก่อนเป็นผู้ทำหน้าที่ติดต่อนัดหมาย (วีระพงษ์ บุญโญภาส, 2540 : 166-167)

การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์มีด้วยกันหลายประเภท แตกต่างกันไปขึ้นอยู่กับวัตถุประสงค์และรูปแบบวิธีการกระทำนั้น แต่สิ่งหนึ่งที่ไม่อาจหลีกเลี่ยงได้สำหรับการกระทำความผิดดังกล่าวไม่ว่าจะเป็นรูปแบบใดก็ตามคือผลของการกระทำความผิด อันนำมาซึ่งความเสียหายต่อเจ้าของข้อมูลนับเป็นมูลค่ามหาศาล ทางออกหรือวิธีการแก้ปัญหาอันเป็นที่ยอมรับของสังคมทั่วไปวิธีหนึ่งก็คือ การนำกฎหมายที่มีอยู่มาจัดการกับการกระทำความผิดประเภทนี้ แต่ในทางปฏิบัติกฎหมายที่มีอยู่ไม่สามารถที่จะปรับใช้ได้หรือปรับใช้ได้ก็ไม่สมบูรณ์ ทางออกประการต่อมาก็คือการแก้ไขเพิ่มเติมหรือการบัญญัติกฎหมายขึ้นมาใหม่ ให้สามารถครอบคลุมถึงการกระทำความผิดในลักษณะดังกล่าว เพื่อที่จะได้นำตัวผู้กระทำผิดมาลงโทษ ดังนั้น ก่อนที่จะทำการวิเคราะห์ถึงปัญหาทางกฎหมาย สมควรอย่างยิ่งที่จะต้องกล่าวถึงลักษณะของการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ว่ามีรูปแบบวิธีการใดบ้าง

3.1 การลักลอบเข้าถึงและการใช้ข้อมูล

ก่อนที่จะกล่าวถึงการลักลอบเข้าถึงและการใช้ข้อมูล จำเป็นอย่างยิ่งที่จะต้องทราบถึงความหมายของคำว่าการเข้าถึง (Access) เสียก่อน แม้ว่าความหมายของคำนี้จะเป็นที่ทราบกันทั่วไปในหมู่นักคอมพิวเตอร์และอาจถือกันว่าไม่ใช่เรื่องสำคัญมากนัก แต่มีความจำเป็นอย่างมากสำหรับนักกฎหมายโดยเฉพาะนักกฎหมายอาญา อันจะต้องยึดถือหลักการตีความโดยเคร่งครัดกฎหมายอันมีโทษทางอาญาของประเทศไทยยังไม่เคยมีการบัญญัติให้คำจำกัดความคำๆ นี้ไว้เป็นลายลักษณ์อักษร แต่เราสามารถที่จะศึกษาจากคำนิยามของกฎหมายต่างประเทศได้ เพื่อใช้เป็นแนวทางในการบัญญัติกฎหมายของประเทศต่อไป

คำนิยามของคำว่า "เข้าถึง" ที่กฎหมายของสหรัฐอเมริกาส่วนใหญ่นิยมใช้กันอยู่ ได้แก่

"เข้าถึง" (Access) หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากหรืออีกนัยหนึ่ง เอาประโยชน์ใดๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้

ตามคำนิยามนี้ใช้คำว่า "อีกนัยหนึ่ง..." ดังนั้น การเข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์จึงมีความหมายในลักษณะของการกระทำที่เป็นไปเพื่อการเอาประโยชน์ของเครื่องคอมพิวเตอร์ ฯลฯ มาใช้ด้วย ดังนั้น ความหมายของการกระทำต่างๆ ในคำนิยามอาจอธิบายได้ดังนี้

"เข้าไปสู่" (Approach) หมายถึง การกระทำที่เป็นการเข้าหาหรือเข้าไปสู่สิ่งที่ตนต้องการภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์

"สั่ง" (Instruct) หมายถึง การกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ทำงานให้ตามความต้องการของตน

"สื่อสารกับ" (Communicate with) หมายถึง การกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ด้วยวิธีการทางการสื่อสาร เช่น ผ่านสายโทรศัพท์ เป็นต้น เพื่อให้ได้ข้อมูลหรือประโยชน์อย่างอื่นตามความต้องการของตน

"ใส่ข้อมูลเข้าไปเก็บไว้" (Store data in) หมายถึง การกระทำที่เป็นการนำข้อมูลใส่เข้าไปในเครื่องคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อตนจะได้ประโยชน์จากการทำงานของเครื่องคอมพิวเตอร์ ฯลฯ ในภายหลัง

"ล้วงข้อมูลมาจาก" (Retrieve data from) หมายถึง การกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เพื่อประโยชน์ของตน

"เอาประโยชน์ใดๆ มาใช้" (Make use of any resources of) หมายถึง การกระทำใดๆ ต่อเครื่องคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ที่เป็นไปเพื่อประโยชน์ของตน (ภานุ รังสีสหัส, 2533 : 53)

การกระทำความผิดในการลักลอบเข้าถึงและการใช้ข้อมูลนั้น เนื่องจากปัจจุบันฐานข้อมูลในคอมพิวเตอร์ของหน่วยงานต่างๆ นิยมใช้ระบบฐานข้อมูลสำเร็จรูปสามารถเข้าถึง (Access) ได้โดยง่าย ไม่จำต้องอาศัยการเขียนโปรแกรมให้ยุ่งยาก ทำให้การลักลอบเข้าถึงข้อมูลหรือโดยทั่วไปนิยมเรียกกันว่าการเข้าถึงข้อมูลโดยปราศจากอำนาจ (Unauthorized Access) สามารถกระทำได้สะดวก ไม่ว่าผู้กระทำจะเป็นบุคคลภายในหรือบุคคลภายนอกหน่วยงานก็ตาม โดยปกติแล้วเกือบทุกหน่วยงาน จะมีการจำกัดอำนาจและเวลาของการเข้าถึงสำหรับบุคคลในหน่วยงานไว้ เพื่อวัตถุประสงค์การเข้าถึงข้อมูลเฉพาะอย่าง แต่ผู้กระทำจะกระทำนอกเหนืออำนาจหรือเวลาโดยหาโอกาสที่เหมาะสม เพื่อกระทำการโดยปราศจากการอนุญาตให้เข้าถึงข้อมูล การเข้าถึงข้อมูลบางกรณี ผู้กระทำมีอำนาจแห่งการเข้าถึง แต่ได้ใช้การเข้าถึงนั้นเพื่อที่จะได้รับหรือทำการแก้ไขเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์นั้น ซึ่งผู้ที่เข้าถึงไม่มีสิทธิที่จะได้รับหรือแก้ไขเปลี่ยนแปลงข้อมูลนั้น จะเรียกการกระทำในลักษณะนี้ว่า "การกระทำเกินกว่าอำนาจแห่งการเข้าถึง" (Exceeds Authorized Access)

สำหรับวิธีการของการเข้าถึงข้อมูล ด้วยเทคโนโลยีในปัจจุบันไม่ต้องเข้าไปในสถานที่ตั้งของคอมพิวเตอร์หลัก เพียงแต่มีคอมพิวเตอร์ส่วนบุคคลที่ติดตั้งซอฟต์แวร์ในการติดต่อกับเครือข่ายและโมเด็มที่พ่วงกับคู่สายโทรศัพท์ โดยทำการติดตั้งตามรายละเอียดในหัวข้อ 2.1.2.4 (ง) ก็จะสามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่ประสงค์จะเข้าถึงและใช้ข้อมูลนั้นได้ ความมุ่งหวังของผู้กระทำที่เป็นบุคคลภายในหน่วยงาน บางกรณีไม่ถึงกับเป็นการจารกรรมข้อมูลเพื่อประโยชน์ทางธุรกิจ แต่กระทำเพราะความอยากรู้อยากเห็นข้อมูลส่วนตัวของตนเองหรือของพนักงานคนอื่นที่หน่วยงานเก็บไว้เป็นความลับ เช่น รายได้ของพนักงาน แต่ก็มีบางกรณีที่หน่วยงานจะต้องให้ความสนใจเป็นอย่างยิ่ง เพราะผู้กระทำได้กระทำไปเนื่องจากต้องการทดสอบความสามารถของตนเองในการที่จะผ่านระบบการรักษาความปลอดภัย

ระบบการรักษาความปลอดภัยของคอมพิวเตอร์ที่ใช้กันโดยทั่วไป อุปกรณ์ต่างๆ จะจำกัดการเข้าถึง โดยผู้มีอำนาจใช้จะต้องมีการระบุผู้ใช้ (User Identification : User-ID) และรหัสผ่าน (Password) เพื่อใช้เป็นกุญแจเข้าไปในระบบ อย่างไรก็ตามในทางปฏิบัติอาจจะไม่แน่นหนาพอเท่าที่ควรจะเป็น เพราะทั้งการระบุผู้ใช้และรหัสผ่านไม่ได้ถูกเก็บเป็นความลับส่วนตัว แต่จะเป็นที่ทราบกันในบรรดาเพื่อนร่วมงานเพื่อความสะดวกในการปฏิบัติงาน หรือบางกรณีสถานที่ที่จะต้องพิสูจน์รหัสผ่านอยู่ในตำแหน่งที่ไม่เหมาะสม บุคคลอื่นสามารถเห็นรหัสผ่านของผู้พิสูจน์ได้ง่าย และหลายครั้งที่ผู้กระทำความผิดสามารถเข้าถึงข้อมูลจากการทำนายรหัสผ่าน โดยการสุ่มตัวเลขหรือตัวอักษรที่มีความสัมพันธ์กับเจ้าของรหัสผ่าน เช่น ชื่อเล่น วันเดือนปีเกิด เป็นต้น

ถ้าจะปรับการกระทำความผิดดังกล่าวกับฐานความผิดทางอาญาแล้ว ก็คงจะต้องปรับได้กับความผิดฐานลักทรัพย์และฐานบุกรุก ซึ่งไม่น่าจะมีปัญหาอะไรสำหรับการบังคับใช้กฎหมาย ถ้าหากการกระทำดังกล่าวได้กระทำต่อตัวเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆ ที่เป็นส่วนประกอบของคอมพิวเตอร์อันสามารถมองเห็นได้ด้วยทางกายภาพ หรือผู้กระทำต้องเข้าไปในอาคารศูนย์คอมพิวเตอร์แห่งนั้น แต่ในความเป็นจริงข้อมูลในคอมพิวเตอร์เป็นสิ่งที่ไม่สามารถมองเห็นได้ด้วยทางกายภาพ การปรับใช้กฎหมายจึงก่อให้เกิดปัญหาการตีความ อันเป็นสาเหตุให้หลายประเทศต้องบัญญัติกฎหมายมาบังคับใช้กับการกระทำความผิดชนิดนี้เป็นการเฉพาะ สำหรับปัญหาองค์ประกอบความผิดอีกประการหนึ่งก็คือองค์ประกอบภายในหรือเจตนา ซึ่งบางครั้งผู้กระทำได้กระทำเพียงเพื่ออยากรู้อยากเห็นข้อมูลบางประเภทและก็มิได้มีเจตนาที่ชั่วร้ายจนเกินไป แต่ข้อมูลนั้นอาจเป็นความลับ ทำให้เราจะต้องพิจารณาถึงความเหมาะสมที่จะใช้กฎหมายอาญาเพื่อป้องกันข้อมูล

อันเป็นปัญหาสำหรับนักกฎหมายอาญาว่าการกระทำอันเป็น "การบุกรุกทางคอมพิวเตอร์" (Computer Trespass) ควรที่จะผิดกฎหมายหรือไม่ แม้จะมีคำกล่าวที่ว่าผู้กระทำไม่มีเจตนาชั่วร้ายแต่ผู้กระทำก็ได้รับประโยชน์จากการเข้าถึงข้อมูลนั้น และก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล อันอาจจะกระทบต่อข้อมูลที่เป็นความลับหรือข้อมูลที่มีความอ่อนไหว แม้ว่าบางกรณีผู้กระทำอาจจะไม่ได้รับผลประโยชน์อะไรเลยเพราะระบบถูกปิดลงเสียก่อน อันเนื่องมาจากการพยายามที่จะฝ่าระบบรักษาความปลอดภัย แต่เจ้าของก็เกิดความสูญเสียหรือไม่ได้รับความสะดวกที่ระบบถูกปิดลง

นับว่าเป็นสิ่งที่ยากที่จะแบ่งแยกความแตกต่างระหว่าง การมีเจตนาของนักคอมพิวเตอร์ ซึ่งนายฮิวโก คอร์นวอล์ (Hugo Cornwall) นักคอมพิวเตอร์และผู้แต่งหนังสือเรื่องการเข้าถึงโดยปราศจากอำนาจได้กล่าวว่า คอมพิวเตอร์สำหรับตนแล้วเป็นเพียงกีฬาชนิดหนึ่งโดยเฉพาะการพัฒนาสิ่งใหม่ๆ ของคอมพิวเตอร์ ย่อมเป็นจุดมุ่งหมายที่น่าสนใจที่จะเข้าถึง โดยที่ตนเองไม่เคยมีเจตนาที่จะก่อให้เกิดความเสียหายแต่อย่างใด (Cornwall, 1985 : 8) เจตนาหรือวัตถุประสงค์ของการเข้าถึงโดยปราศจากอำนาจ ดูเหมือนจะเป็นสิ่งที่เคลือบคลุมอยู่ภายในจิตใจของผู้กระทำอันยากที่จะชี้เฉพาะเจาะจงลงไป ดังนั้น การฟ้องร้องในหลายคดีได้ใช้องค์ประกอบความผิดฐานลักขโมย ฉ้อโกง หรือการพยายามกระทำความผิด อันถือว่าการลงมือกระทำซึ่งมากกว่าการตระเตรียมการก็เป็นความผิดแล้ว โดยไม่ต้องคำนึงถึงผลของการกระทำ

ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะของการเข้าถึงโดยปราศจากอำนาจโดยผู้กระทำไม่มีเจตนาที่ชั่วร้าย

คดีนี้เกิดขึ้นที่รัฐแคลิฟอร์เนีย เครื่องคอมพิวเตอร์ของกระทรวงกลาโหม สหรัฐอเมริกา ถูกเข้าถึงโดยปราศจากอำนาจ ทางเพื่อนๆ และครูที่สอนเด็กนักเรียน 2 คนที่ถูกการกล่าวหาเกี่ยวกับเรื่องนี้ได้ออกมากล่าวว่าพวกเขาเชื่อว่าเด็กนักเรียนทั้ง 2 คนนี้ไม่ใช่ผู้กระทำการที่มีเจตนาที่เลวร้ายแฝงอยู่แต่อย่างใด โดยครูที่สอนวิชาคอมพิวเตอร์ของเด็กทั้ง 2 คนนี้ได้กล่าวแสดงความคิดว่า "เด็กทั้ง 2 คนปกติเป็นเด็กดีเป็นเด็กที่ฉลาด ทางตัวครูเองก็ได้ทราบเรื่องว่าเด็กอาจจะได้กระทำอะไรลงไป แต่ก็ยังยืนยันว่าเด็กทั้ง 2 นี้เป็นเด็กดี" ส่วนเพื่อนๆ ของผู้ต้องหาที่เป็นเด็กจำนวน 15 คน ได้กล่าวเป็นเสียงเดียวกับคุณครูของพวกเขาทั้งสิ้น นอกจากนั้นยังมีการสัมภาษณ์เด็กมัธยมคนอื่นๆ อีก 20 คน ในจำนวน 450 คนด้วย ก็กล่าวเป็นเสียงเดียวกันว่าเด็กทั้ง 2 คนนี้ไม่เคยมีประวัติที่เคยสร้างเรื่องไม่ดีในโรงเรียนมาก่อนเช่นกัน ขณะที่ทางหน่วยงานสืบสวนสอบสวนของรัฐบาลกลางสหรัฐอเมริกา (Federal Bureau of Investigation : FBI) กำลังดำเนินการสืบสวนเรื่องนี้ ว่ามี

เครื่องคอมพิวเตอร์เครื่องไหนของหน่วยงานดังกล่าวที่ได้รับผลกระทบบ้าง แต่ว่าทางคณะผู้สืบสวนก็ไม่ได้ให้ความคิดเห็นต่อคดีนี้แต่อย่างใด สำหรับที่บ้านของเด็กทั้ง 2 คนนี้ ก็ได้ถูกทางการยึดไว้ รวมทั้งหลักฐานอื่นๆ แต่ก็ไม่ได้มีการจับกุมบุคคลใดทั้งสิ้นรวมทั้งตัวของเด็กทั้ง 2 คนที่ได้รับการกล่าวหานี้ด้วย

(Http://www.fm97.ksc.net/it_talk/980314/newstalk.html, 11 June 1998)

อีกตัวอย่างหนึ่งเป็นเรื่องเกี่ยวกับวัยรุ่นชาวเยอรมัน 2 คน ได้กระทำการเข้าถึงโดยปราศจากอำนาจในระบบทีออนไลน์ (T-Online) เป็นธุรกิจบริการชนิดหนึ่งดำเนินการโดยบริษัทโทรศัพท์แห่งชาติเยอรมัน ผู้กระทำทั้ง 2 คนอายุเพียง 16 ปีเท่านั้น ได้กล่าวอวดถึงความสามารถของตนเองให้กับหนังสือนิตยสารเล่มหนึ่งของเยอรมัน ทำให้การเข้าถึงข้อมูลโดยปราศจากอำนาจกลายเป็นสิ่งที่น่าเป็นห่วงมากสำหรับข้อมูลต่างๆ ในเครือข่ายคอมพิวเตอร์ เหตุการณ์ดังกล่าวเกิดขึ้นเนื่องจากวัยรุ่นชาวเยอรมัน 2 คนนี้ฉลาดทั้งยังต้องการความตื่นเต้นและความท้าทายจึงได้กระทำการลงไป

(Http://www.fm97.ksc.net/it_talk/980411/newstalk.html, 11 June 1998)

ตัวอย่างการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะของการเข้าถึงโดยปราศจากอำนาจโดยที่ผู้กระทำมีเจตนาที่ชั่วร้าย

การกระทำนี้ได้เกิดขึ้นที่กรุงวอชิงตัน เครือข่ายเครื่องคอมพิวเตอร์ที่ไม่ได้รับการคัดแยกของศูนย์กลางทางการทหารของสหรัฐอเมริกา (Pentagon) ถูกละเลย ทำให้มีการเข้าถึงโดยปราศจากอำนาจ นายจอห์น ฮาร์มี่ (John Harme) ซึ่งเป็นรองเลขาธิการของกระทรวงกลาโหมกล่าวว่า "เป็นการโจมตีทางระบบที่ได้รับการเตรียมการมาอย่างดีเท่าที่เคยเห็นมา และดูเหมือนว่าจะมีกลุ่มคนเล็กๆ กลุ่มหนึ่งที่เป็นรายบุคคลที่เข้ามาโจมตีในครั้งนี้" และยังได้กล่าวต่อไปอีกว่าตนรู้สึกฝืนใจจากการที่ต้องมาเปิดเผยข้อมูลต่างๆ ของการโจมตีครั้งนี้เพราะว่าทางหน่วยงานทหารก็กำลังทำงานร่วมกับทางกระทรวงยุติธรรม ในการติดตามการกระทำอาชญากรรมเหล่านี้อยู่ เจ้าหน้าที่กล่าวว่าการโจมตีเหล่านี้ ดูเหมือนจะมุ่งไปที่ข้อมูลที่ไม่มีการจำแนกว่าเป็นความลับของประเทศ (Unclassified) เช่น ข้อมูลบัญชีเงินเดือนส่วนตัว เป็นต้น ส่วนข้อมูลที่มีการจำแนกว่าเป็นความลับของประเทศ (Classified) นั้นไม่ได้รับการแตะต้องแต่อย่างใด

(Http://www.fm97.ksc.net/it_talk/980307/newstalk.html, 11 June 1998)

อีกตัวอย่างหนึ่ง ได้มีผู้ที่กระทำการเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ โดยผู้กระทำได้อาศัยอยู่ที่ประเทศอาร์เจนตินาตกลงใจที่จะมาที่กรุงบอสตัน เพื่อทำการสารภาพความผิดที่เขาได้กระทำการเข้าไปในระบบคอมพิวเตอร์ของมหาวิทยาลัยฮาร์เวิร์ด (Harvard University) เพื่อเข้าไปสืบค้นเอกสารต่างๆ ของทางกองทหารสหรัฐอเมริกา ซึ่งทางเจ้าหน้าที่ของประเทศสหรัฐอเมริกาได้ทำการตามล่า นายจูลิโอ ซีซ่าร์ อาร์ดิต้า (Julio Cesar Ardita) นักศึกษาคณะวิทยาศาสตร์คอมพิวเตอร์ วัย 23 ปี และที่สำคัญคือเป็นบุตรของนายทหารเก่าประเทศอาร์เจนตินา โดยทางเจ้าหน้าที่ทางการศาลได้ขอให้มีการยึดของกลาง ซึ่งได้แก่ แฟ้มข้อมูลต่างๆ และเครื่องคอมพิวเตอร์ของเขาอีกหนึ่งเครื่อง เนื่องจากการดำเนินคดีต่างๆ ภายใต้สนธิสัญญาระหว่างประเทศของสหรัฐอเมริกานั้นไม่ได้เป็นความผิดข้ามแดน ดังนั้นนายอาร์ดิต้าจะต้องทำการยอมรับว่าไม่ได้กระทำการข้ามแดน และภายใต้ข้อตกลงทนายความจากประเทศสหรัฐอเมริกาได้กล่าวว่านายอาร์ดิต้าจะต้องถูกดำเนินคดี และต้องสารภาพความผิดด้วยความบริสุทธิ์ใจว่าได้กระทำการแทรกแซงการสื่อสารทางอิเล็กทรอนิกส์บนเครื่องคอมพิวเตอร์ของทหารจริง แต่ไม่ได้ทำลายแฟ้มข้อมูลต่างๆ บนเครื่องคอมพิวเตอร์ของทหาร ซึ่งเขาจะต้องได้รับการตัดสินจำคุก 3 ปี และปรับอีกจำนวน 5,000 เหรียญสหรัฐอเมริกา

(Http://www.fm97.ksc.net/it_talk/971220/newstalk.html, 11 June 1998)

3.2 การคัดลอกข้อมูล

การคัดลอกข้อมูลโดยปราศจากอำนาจ เป็นการกระทำหลังจากผ่านขั้นตอนของการเข้าถึงข้อมูลแล้ว การคัดลอกข้อมูลสามารถกระทำได้ 2 แบบ แบบที่หนึ่งคือการคัดลอกข้อมูลเหมือนต้นแบบทั้งหมดหรือทำสำเนา (Copy) อีกแบบหนึ่งคือการคัดลอกข้อมูลเหมือนต้นแบบทั้งหมดหรือบางส่วนหรือตัดทอน (Extract) การกระทำทั้งสองแบบผู้กระทำสามารถกระทำได้โดยง่ายเพียงแต่สามารถเข้าถึงข้อมูลดังที่กล่าวมาแล้ว เว้นแต่ในบางกรณีเท่านั้นที่จำเป็นจะต้องอาศัยความรู้ทางเทคโนโลยีสารสนเทศเข้ามาช่วย แต่ไม่ว่าจะกระทำด้วยวิธีใดก็ตามจะไม่ทำให้ข้อมูลลดน้อยลงไป และผู้กระทำก็ไม่ประสงค์จะแทรกแซงเนื้อหาแต่ประการใด นอกเหนือจากการคัดลอกข้อมูลยังมีการกระทำอีกลักษณะหนึ่งที่ คือการลักลอบสกัดข้อมูลของบุคคลอื่นโดยปราศจากอำนาจ การสกัดข้อมูลในลักษณะนี้หมายถึงการลอบนำเอาข้อมูลของบุคคลอื่นมาด้วยวิธีใดก็ตาม เช่น การแอบซ่อนอุปกรณ์ดักฟัง การใช้กล้องถ่ายภาพที่สามารถทำงานได้ในระยะไกล หรือการใช้อุปกรณ์อื่นๆ ที่เชื่อมโยงกับคอมพิวเตอร์เพื่อที่จะทำการสกัดข้อมูล โดยจะเรียกว่าการกระทำดังกล่าวว่าเป็นการสกัดโดยปราศจากอำนาจ (Unauthorized Interception)

แต่ไม่ว่าการคัดลอกข้อมูลจะกระทำด้วยวิธีการใดก็ตาม เช่น การสกัดข้อมูลเพื่อบันทึกลงในสื่อต่างๆ หรือด้วยวิธีอื่น ก็จะส่งผลให้ผู้กระทำนั้นได้รับประโยชน์มหาศาล เพราะโดยมากแล้วข้อมูลที่ถูกจารกรรมจะเป็นข้อมูลที่เป็นความลับมีมูลค่าทางธุรกิจ เช่น ข้อมูลทางด้านการเงิน ข้อมูลทางด้านอุตสาหกรรม โดยมีมูลเหตุของการจารกรรมข้อมูลหลายสาเหตุ เช่น การฉ้อฉล การฉ้อโกง การรีดไถของลูกจ้าง การแทรกซึมของบริษัทคู่แข่งโดยใช้ลูกจ้างเป็นเครื่องมือ และด้วยเทคโนโลยีในปัจจุบัน นอกเหนือจากการที่ผู้กระทำได้รับข้อมูลไปด้วยวิธีการที่มิชอบแล้ว ยังได้ปกปิดการกระทำของตนเพื่อให้เหยื่อละเลยต่อความเสียหายหรือความปลอดภัยของข้อมูล เพื่อที่ตนจะได้ใช้ประโยชน์จากข้อมูลนั้นได้นานที่สุดที่เท่าจะเป็นไปได้

ตามรายงานของคณะกรรมาธิการแก้ไขกฎหมายของอังกฤษ (The Audit Commission) ในปี 1987 พบว่าในคดีหนึ่งนักคอมพิวเตอร์ ซึ่งตามสัญญาเขามีอำนาจที่จะเข้าถึงระบบคอมพิวเตอร์ เขาได้ใช้อภิสิทธิ์เอาเทปคอมพิวเตอร์ ออกไปจากที่ทำงานและทำการคัดลอกข้อมูลจากเทปคอมพิวเตอร์ต่างๆ ของบริษัทไว้ ซึ่งการคัดลอกข้อมูลนี้ได้ปรากฏเรื่องขึ้นมา เมื่อเขาได้เสนอที่จะขายสิ่งที่คัดลอกนี้ต่อนายจ้างใหม่ของเขา (พรชัย เหลียวพัฒนพงศ์, 2537 : 63)

มีรูปแบบการลักลอบคัดลอกข้อมูลของบุคคลที่ไม่ได้รับอนุญาตให้เข้าไปในระบบ ที่จะนำมาเป็นกรณีศึกษาอีกรูปแบบหนึ่ง โดยมีสาระสำคัญที่จะพิจารณา 2 ประการ คือ

1. เจ้าของข้อมูลมีความประสงค์ที่จะให้มีการใช้ข้อมูลโดยทั่วไป (Willing to Make Access Abailable) โดยขึ้นอยู่กับค่าธรรมเนียมที่จะได้รับ
2. ผู้ใช้ข้อมูลไม่ได้มีความประสงค์ที่จะเผยแพร่ข้อมูลดังกล่าวไปยังสาธารณะ เป็นการกระทำในลักษณะของผู้บุกรุก

กรณีศึกษานี้เป็นคดีที่เกิดขึ้นกับบริษัทบริสทีส เทเลคอม (Bristish Telecom) ผู้ให้บริการทางคอมพิวเตอร์ที่มีชื่อว่าพรีสเทล (Prestel) บริการนี้เป็นบริการไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail) ให้กับผู้สมัครเข้าใช้บริการ โดยจะกำหนดรหัสผ่านและหมายเลขผู้ขอใช้บริการ ทั้งนี้ เพื่อควบคุมการใช้บริการและนำมาคิดเป็นค่าธรรมเนียมในการให้บริการ โดยเจ้าหน้าที่ของบริษัทจะได้รับรหัสผ่านพิเศษเพื่อเอาไว้ใช้งาน อันเป็นเป้าหมายของผู้ที่จะทำการบุกรุกที่ต้องการทราบรหัสผ่านพิเศษนี้ ซึ่งจะทำให้สามารถเข้ามาใช้ระบบได้โดยไม่ต้องเสียค่าบริการแต่อย่างใด โดยคดีนี้มีการกล่าวหาว่านายโกลด์ (Gold) ได้ร่วมมือกับนายชีฟริน (Schifreen) กระทำการเข้ามาลักขโมยรหัสผ่านพิเศษนี้ไปใช้ก่อนที่จะถูกจับได้ในที่สุด อย่างไรก็ตามทั้งสองคนได้ถูกปล่อยตัวไป

เพราะศาลได้ชี้ประเด็นคำนิยามของคำว่า "เครื่องมือที่ใช้ในการกระทำผิด" (Instrument) ใน The Theft Act of 1968 ได้กำหนดเพียงจานบันทึก แถบบันทึก เครื่องบันทึกเสียงและสื่ออื่นๆ ซึ่งได้จัดเก็บข้อมูลจึงจะถือว่าเป็นเครื่องมือ

สาเหตุที่ไม่สามารถดำเนินคดีในกรณีนี้ได้มีด้วยกัน 2 ประการคือ ประการแรกเนื่องมาจากลักษณะของรหัสผ่านเองไม่ได้มีรายละเอียดระบุถึงการคงอยู่ของรหัสผ่านและใช้เวลาไม่ถึง 1 วินาที ซึ่งเป็นเวลาที่น้อยมากจนไม่สามารถวัดเป็นระยะได้ตามกฎหมาย ประการที่สองก็คือการที่ไม่สามารถระบุว่าระบบคอมพิวเตอร์ของบริการดังกล่าวนั้นตกเป็นเหยื่อ และเป็นสิ่งที่ถูกทำให้เกิดการฉ้อฉลขึ้น ดังนั้น ศาลจึงได้วินิจฉัยว่าการกระทำดังกล่าว จำเลยไม่ได้กระทำความผิดเพียงแต่เป็นการใช้เทคนิค (Trick) เท่านั้น จึงไม่ถือว่าได้เป็นการก่ออาชญากรรม

จากกรณีดังกล่าวแสดงให้เห็นว่าเจ้าของข้อมูลที่มีไว้เพื่อการทำธุรกิจการค้านั้น มีความเสี่ยงในการตกเป็นเหยื่อหรือเป้าหมายของบรรดาผู้บุกรุกได้ ซึ่งจำเป็นอย่างยิ่งที่จะต้องมีการปฏิรูปกฎหมาย อย่างไรก็ตามคดีนี้เกิดขึ้นในประเทศอังกฤษ ถ้าเกิดขึ้นที่ประเทศสก็อตแลนด์จำเลยทั้งสองอาจจะต้องถูกลงโทษ เพราะกฎหมายของประเทศสก็อตแลนด์จะพิจารณาจากวัตถุประสงค์ของการได้มาซึ่งข้อมูลเป็นหลักว่าได้มีการได้มาอย่างถูกต้องหรือไม่ แต่กฎหมายของประเทศอังกฤษจะพิจารณาด้วยว่าผู้ถูกกระทำนั้น ซึ่งในที่นี้คือเครื่องคอมพิวเตอร์นั้นไม่สามารถถูกระบุว่าโดนโกงได้ สรุปว่าคดีนี้จำเลยไม่ต้องรับผิดแต่อย่างใด
(Http://www.strath.ac.uk/Departments/Law/diglib/book/criminal, 14 August 1998)

ยังมีตัวอย่างของการคัดลอกข้อมูลโดยปราศจากอำนาจอีกหลายตัวอย่าง ดังนี้

ชายคนหนึ่งชื่อนายคาร์ลอส ฟิลิป ซาลกาโด (Carlos Filipe Salgado) วัย 36 ปี ได้ถูกทางหน่วยงานสืบสวนสอบสวนของรัฐบาลกลางสหรัฐอเมริกา (Federal Bureau of Investigation : FBI) จับตัวมาดำเนินคดีในข้อหาพยายามเข้าไปขโมยข้อมูลจากฐานข้อมูลหมายเลขบัตรเครดิตกว่าเจ็ดแสนหมายเลขในเครือข่ายต่างๆ ที่ให้บริการส่งของบนเครือข่ายอินเตอร์เน็ต ในที่สุดเขาก็ถูกจับได้ตามแผนของทางการ ซึ่งได้พยายามติดตามตัวนายซาลกาโดเป็นเวลานาน โดยเจ้าหน้าที่ในหน่วยงานดังกล่าวแสร้งทำเป็นว่าให้ความสนใจที่จะซื้อหมายเลขบัตรเครดิต ที่เขาเสนอขายในราคาถึง 260,000 เหรียญสหรัฐอเมริกา โดยได้ทำการติดต่อกับนายซาลกาโดทางเครือข่ายอินเตอร์เน็ต และนัดให้นำหมายเลขบัตรเครดิตไปส่งให้ที่สนามบินเมืองซานฟรานซิสโก เขาถูกจับในเวลาต่อมาเพราะไม่รู้ว่าเป็นแผนการของเจ้าหน้าที่ ในช่วงจับกุมทางการกล่าวว่านายซาลกาโด

อาจจะถูกตัดสินโทษด้วยข้อหาบุกรุกเข้าไปในเครือข่ายคอมพิวเตอร์ เพื่อขโมยข้อมูลเพียงข้อหาเดียว ซึ่งอาจจะถูกจำคุก 15 ปี หรือปรับไม่เกิน 250,000 เหรียญสหรัฐอเมริกา หรือทั้งจำทั้งปรับ หลังจากนั้นไม่นานนายซาลกาโดถูกนำตัวมาขึ้นศาล ศาลตัดสินว่าเขาทำผิดกฎหมายทั้งหมด 4 ข้อหา ดังนี้

ข้อหาที่ 1.คือ เข้าไปในเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต และมีวัตถุประสงค์เพื่อขโมยข้อมูล

ข้อหาที่ 2.คือ จำหน่ายหมายเลขบัตรเครดิตที่ลักขโมยมา

ข้อหาที่ 3.คือ มีหมายเลขบัตรเครดิตที่ได้มาอย่างผิดกฎหมายอยู่ในความครอบครองมากกว่า 15 หมายเลขขึ้นไป

ข้อหาที่ 4.คือ เจตนากระทำความผิด

ในที่สุดเขาก็ถูกศาลตัดสินจำคุก 30 ปี และปรับเป็นเงินอีก 1,000,000 เหรียญสหรัฐอเมริกา (Http://www.fm97.ksc.net/it_talk/970914/newstalk.html, 11 June 1998)

อีกตัวอย่างเกิดขึ้นที่รัฐโอไฮโอ นายสตีเฟน ลุย นักเขียนโปรแกรมคอมพิวเตอร์ วัย 24 ปี ถูกศาลตัดสินจำคุก 2 ปี หลังจากที่ได้ยอมรับว่าตนได้เข้าไปในระบบคอมพิวเตอร์ของทหาร กองกำลังทางอากาศ (Wright Patterson) จริง นายลุย เดิมทีเป็นชาวจีนที่ทำงานเพื่อสัญญาทางการทหาร โดยได้รับการลงโทษด้วยข้อหากระทำการคัดลอกข้อมูลโดยวิธีการบรรจุลง (Download) รหัสข้อมูลต่างๆ จากฐานข้อมูล (Database) ที่มีมูลค่ากว่า 148 ล้านเหรียญสหรัฐอเมริกา ซึ่งเป็นข้อมูลในส่วนของการสืบสวนเรื่องความพร้อมทางการต่อสู้ของกองกำลังทางอากาศ และเรื่องระบบจรวดมิสไซล์ทั่วโลก นายวิลเลี่ยม คอลเมอร์ (William Colmer) ผู้ที่เป็นผู้จัดการเรื่องระบบคอมพิวเตอร์กล่าวในศาลแขวงของสหรัฐอเมริกาว่า การบุกรุกนั้นเป็นเรื่องที่นำไปสู่การวิเคราะห์ระบบข้อมูลต่างๆ ของกองทัพอากาศกว่าหลายๆ พันระบบทั่วโลก เพื่อทำการตรวจสอบเรื่องจุดด้อยอื่นๆ ที่อาจจะเกิดขึ้นได้เช่นกันและได้กล่าวว่าซอฟต์แวร์เพื่อที่จะทำการยกระดับ (Upgrade) ความปลอดภัยของระบบคอมพิวเตอร์ของทหาร กองกำลังทางอากาศ (Wright Patterson) นั้น ได้ถูกใช้มาเป็นเวลานานแล้วเพียงแต่ว่าไม่ได้ใช้ในเวลาที่เกิดเหตุขึ้นเท่านั้น โดยการติดตั้งยังไม่เข้าที่ และในขณะนั้นทางเขาเองก็ตัดสินใจที่จะใช้งบประมาณที่มีไว้เพื่อเรื่องอื่นด้วย (Http://www.fm97.ksc.net/it_talk/971227/newstalk.html, 11 June 1998)

อีกตัวอย่างหนึ่ง เด็กวัยรุ่น 5 คนที่มีความฉลาดมากพอที่จะเข้าไปทำลายระบบรักษาความปลอดภัยในคอมพิวเตอร์ เพื่อที่จะขโมยเอาหมายเลขบัตรเครดิตออกมาเสร็จแล้วก็จะมีผู้มา

ซื้อหมายเลขที่ถูกขโมยมานั้น ตำรวจกล่าวว่าบรรดาเด็กทั้ง 5 คนนี้ มีอยู่คนหนึ่งอายุเพียง 15 ปี และได้เข้าศึกษาในวิทยาลัยแล้ว ได้กระทำการถอดรหัสของระบบรักษาความปลอดภัยเพื่อที่จะขโมยหมายเลขบัตรเครดิตจำนวน 20-25 หมายเลข เด็กวัยรุ่นเหล่านี้ได้ขายหมายเลขบัตรเครดิตโดยมีมูลค่าหลายพันเหรียญสหรัฐอเมริกา และยังได้ทำการสั่งซื้อของด้วยหมายเลขบัตรเครดิตนี้ด้วย ยอดซื้อสิ่งของต่างๆ จะปรากฏในบัญชีของเจ้าของบัญชีทุกๆ บัญชี โดยมีบัญชีหนึ่งปรากฏที่อยู่ของคู่สามีภรรยาคู่หนึ่งในบูลมิงตัน (Bloomington) เด็กกลุ่มนี้ได้หมายเลขบัตรเครดิตมาจากการเข้าไปในเครือข่ายการจำหน่ายสินค้า (Shopping) ผ่านเครือข่ายอินเตอร์เน็ต และจากร้านซักรีดแห่งหนึ่งซึ่งมีเด็กคนหนึ่งทำงานอยู่ ตำรวจกล่าวว่าได้พบอุปกรณ์คอมพิวเตอร์ เช่น เครื่องกราดตรวจ (Scanners) ตัวจอภาพ (Monitors) เครื่องเสียงติดรถยนต์ โทรศัพท์เคลื่อนที่และอุปกรณ์ไฟฟ้าอย่างอื่นอีกมากที่บ้านของกลุ่มผู้ต้องสงสัยเหล่านี้ เด็กกลุ่มนี้ยังถูกตัดสินลงโทษในข้อหาทำลายชื่อเสียงเครือข่ายของโรงเรียนมัธยมแห่งหนึ่ง ด้วยการเอาภาพอนาจารไปลงอีกข้อหาหนึ่งด้วย

(Http://www.fm97.ksc.net/it_talk/970831/newstalk.html, 11 June 1998)

สำหรับแนวทางป้องกันการคัดลอกข้อมูลโดยปราศจากอำนาจ จำเป็นอย่างยิ่งที่ต้องมีการวางมาตรการรักษาความปลอดภัยที่เหมาะสม เช่น ความปลอดภัยทางกายภาพและควบคุมการเข้าถึงคอมพิวเตอร์ เช่น การระบุผู้ใช้ (User Identification : User-ID) รหัสผ่าน (Password) และถ้าเป็นไปได้ควรจะต้องมีการติดตั้งเทคโนโลยีที่ทันสมัย เพื่อที่จะป้องกันการคัดลอกข้อมูลดังตัวอย่างต่อไปนี้

บริษัทคอมพิวเตอร์และอิเล็กทรอนิกส์ 5 บริษัท ได้กล่าวว่าทางกลุ่มบริษัทได้ร่วมมือกันปรับขบวนการเทคโนโลยี เพื่อป้องกันภาพยนตร์และเพลงจากการคัดลอกหรือทำสำเนาที่ผิดกฎหมาย ส่วนที่เกี่ยวกับกลวิธีสำหรับอุตสาหกรรมบันเทิง ก็มีบริษัทอินเทล โซนี่ ฮิตาชิ มัตซูชิตา อิเล็กทริค และโตชิบา ได้ประกาศความร่วมมือกันในมาตรฐานวิทยาการรหัสลับ โดยมีเป้าหมายเพื่อการป้องกันภาพยนตร์ที่มีราคาแพง การเสนอวิทยาการรหัสลับเพื่อเป็นการโปร่งใสสบายใจของบริษัท วิทยาการรหัสลับนี้จะไม่มีผลกระทบในการอุปกรณ์ไฟฟ้าต่างๆ เช่น โทรทัศน์ คอมพิวเตอร์ส่วนบุคคล จานบันทึก และอุปกรณ์สนับสนุนอื่นๆ นายคริส คุ๊กสัน รองประธานบริหารของบริษัทวอร์เนอร์ บราเทอร์ กล่าวว่าการพัฒนาความสามารถของการป้องกันเนื้อหานี้เป็นขั้นที่สำคัญมากในการสื่อสารทางรูปภาพและเสียงที่มีคุณภาพสูงให้กับลูกค้า

(Http://www.fm97.ksc.net/it_talk/970307/newstalk.html, 11 June 1998)

3.3 การแก้ไขเปลี่ยนแปลงข้อมูล

การแก้ไขเปลี่ยนแปลงข้อมูลเป็นการกระทำที่ต้องอาศัยการเข้าถึงข้อมูล โดยผู้กระทำมุ่งกระทำการบางอย่างเกี่ยวกับข้อมูลในคอมพิวเตอร์ เช่น การเพิ่มเติมเข้าไป การตัดทอนข้อมูล หรือการจำกัดข้อมูล ข้อมูลที่ถูกแก้ไขเปลี่ยนแปลงล้วนแล้วแต่เป็นข้อมูลที่มีความสำคัญ หรือเป็นข้อมูลหลัก เช่น การแก้ไขเปลี่ยนแปลงชื่อโดเมน (Domain Name) สาเหตุหนึ่งที่มีการแยกความผิดในลักษณะนี้ออกเป็นความผิดอีกฐานหนึ่ง ก็เพราะเกิดปัญหาความขัดข้องในการที่จะนำบทบัญญัติความผิดฐานปลอมเอกสารมาใช้บังคับ ทำให้หลายบางประเทศต้องบัญญัติความผิดฐานนี้แยกออกมาเป็นความผิดอีกฐานหนึ่งโดยเฉพาะเพื่อขจัดปัญหาในเรื่องนี้ ซึ่งจะได้วิเคราะห์และกล่าวถึงต่อไป

โดยปกติการแก้ไขเปลี่ยนแปลงข้อมูลผู้กระทำจะมีวัตถุประสงค์เพื่อการฉ้อโกง เรียกกันว่าการฉ้อโกงทางคอมพิวเตอร์ (Computer Fraud) เช่น การฉ้อโกงโดยบัตรฝากถอนเงินสดอัตโนมัติ (Automatic Teller Machine : ATM) การฉ้อโกงทางบัตรเครดิต การฉ้อโกงโดยการยักยอกโอนถ่ายเงินทางอิเล็กทรอนิกส์ และจากการสำรวจของหลายๆ สถาบันปรากฏว่าการฉ้อโกงทางคอมพิวเตอร์เป็นการกระทำความผิดที่เกิดขึ้นมากที่สุด ในจำนวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตัวอย่างเช่น สถาบันเทคโนโลยีคอนฟิลส์ (The Conlfield Institute of Technology) ประเทศออสเตรเลีย ได้ทำการสำรวจการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จำนวน 123 ครั้ง พบว่าเป็นการฉ้อโกงทางคอมพิวเตอร์ถึง 60 ครั้ง

สำหรับเหตุผลที่สำคัญของการฉ้อโกงทางคอมพิวเตอร์ โดยผู้กระทำจะทำการแก้ไขเปลี่ยนแปลงข้อมูลก็เพื่อให้ได้ไปซึ่งทรัพย์สินหรือสิ่งอื่น เช่น การที่พนักงานเข้าไปแก้ไขเปลี่ยนแปลงเงินเดือน การเพิ่มยอดเงินฝากธนาคาร การลดยอดหนี้ที่มีอยู่กับสถาบันการเงิน การโอนเงินทางอิเล็กทรอนิกส์ การกระทำการฉ้อโกงทางคอมพิวเตอร์เหล่านี้สามารถกระทำได้ในขั้นตอนต่างๆ ในการทำงานของเครื่องคอมพิวเตอร์

1. ขั้นตอนการนำเข้า (Input) ผู้ที่ทำการฉ้อโกงในขั้นตอนนี้ไม่ต้องอาศัยความรู้ทางด้านคอมพิวเตอร์ เพียงแต่สามารถเข้าถึงข้อมูลที่จะส่งผ่านไปให้คอมพิวเตอร์ประมวลผล ก็กระทำการแก้ไขเปลี่ยนแปลงข้อมูลได้ โดยการเพิ่มข้อมูล การแก้ไขเปลี่ยนแปลงข้อมูล การลบข้อมูล วิธีการจัดทำการปรุงแต่งข้อมูลนี้เป็นวิธีที่ผู้ทุจริตทำกันมากที่สุดวิธีหนึ่ง อันเป็นวิธีการที่วงการ

คอมพิวเตอร์รู้จักกันว่า "เข้าผิดออกผิด" (Garbage in Garbage out) หรือกล่าวอีกนัยหนึ่งก็คือว่า ถ้าเอาขยะใส่เข้าคอมพิวเตอร์ ก็จะได้ขยะนั้นกลับออกมา โดยจัดทำได้หลายประการ เช่น

ก. การเพิ่มรายการที่จะบันทึก

ข. การงดเว้นการบันทึกรายการที่ควรจะบันทึก

ค. การดัดแปลงรายการที่จะบันทึก

ง. การทำการปรับปรุงรายการที่จะบันทึก

จ. การทำการปรับปรุงรายการโดยเจตนาทำผิด

ฉ. การใช้วิธีการแก้ไขข้อผิดพลาดนอกเหนือจากวิธีที่ได้กำหนดไว้ (เกียรติศักดิ์ จีรเธียรนาถ, 2528 : 117 อ้างถึงใน ภานุ รังสีสหัส, 2533 : 98)

วิธีการแก้ไขเปลี่ยนแปลงข้อมูลในขั้นตอนนำข้อมูลเข้า (Data Diddling) คือการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต กระทำก่อนหรือระหว่างที่กำลังบันทึกข้อมูลลงไปในคอมพิวเตอร์ การแก้ไขเปลี่ยนแปลงข้อมูลดังกล่าวนี้สามารถกระทำโดยบุคคลใดก็ได้ที่สามารถเข้าถึงตัวข้อมูล เช่น พนักงานที่มีหน้าที่บันทึกเวลาการทำงานของพนักงานทั้งหมด ทำการแก้ไขเปลี่ยนแปลงตัวเลขชั่วโมงการทำงานของพนักงานคนอื่น มาเป็นชั่วโมงการทำงานของตนเอง ซึ่งข้อมูลดังกล่าวหากถูกแก้ไขเปลี่ยนแปลงเพียงเล็กน้อย พนักงานแต่ละคนจะไม่เกิดความสงสัย (ทวีศักดิ์ กออนันตกูล, 2541 : 4)

ตัวอย่างการกระทำความผิดในขั้นตอนนำข้อมูลเข้า

มีคดีหนึ่งเกิดขึ้นในฮ่องกง คือพนักงานธนาคารแห่งหนึ่งที่ทำงานให้กับรองประธานฝ่ายปฏิบัติการ ถูกดำเนินคดีข้อหายักยอกเงินโดยอาศัยคอมพิวเตอร์ในความรับผิดชอบของตนเพิ่มเงินเดือนให้กับตัวเอง พนักงานที่ถูกกล่าวหามีหน้าที่คำนวณและเตรียมข้อมูลเงินเดือนสำหรับพนักงานของธนาคารทุกคน โดยจะทำการกรอกข้อมูลลงแผ่นจานบันทึกแล้วส่งให้คอมพิวเตอร์ส่วนกลางของธนาคารประมวลผล โดยที่ถูกกล่าวหาได้เพิ่มเงินเดือนให้กับตนเองเกินกว่าความเป็นจริงถึง 409,000 เหรียญฮ่องกง จากการกระทำสำเร็จถึง 27 ครั้ง และใช้เวลาถึง 3 ปี ในที่สุดก็ถูกจับได้เมื่อไปกระทำความผิดอาญาอีกประเภทหนึ่ง

2. ขั้นตอนการเขียนโปรแกรม (Programming) ผู้ที่จะกระทำการฉ้อโกงในขั้นตอนนี้ต้องมีความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์มากพอสมควร และการค้นพบการกระทำผิดเช่นนี้ก็เป็นสิ่งที่ยากอย่างยิ่ง จึงเป็นแรงจูงใจอย่างสูงสำหรับผู้กระทำความผิด เพราะได้ผลตอบแทนสูงและยากต่อการจับกุม โดยผู้กระทำจะอาศัยการเขียนโปรแกรมเพื่อให้เครื่องคอมพิวเตอร์ช่วยทำการแก้ไขเปลี่ยนแปลงข้อมูล ไม่ว่าจะเป็นการเพิ่ม ลด หรือ แก้ไขเปลี่ยนแปลงข้อมูล คอมพิวเตอร์จะทำงานได้จะต้องมีคำสั่งเป็นภาษาเครื่อง (Machine Language) เป็นภาษาที่คอมพิวเตอร์เข้าใจซึ่งแตกต่างกับภาษาอื่นที่มนุษย์สามารถอ่านและเข้าใจได้ การฉ้อโกงในขั้นตอนนี้ต้องเกี่ยวข้องกับโปรแกรม ซึ่งสามารถแบ่งโปรแกรมออกเป็นสามชนิด ดังนี้ ชนิดที่หนึ่งโปรแกรมควบคุมการปฏิบัติงานภายในเครื่องหรือโปรแกรมระบบ (System Program) ผู้ใช้โดยทั่วๆ ไป จะไม่สามารถเข้าไปเกี่ยวข้องกับโปรแกรมชนิดนี้ได้ แต่ถ้าบุคคลใดทราบรหัสการเข้าถึงแฟ้มข้อมูลและมีความรู้เกี่ยวกับการปฏิบัติงานของเครื่อง ก็สามารถแก้ไขเปลี่ยนแปลงเนื้อข้อมูลในแฟ้มข้อมูลได้โดยตรง โปรแกรมชนิดที่สองคือโปรแกรมอรรถประโยชน์ (Utility Program) โดยมากจะเป็นคำสั่งสำเร็จรูปเพื่อประโยชน์สำหรับการใช้งาน เช่น การคัดลอกข้อมูล ผู้กระทำการทุจริตจะทำการแก้ไขคำสั่ง เช่น ไม่ให้คัดลอกข้อมูลบางประเภทที่ไม่ต้องการให้ผู้อื่นทราบ โปรแกรมชนิดที่สามคือโปรแกรมประยุกต์ (Application Program) เป็นการเขียนโปรแกรมขึ้นมาใช้งานเฉพาะกิจ โดยมากผู้กระทำการทุจริตจะเป็นผู้เขียนโปรแกรมนั้น โดยมีรูปแบบการกระทำแตกต่างกันหลายรูปแบบ เช่น

การฉ้อโกงแบบม้าโทรจัน (Trojan Horse) การกระทำในรูปแบบนี้จะเป็นการเพิ่มขยายหรือเปลี่ยนแปลงโปรแกรมการทำงานเพื่อประโยชน์ในการฉ้อโกง โดยส่วนที่เพิ่มขยายหรือเปลี่ยนแปลงนั้นมีจุดประสงค์เพื่อการฉ้อโกง เช่น การเพิ่มเงินในบัญชีของตน การเพิ่มข้อมูลที่น่าเชื่อถือ การลดยอดหนี้ของตน การลบข้อมูลที่ทำให้ขาดความเชื่อถือ และส่วนที่สำคัญคือเมื่อโปรแกรมในส่วนที่เพิ่มขยายหรือเปลี่ยนแปลงทำงานครบถ้วนตามวัตถุประสงค์ที่วางไว้แล้ว ก็จะมีคำสั่งให้ลบโปรแกรมส่วนที่เพิ่มขยายหรือเปลี่ยนแปลงนั้นทิ้งไปทันที ซึ่งจะทำให้การตรวจสอบและค้นหาพยานหลักฐานในการกระทำความผิดกระทำได้ยากลำบาก (วีระพงษ์ บุญโญภาส, 2540 : 165)

การฉ้อโกงแบบโลจิกบอมบ์ (Logic Bomb) การกระทำในรูปแบบนี้จะเป็นการเพิ่มเติมหรือเปลี่ยนแปลงโปรแกรมการทำงานคล้ายกับแบบม้าโทรจัน โดยมีจุดประสงค์เพื่อการฉ้อโกงเหมือนกัน แต่แตกต่างกันตรงที่โปรแกรมแบบโลจิกบอมบ์นี้จะถูกทำลายไปในเวลาที่กำหนดไว้ บางกรณีใช้ก่อวินาศกรรมทำลายระบบคอมพิวเตอร์ทั้งระบบ ซึ่งก็จะทำให้การตรวจสอบและค้น

หาพยานหลักฐานในการกระทำความผิดกระทำได้ยากลำบากเช่นกัน (วีระพงษ์ บุญโญภาส, 2540 : 165)

การฉ้อโกงแบบประตูกับดัก (Trap Doors) เป็นวิธีการเขียนโปรแกรมที่มีการเลียนแบบให้หน้าจอการทำงานคล้ายกับหน้าจอการทำงานปกติของระบบคอมพิวเตอร์ เพื่อลวงผู้ที่มีอำนาจในการใช้คอมพิวเตอร์ใส่การระบุผู้ใช้ (User Identification : User-ID) หรือรหัสผ่าน (Password) โดยโปรแกรมนี้จะเก็บข้อมูลที่ต้องการไว้ในแฟ้มข้อมูลลับ (ทวีศักดิ์ กออนันตกูล, 2541 : 5)

การฉ้อโกงแบบซาลามิ (Salami) การกระทำในรูปแบบนี้จะเป็นการกระทำของผู้เขียนโปรแกรมโดยตรง เพราะเป็นการอาศัยคำสั่งของโปรแกรมเพื่อที่จะฉ้อโกงเศษเงินจำนวนเล็กน้อยจากหลายๆ บัญชี ซึ่งถ้าเจ้าของบัญชีหรือผู้ตรวจสอบไม่ได้ใช้ความละเอียดถี่ถ้วนอย่างมากจะสังเกตไม่เห็นสิ่งผิดปกติใดๆ การฉ้อโกงในลักษณะนี้ผู้ที่กระทำการฉ้อโกงจะทำการปัดเศษลง (Round Down Fraud) สำหรับการคำนวณจำนวนเงินต่างๆ เช่น ดอกเบี้ยเงินฝากธนาคาร โดยแทนที่จำนวนเงินที่เครื่องคอมพิวเตอร์บันทึกไว้มีเศษทศนิยมเท่ากับหรือเกินกว่า 0.005 สตางค์ คือ 5 ส่วนใน 10 ส่วนของหนึ่งสตางค์ จะปัดขึ้นอีกหนึ่งสตางค์ (Round Up) และเศษที่ต่ำกว่า 5 ส่วนใน 10 ส่วนของหนึ่งสตางค์ จะปัดเศษลง (Round Down) แต่ผู้กระทำการฉ้อโกงจะสั่งให้โปรแกรมในเครื่องคอมพิวเตอร์ปัดเศษลงเสมอ และเศษที่ถูกปัดออกนั้นจะนำไปเข้าบัญชีอื่นที่ผู้เขียนโปรแกรมสร้างไว้ และจะถูกถอนเงินนั้นออกไปในภายหลัง จะเห็นได้ว่าแม้การกระทำดังกล่าวจะได้เศษสตางค์จากแต่ละบัญชีเป็นจำนวนเงินน้อยมาก แต่ถ้ากระทำกับจำนวนบัญชีที่มากก็จะได้จำนวนเงินมากขึ้นเช่นกัน ส่วนในกรณีที่เจ้าของบัญชีหรือลูกค้าที่เป็นหนี้ก็จะกระทำในลักษณะตรงกันข้ามคือปัดเศษขึ้นเสมอ ส่วนที่ปัดขึ้นก็นำเข้าบัญชีที่จัดเตรียมไว้ (วีระพงษ์ บุญโญภาส, 2540 : 165)

การฉ้อโกงแบบซุปเปอร์แซปปิ้ง (Superzapping) โดยมีที่มาจากคำว่าซุปเปอร์แซป (Superzap) ซึ่งเป็นโปรแกรมอรรถประโยชน์แมโคร (Macro Utility Program) ที่ใช้ในศูนย์คอมพิวเตอร์ของบริษัทไอบีเอ็ม (IBM) เพื่อใช้เป็นเครื่องมือของระบบ (System Tool) ทำให้สามารถเข้าไปในระบบคอมพิวเตอร์ได้ในกรณีฉุกเฉิน เสมือนเป็นกุญแจหลัก (Master Key) ที่จะนำมาใช้เมื่อกุญแจดอกอื่นหายหรือมีปัญหา ผู้กระทำการฉ้อโกงจะอาศัยช่องว่างในโปรแกรม ซึ่งโดยมากแล้วผู้กระทำความผิดจะไม่ใช่ผู้เขียนโปรแกรมนั้น แต่จะเป็นผู้ดูแลรับผิดชอบหรือผู้ใช้

โปรแกรมโดยมีความรู้เกี่ยวกับโปรแกรมบ้างและอาศัยช่องว่างดังกล่าวกระทำความผิด ในบางกรณีอาจจะพบช่องว่างดังกล่าวในโปรแกรมสำเร็จรูป (Package) โปรแกรมอรรถประโยชน์ (Utility Program) เช่น โปรแกรมซุปเปอร์แซป (Superzap) และสิ่งที่น่าเป็นห่วงที่สุดคือโปรแกรมในลักษณะนี้จะมีความเสี่ยงมากหากตกไปอยู่ในมือของผู้ที่ไม่หวังดี (ทวีศักดิ์ กออนันตกูล, 2541 : 5)

3. ขั้นตอนการประมวลผล (Processing) ด้วยระบบการทำงานของคอมพิวเตอร์สามารถทำงานได้อย่างต่อเนื่องและหลายๆ งานในเวลาเดียวกัน การฉ้อโกงในขั้นตอนนี้เป็นการฉ้อโกงขณะที่คอมพิวเตอร์กำลังทำงานอยู่ ผู้กระทำต้องมีความรู้ความชำนาญเกี่ยวกับการทำงานของคอมพิวเตอร์พอสมควร เพราะขณะที่การกระทำความผิดเกิดขึ้นผู้ใช้คอมพิวเตอร์ถ้าไม่มีความชำนาญหรือละเอียดรอบคอบจะไม่ทราบว่ามีการแก้ไขเปลี่ยนแปลงกระบวนการทำงาน เพราะว่าผู้ใช้งานจะเห็นผลสำเร็จของงานก็ต่อเมื่อคอมพิวเตอร์ทำงานเสร็จเรียบร้อยแล้ว และการตรวจสอบหรือพบการกระทำความผิดในลักษณะนี้ก็เป็นสิ่งที่นับว่ายากเช่นกัน โดยมีการกระทำหลายวิธี เช่น

วิธีการทำร้ายแบบไม่ประสานเวลา (Asynchronous attack) เนื่องจากการทำงานของระบบคอมพิวเตอร์เป็นการทำงานแบบไม่ประสานเวลา (Asynchronous) หรือเรียกอีกอย่างว่าระบบหลายตัวประมวล (Multiprocessing System) คือสามารถทำงานหลายๆ อย่างพร้อมกัน โดยการประมวลผลข้อมูลเหล่านั้นจะเสร็จไม่พร้อมกัน ผู้ใช้งานจะทราบว่างานที่ประมวลผลเสร็จหรือไม่ก็ต่อเมื่อเรียกงานนั้นมาดู ระบบดังกล่าวก่อให้เกิดจุดอ่อน ผู้กระทำความผิดจะฉวยโอกาสในระหว่างที่คอมพิวเตอร์กำลังทำงานเข้าไปแก้ไขเปลี่ยนแปลงหรือกระทำการอื่นใด โดยผู้ที่ใช้ไม่ทราบว่ามีการกระทำความผิดเกิดขึ้น (ทวีศักดิ์ กออนันตกูล, 2541 : 6)

วิธีการทำให้ข้อมูลรั่วไหล (Data Leakage) หมายถึงการกระทำให้ข้อมูลรั่วไหลออกไปจากระบบ ซึ่งอาจจะเป็นการกระทำโดยความตั้งใจหรือไม่ก็ตาม เช่น ขณะที่เครื่องคอมพิวเตอร์กำลังแผ่รังสีของคลื่นแม่เหล็กไฟฟ้าอยู่ ผู้กระทำความผิดอาจตั้งเครื่องดักสัญญาณไว้ใกล้กับเครื่องคอมพิวเตอร์เพื่อรับข้อมูลตามที่ตนเองต้องการ (ทวีศักดิ์ กออนันตกูล, 2541 : 6)

4. ขั้นตอนการนำออก (Output) โดยปกติคอมพิวเตอร์จะทำหน้าที่บันทึกข้อมูลออก แต่มีบางกรณีที่จะต้องอาศัยบุคคลเข้ามาช่วยในขั้นตอนนี้ ผู้กระทำการแก้ไขเปลี่ยนแปลงข้อมูลจะมีวัตถุประสงค์เพื่อที่จะบิดเบือนข้อมูล โดยกระทำการเปลี่ยนแปลงข้อมูลภายหลังจากการประมวลผลแล้ว คล้ายกับการฉ้อโกงในขั้นตอนนำข้อมูลเข้า โดยทั่วไปแล้วการฉ้อโกงในขั้นตอนนี้เพียงขั้นตอนเดียวจะมีน้อยมาก ส่วนมากจะกระทำตั้งแต่การนำข้อมูลเข้าเพื่อให้การแสดงผลในขั้นตอนนำข้อมูลออกเป็นไปตามเป้าหมายที่ต้องการ โดยมีวิธีการดังนี้ เช่น

วิธีการที่ได้ข้อมูลที่ทิ้งไว้ในระบบคอมพิวเตอร์ หรือบริเวณใกล้เคียงหลังจากเสร็จการใช้งานแล้ว โดยวิธีการที่ง่ายที่สุดคือการค้นหาตามถังขยะ (Scavenging) ที่อาจมีข้อมูลสำคัญไม่ว่าจะเป็นเบอร์โทรศัพท์หรือรหัสผ่านที่หลงเหลืออยู่ หรืออาจใช้เทคโนโลยีที่สลับซับซ้อนทำการหาข้อมูลที่อยู่ในคอมพิวเตอร์เมื่อผู้ใช้เลิกใช้งานแล้ว ยังมีอีกวิธีหนึ่งที่เรียกว่าการจำลองและการจำลองแบบเชิงแนวคิด (Simulation and Modeling) โดยปัจจุบันคอมพิวเตอร์ถูกใช้เป็นเครื่องมือในการวางแผน การควบคุมและติดตามความเคลื่อนไหวในการประกอบอาชญากรรม และกระบวนการดังกล่าวก็สามารถใช้โดยอาชญากร เพื่อสร้างแบบจำลองในการวางแผนเพื่อประกอบอาชญากรรมได้เช่นกัน เช่น การฉ้อโกงกิจการประกันภัย มีการสร้างแบบจำลองในการปฏิบัติการหรือช่วยในการตัดสินใจในการทำกรมธรรม์ประกันภัย โปรแกรมสามารถทำกรมธรรม์ประกันภัยปลอมขึ้นมาเป็นจำนวนมาก ส่งผลให้บริษัทประกันภัยล้มละลายเมื่อถูกเรียกร้องให้ต้องจ่ายเงินให้กับกรมธรรม์ที่ขาดต่ออายุ หรือกรมธรรม์ที่มีการจ่ายเงินเพียงการบันทึกจำลอง แต่ไม่ได้รับเบี้ยประกันจริง หรือต้องจ่ายเงินให้กับกรมธรรม์ที่เชื่อว่ายังไม่ขาดอายุความ
(ทวีศักดิ์ กออนันตกูล, 2541 : 7)

5. ขั้นตอนการสื่อสารข้อมูล (Data Communications) โดยทั่วไปแล้วคอมพิวเตอร์จะสื่อสารกันทางสายสื่อสารข้อมูล โดยเฉพาะระบบอินเตอร์เน็ต (Internet) ซึ่งเป็นเครือข่ายสื่อสารทั่วโลก โดยผู้กระทำความผิดจะใช้ช่องทางการสื่อสารในการเข้าถึงข้อมูลเพื่อกระทำการใดๆ ตามความต้องการของตน มีวิธีการดังนี้ เช่น

วิธีการขึ้นหลัง (Piggybacking) วิธีการดังกล่าวสามารถทำได้ทั้งทางกายภาพ (Physical) เช่น ผู้กระทำความผิดจะลักลอบเข้าไปในประตูที่มีระบบรักษาความปลอดภัย ผู้นั้นจะรอให้บุคคลที่มีอำนาจหรือได้รับอนุญาตมาใช้ประตูดังกล่าว เมื่อประตูเปิดและบุคคลที่มีอำนาจนั้นได้เข้าไปแล้ว ผู้กระทำความผิดก็จะฉวยโอกาสตอนที่ประตูยังปิดไม่สนิทแอบเข้าไปได้ ในทางอิเล็กทรอนิกส์อันเป็นการกระทำที่ไม่สามารถเห็นได้ด้วยทางกายภาพ อาจเกิดขึ้นในกรณีที่ใช้สายสื่อสารเดียวกันกับผู้ที่มีอำนาจใช้หรือได้รับอนุญาต เช่น ใช้สายเคเบิลหรือโมเด็มเดียวกัน อีกวิธีหนึ่งคือ วิธีการลอบต่อสาย (Wiretapping) เป็นการลักลอบดักฟังสัญญาณการสื่อสารโดยเจตนาที่จะได้รับประโยชน์จากการเข้าถึงข้อมูลผ่านเครือข่ายการสื่อสาร หรือที่เรียกว่าโครงสร้างพื้นฐานสารสนเทศ โดยการกระทำความผิดดังกล่าวกำลังเป็นที่หวาดวิตกกับผู้ที่เกี่ยวข้องเป็นอย่างมาก
(ทวีศักดิ์ กออนันตกูล, 2541 : 7)

จากที่กล่าวมาข้างต้น ไม่ว่าจะเป็นการแก้ไขเปลี่ยนแปลงข้อมูลในขั้นตอนใดก็ตาม ผู้กระทำมีวัตถุประสงค์เพื่อที่จะกระทำความผิดทั้งสิ้นโดยมากจะเป็นความผิดฐานฉ้อโกง ลักทรัพย์ ยักยอกทรัพย์ และปลอมแปลงข้อมูล

ตัวอย่างการกระทำการฉ้อโกงโดยทางบัตรเครดิต

อดีตนักศึกษาในฟลอริด้าได้ถูกฟ้องร้อง เนื่องจากการพยายามที่จะฉ้อโกงบัตรเครดิตบนเครือข่ายอินเตอร์เน็ต นายไนม์ ฮามุส (Naim Hamud) ถูกฟ้องร้องเกี่ยวกับการฉ้อโกงบัตรเครดิต ในศาลสหรัฐอเมริกา สำนักงานทนายความสหรัฐอเมริกาในมลรัฐฟลอริดาใต้ (Southern Florida) ได้กล่าวว่านายฮามุสถูกปล่อยไปด้วยเงินประกัน 25,000 เหรียญสหรัฐอเมริกา นายฮามุสเป็นผู้ต้องสงสัยในการใช้บัตรเครดิตผ่านเครือข่ายอินเตอร์เน็ต โดยใช้ชื่อของนักศึกษามหาวิทยาลัยแห่งหนึ่ง ที่เขาได้คัดลอกข้อมูลออกมาจากระบบคอมพิวเตอร์ของมหาวิทยาลัยอันเป็นสถานที่ที่เขาศึกษาอยู่ เจ้าหน้าที่ควบคุมกฎหมายได้ทำการเตือนภัยให้ระวัง เมื่อสถาบันการเงินและธนาคารหลายๆ แห่งร้องเรียนไปยังกล่องไปรษณีย์ว่ามีการฉ้อโกงทางบัตรเครดิตจำนวนมาก นายฮามุสได้ลาออกจากมหาวิทยาลัยก่อนที่จะถูกจับ และถ้าผลการตัดสินออกมาว่าเขาได้กระทำความผิด จะต้องถูกจำคุกมากกว่า 5 ปีขึ้นไป และปรับไม่เกิน 250,000 เหรียญสหรัฐอเมริกา อันเป็นโทษของการฉ้อโกงทางบัตรเครดิต

(Http://www.fm97.ksc.net/it_talk/970914/newstalk.html, 11 June 1998)

อีกตัวอย่างหนึ่ง เกิดขึ้นที่ประเทศฮ่องกง ได้มีชายคนหนึ่งอายุ 24 ปี ถูกจับกุมในข้อหากระทำการโกงการสั่งจองตั๋วเครื่องบินโดยผ่านทางเครือข่ายอินเตอร์เน็ต ซึ่งเดิมเขาเป็นนักศึกษา โดยกล่าวว่าเขาได้รับรายละเอียดของบัตรเครดิตมาจำนวนหนึ่งจากใบกำกับสินค้าต่างๆ ที่ถูกส่งไปยังเจ้าหน้าที่และนักศึกษาหลายๆ คนในตู้รับจดหมายธรรมดาๆ ใบหนึ่งของมหาวิทยาลัย เมื่อเขาพบเห็นเช่นนี้ก็เลยทำการใช้หมายเลขบัตรเหล่านั้นทันที ด้วยการสั่งซื้อตั๋วเครื่องบินจากตัวแทนจำหน่าย (Travel Agents) ต่างๆ บนเครือข่ายอินเตอร์เน็ต และก็ขอให้ทางบริษัทที่รับสั่งจองส่งมาทางตู้ไปรษณีย์ใบเดิม หลังจากนั้นประมาณ 1 สัปดาห์ เขาก็ถูกจับกุมตัวโดยมีหลักฐานคือตั๋วเครื่องบินจำนวน 12 ใบ มูลค่า 12,000 เหรียญสหรัฐอเมริกา และหมายเลขบัตรเครดิตพร้อมทั้งรายละเอียดต่างๆ ของบุคคลอื่น

(Http://www.fm97.ksc.net/it_talk/971122/newstalk.html, 11 June 1998)

ตัวอย่างการกระทำการฉ้อโกงโดยการโอนเงินทางอิเล็กทรอนิกส์

ที่กรุงนิวยอร์ก ศาลได้ทำการฟ้องชาวรัสเซียพร้อมกับพรรคพวกซึ่งได้กระทำความผิดในข้อหาลักลอบเข้าไปในระบบคอมพิวเตอร์ภายในของธนาคารซิตี้แบ็งค์ และได้ทำการโอนเงินที่ครอบคลุมบัญชีของลูกค้าทั้งหมด 5 ประเทศ ได้แก่ ประเทศฟินแลนด์ เนเธอร์แลนด์ เยอรมนี อิสราเอล และสหรัฐอเมริกา เป็นจำนวนเงิน 10,000,000 เหรียญสหรัฐอเมริกา (สิบล้านเหรียญสหรัฐอเมริกา) ไปยังบัญชีของตนเองและพรรคพวก นายวลาดิเมอร์ ลีโอนีโดวิช เลวิน ชายวัย 30 ปี ได้รับการตัดสินลงโทษจำคุก 5 ปี และปรับอีก 250,000 เหรียญสหรัฐอเมริกา โดยรายละเอียดมีอยู่ว่าเมื่อเดือนมิถุนายน - เดือนสิงหาคม ค.ศ. 1994 นายเลวินได้ลักลอบเข้าไปทำการโอนเงินในเครือข่ายดังกล่าว โดยใช้รหัสประจำตัวต่างๆ รวมถึงรหัสผ่านที่เป็นของลูกค้าธนาคาร (Http://www.fm97.ksc.net/it_talk/980207/newstalk.html, 11 June 1998)

ตัวอย่างการกระทำการฉ้อโกงโดยการจำหน่ายหุ้นปลอม

ที่นครซานฟรานซิสโก ได้มีชาวแคลิฟอร์เนียคนหนึ่งถูกจับกุมในข้อหากระทำการฉ้อโกงเงินผู้ลงทุนประมาณ 150 คน เป็นเงิน 190,000 เหรียญสหรัฐอเมริกา โดยมีวิธีการที่จะจำหน่ายหุ้นในบริษัทของเขาผ่านเครือข่ายอินเตอร์เน็ต คณะกรรมาธิการควบคุมการค้าหุ้นของสหรัฐอเมริกาได้ฟ้องร้องนายแมททิว โบวิน (Matthew Bowin) อายุ 34 ปี ในข้อหาละเมิดกฎหมายควบคุมความปลอดภัยของสหรัฐอเมริกา นายโบวินได้ลงโฆษณาเกี่ยวกับรายละเอียดธุรกิจของเขาผ่านเครือข่ายอินเตอร์เน็ต ต่อมาเขาก็รับเงินจากผู้ร่วมลงทุนกับเขา โดยมีผู้ร่วมลงทุนทั้งภายในและภายนอกประเทศ ในจำนวนนี้รวมถึงผู้ลงทุนชาวฮ่องกงด้วย นายโบวินได้สัญญากับผู้ลงทุนว่าเขาเป็นคนถือเงินของผู้ลงทุนไว้ตามหนังสือสัญญา จนกระทั่งได้เงินเพิ่มขึ้นถึง 500,000 เหรียญ เมื่อถึงจุดนี้เขาจะออกหนังสือรับรองของหุ้น (Stock Certificates) ให้แก่ผู้ร่วมลงทุน แต่ความเป็นจริงเมื่อเขาได้รับเงินมาเขากลับนำเงินทั้งหมดไปใช้ส่วนตัว จากการตรวจสอบยังพบอีกว่านายโบวินได้มีรูปแบบการฉ้อโกงต่างๆ ถึง 65 แบบ รวมทั้งการลักขโมยและการจำหน่ายหุ้นปลอมด้วย (Http://www.fm97.ksc.net/it_talk/980418/newstalk.html, 11 June 1998)

3.4 การลบและการทำลายข้อมูล

การลบข้อมูลและการทำลายข้อมูลอันนำมาซึ่งความเสียหายนั้น บางกรณีอาจจะรวมถึงการแก้ไขเปลี่ยนแปลงข้อมูลเพื่อที่จะทำลายข้อมูลที่มีอยู่ การลบและการทำลายข้อมูลนี้จะต้องอาศัยการเข้าถึงทางคอมพิวเตอร์ โดยความเสียหายที่เกิดขึ้นเจ้าของข้อมูลไม่สามารถที่จะรู้เห็นได้

ด้วยทางกายภาพ จึงจำเป็นอย่างยิ่งที่ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลไว้ระดับหนึ่ง ซึ่งไม่สามารถที่จะครอบคลุมการป้องกันไว้ได้ทั้งหมด ก็เพราะสาเหตุและวิธีการของผู้ไม่หวังดีที่ต้องการจะลบหรือทำลายข้อมูลนั้นมีมากมายหลายสาเหตุ บางกรณีเกิดจากความโกรธแค้นของพนักงานในหน่วยงาน บางกรณีเกิดจากเหตุผลทางการเมืองหรือเหตุผลทางธุรกิจ และสาเหตุที่พบมากที่สุดก็คือการฉ้อโกงต่างๆ ซึ่งต้องมีการลบหรือทำลายข้อมูลอันเป็นส่วนหนึ่งของการฉ้อโกง ส่วนวิธีการก็มีหลากหลายรูปแบบ เริ่มตั้งแต่การทำให้เครื่องคอมพิวเตอร์หยุดทำงานหรือระบบขัดข้อง (Crash System) การเข้าถึงโดยปราศจากอำนาจเพื่อเข้าไปลบข้อมูลหรือทำลายข้อมูล เช่น ข้อมูลที่ตนเป็นลูกหนี้ การใส่โปรแกรมบางชนิดซึ่งมีความสามารถที่จะลบข้อมูลจำนวนมากในระยะเวลาอันสั้น โดยโปรแกรมบางชนิดสามารถตั้งเวลาหรือเงื่อนไข ให้ทำลายข้อมูลภายหลังจากที่ผู้กระทำได้ออกจากระบบคอมพิวเตอร์นั้นไปแล้ว

บางกรณีการลบและการทำลายข้อมูล จะมีการกระทำที่ทำให้เกิดความเสียหายอื่นๆ ทางคอมพิวเตอร์รวมอยู่ด้วย เช่น ตัวเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ เครือข่ายคอมพิวเตอร์ ซึ่งอาจถือได้ว่าเป็นการทำให้เสียหายทางกายภาพอีกประการหนึ่ง อันเป็นรูปแบบของการกระทำความผิดทางคอมพิวเตอร์ ที่สามารถจะอธิบายลักษณะว่าเป็นการกระทำความผิดทางอาญา คือเป็นการทำให้เสียทรัพย์ โดยเป็นการกระทำต่อทรัพย์ทางคอมพิวเตอร์ แต่ละประเทศก็จะมีกฎหมายเกี่ยวกับความผิดฐานทำให้เสียทรัพย์แบบใดแบบหนึ่งไว้บังคับใช้ อันเป็นกฎหมายที่ห้ามการทำให้เสียหายทางกายภาพแก่ทรัพย์สินส่วนบุคคลของผู้อื่น บางประเทศยังมีกฎหมายเกี่ยวกับ "การรบกวนการใช้ประโยชน์" ซึ่งเป็นกฎหมายที่บัญญัติให้การเข้าไปยุ่งกับทรัพย์สินของบุคคลอื่นจนเกิดความเสียหายแก่บุคคลนั้น เป็นการกระทำความผิดทางอาญาอีกด้วย
(ภานุ รังสีสหัส, 2533 : 127)

การลบและการทำลายข้อมูลนั้นมีคดีที่ได้รับการบันทึกไว้ในสมัยแรกๆ ของทางการประเทศอังกฤษ คือคดี ค็อคซ กับ ไรลย์ (Cox vs. Riley) ไรลย์ถูกกล่าวหาว่าเป็นลูกจ้างที่ใช้เครื่องเลื่อยอัตโนมัติ ซึ่งเป็นเครื่องเลื่อยที่ยังคงมีลักษณะที่เป็นอุปกรณ์แบบธรรมดาทั่วไป เพียงแต่มีระบบควบคุมงานของแผ่นวงจรที่ใช้ในการพิมพ์ของคอมพิวเตอร์ในแบบยุคต้นๆ มีโปรแกรมที่ควบคุมการทำงานของเลื่อยอัตโนมัติและมีระบบช่วยการจัดการลบโปรแกรม การลบโปรแกรมนี้จะทำให้แผ่นวงจร สามารถทำการตั้งโปรแกรมชุดใหม่ขึ้นมาได้เหมือนกับการลบเนื้อเพลงในเทปเพลงโดยการทำการบันทึกเพลงใหม่เข้าไปแทน

ในตอนแรกผู้ถูกกล่าวหาถูกระบุว่าเป็นผู้กระทำความผิดในฐานทำลายข้อมูล จนกระทั่งศาลได้วินิจฉัยประเด็นข้อสงสัยที่ว่าได้มีการเกิดการทำลายทรัพย์สินขึ้นหรือไม่ เพราะจำเลยได้ชี้ประเด็นว่าไม่มีการก่อให้เกิดความเสียหายให้กับเครื่องเลื่อยแต่ประการใด แม้ว่าแผ่นวงจรที่ใช้ในการพิมพ์ได้ถูกทำลายลงแต่ตัวสื่อที่ใช้ในการเก็บก็ยังคงอยู่ในสภาพปกติ ซึ่งศาลได้วินิจฉัยให้เห็นว่าได้เกิดความเสียหายต่อเจ้าของเลื่อยแล้ว โดยเจ้าของเลื่อยต้องใช้เวลาและแรงงานที่จะต้องดำเนินการแก้ไขให้อยู่ในสภาพปกติ ซึ่งสามารถนำมาเปรียบเทียบได้กับกรณีที่มีผู้กระทำความผิดทำการพ่นสีใส่กำแพง ซึ่งกำแพงก็ยังคงสภาพที่แข็งแรงอยู่แต่ค่าใช้จ่ายที่เกิดขึ้นจากการดำเนินการให้อยู่ในสภาพปกตินั้น เป็นสิ่งแสดงถึงความเสียหายที่เกิดขึ้น

อีกคดีหนึ่งที่ถือได้ว่าเป็นคดีต้นแบบของการจารกรรมทางคอมพิวเตอร์ ในประเทศอังกฤษได้มีการสร้างเครือข่ายคอมพิวเตอร์ร่วมกันเครือข่ายหนึ่งมีชื่อว่าจาเน็ต (Joint Academic Network : JANET) เพื่อให้ผู้ใช้งานที่สามารถต่อเชื่อมเข้ากับระบบงาน ณ สถานที่ใดสถานที่หนึ่งของเครือข่ายนี้ได้ โดยสามารถเข้าไปใช้งานของเครือข่ายของสถาบันอื่น ทั้งนี้ ผู้ใช้งานจะต้องได้รับรหัสผ่าน (Password) อย่างไรก็ตามรหัสผ่านที่กำหนดขึ้นนั้นเป็นการกำหนดแบบง่ายๆ เพราะเป็นการใช้งานเพื่อการศึกษา ชายผู้หนึ่งได้ทำการผ่านเข้าไปในเครือข่ายโดยไม่ได้รับอนุญาต การกระทำดังกล่าวของเขาได้ถูกตั้งข้อหาใน 2 ประเด็น

1. ได้ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ เพราะได้ทำให้ระบบคอมพิวเตอร์ขัดข้องและหยุดการให้บริการชั่วขณะ

2. ได้ก่อให้เกิดความเสียหายต่ออุปกรณ์แผ่นจานบันทึก ซึ่งเป็นสิ่งที่จัดเก็บโปรแกรมและข้อมูลของระบบคอมพิวเตอร์อันได้รวบรวมข้อมูลไว้ทั้งหมด เสมือนตัวบันทึกข้อมูลหรือบนแผ่นกระดาษที่ใช้ในการบันทึก

อย่างไรก็ตาม ข้อกล่าวหาที่ว่าได้ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ได้ตกไปโดยคณะลูกขุน แต่ศาลได้ตัดสินลงโทษในส่วนของข้อกล่าวหาที่ 2 ถึงแม้ว่าทนายของจำเลยได้โต้แย้งว่าการทำลายความเสียหายนั้นต้องเป็นการทำความเสียหายกับสิ่งที่จับต้องได้ ศาลอุทธรณ์ได้ให้ความเห็นไว้ว่ากฎหมายได้บัญญัติไว้ว่าทรัพย์สินที่มีตัวตนได้ถูกทำให้เกิดความเสียหาย ไม่ใช่ความเสียหายต้องเป็นสิ่งที่จับต้องได้ การตัดสินของคดีนี้เป็นเครื่องยืนยันแนวทางการพิจารณาของศาลว่าการกระทำใดๆ ที่ก่อให้เกิดการแก้ไขในข้อมูลที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์ถือได้ว่าเป็นการประกอบอาชญากรรมขึ้นแล้ว

(Http://www.strath.ac.uk/Departments/Law/digib/book/criminal, 14 August 1998)

นอกจากกรณีที่กล่าวแล้ว ยังมีตัวอย่างการลบและการทำลายข้อมูลอีกหลายตัวอย่าง เช่น

ที่กรุงวอชิงตันเจ้าหน้าที่อาวุโสท่านหนึ่งของสหรัฐอเมริกา เปิดเผยว่าระบบคอมพิวเตอร์ต่างๆ ของกระทรวงกลาโหมเกิดความเสียหายมากกว่า 250 เครื่อง และอาจจะเพิ่มจำนวนความเสียหายมากขึ้นอีก นายเคนเน็ท มินิฮาน (Kenneth Minihan) ผู้อำนวยการศูนย์การป้องกันภัยแห่งชาติกล่าวว่าพวกตนทราบดีถึงข้อบกพร่องต่างๆ ในระบบการสื่อสารทางคอมพิวเตอร์และเครือข่ายที่กำลังถูกรบกวนจากพวกมนุษย์ผู้ที่ไม่หวังดี ซึ่งนับว่าเป็นตัวการสำคัญของความเสียหายในครั้งนี้ การรบกวนนั้นจะเป็นเรื่องที่เกี่ยวกับเครือข่ายที่เรียกว่า "สนิฟเฟอร์" (Sniffers) หรือโปรแกรมที่ใช้ดักฟังการสื่อสารและการขนส่งต่างๆ รวมทั้งยังมีซอฟต์แวร์และเครื่องมือการจารกรรมข้อมูลที่สลับซับซ้อนอื่นๆ ด้วย และเขายังได้กล่าวอีกว่าประเทศสหรัฐอเมริกาเป็นประเทศที่ใช้เครือข่ายคอมพิวเตอร์มากกว่าประเทศอื่น โดยถือเป็นแหล่งข้อมูลที่สำคัญบนเครือข่ายอินเตอร์เน็ต (Http://www.fm97.ksc.net/it_talk/971115/newstalk.html, 11 June 1998)

อีกตัวอย่างหนึ่งเกิดขึ้นที่เมืองโตรอนโต ประเทศแคนาดา ตำรวจของประเทศได้จับกุมชายผู้ต้องสงสัยชาวแคนาดา วัย 22 ปี ที่ตำรวจสงสัยว่าเขาจะเป็นคนที่บุกรุกเข้าไปในระบบคอมพิวเตอร์ขององค์การนาซ่า (National Aeronautic and Space Administration : NASA) อันเป็นเหตุให้เกิดความเสียหายหลายพันเหรียญสหรัฐอเมริกา ตำรวจของเมืองออนตาริโอ ประเทศแคนาดา ได้ฟ้องร้องนายเจสัน (Jason) ผู้ถูกกล่าวหารายนี้ในเวลาต่อมา ด้วยข้อหาที่มีจุดประสงค์ร้ายในการเข้าไปในระบบคอมพิวเตอร์ขององค์การนาซ่าอย่างผิดกฎหมาย โดยเขามีความตั้งใจที่จะสร้างความวุ่นวาย ด้วยการเข้าไปบุกรุกข้อมูลของระบบคอมพิวเตอร์ดังกล่าวอย่างผิดกฎหมาย ตำรวจกล่าวว่าสำหรับมูลค่าของความเสียหายนั้นดีเป็นมูลค่าทางการเงินออกมาได้ถึง 70,000 เหรียญสหรัฐอเมริกา (ถ้าเทียบเป็นเงินไทยที่ 38 บาทต่อ 1 เหรียญสหรัฐอเมริกา ก็ประมาณ 2,660,000 บาท) ซึ่งจากเหตุการณ์ครั้งนี้เป็นเหตุให้เจ้าหน้าที่ของระบบคอมพิวเตอร์นี้ถูกบังคับให้ต้องมีการปรับปรุง และเปลี่ยนแปลงระบบคอมพิวเตอร์กันเป็นการใหญ่โดยเฉพาะตรงจุดที่เกี่ยวกับระบบความปลอดภัยต่างๆ (Http://www.fm97.ksc.net/it_talk/980418/newstalk.html, 11 June 1998)

ในส่วนการลบและการทำลายข้อมูลที่ได้กล่าวมาทั้งหมดนี้ เป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายโดยที่ผู้เสียหายไม่สามารถรู้เห็นได้ด้วยทางกายภาพ นอกจากความผิดดังกล่าวแล้วผู้กระทำยังต้องรับผิดฐานทำให้เสียทรัพย์อีกหรือไม่นั้น มีประเด็นปัญหาที่จะต้อง

พิเคราะห์อีกหลายประเด็น เช่น เรื่องของคำนิยามว่าข้อมูลเป็นทรัพย์ตามความหมายของบทบัญญัติความผิดฐานทำให้เสียทรัพย์หรือไม่ ซึ่งจะมีการกล่าวถึงและวิเคราะห์ต่อไป

3.5 ไวรัสคอมพิวเตอร์กับการทำลายข้อมูล

ไวรัสคอมพิวเตอร์ (Virus Computer) คือโปรแกรมที่มีความสามารถในการแก้ไขดัดแปลงโปรแกรมอื่น เพื่อที่จะทำให้โปรแกรมนั้นๆ สามารถเป็นที่อยู่ของไวรัสคอมพิวเตอร์ได้และสามารถทำให้ไวรัสคอมพิวเตอร์ทำงานได้ต่อไปเรื่อยๆ เมื่อมีการเรียกใช้โปรแกรมที่มีโปรแกรมไวรัสคอมพิวเตอร์นั้น (ทวีศักดิ์ กออนันตกูล 2541 : 8)

การก่อให้เกิดไวรัสคอมพิวเตอร์ เป็นปรากฏการณ์หนึ่งที่เกิดขึ้นในวงการคอมพิวเตอร์ ทำให้เกิดความเสียหายและความสูญเสียอย่างมหาศาลต่อข้อมูลหรือทรัพย์สิน เช่นเดียวกับการกระทำผิดเกี่ยวกับข้อมูลในรูปแบบอื่นๆ ไวรัสคอมพิวเตอร์เป็นที่รู้จักกันใน ค.ศ 1980 โดยเริ่มต้นที่ประเทศสหรัฐอเมริกาและได้แพร่หลายไปในประเทศอื่นๆ และเมื่อเดือนพฤศจิกายน ค.ศ. 1988 สหรัฐอเมริกาได้เผยแพร่ข่าวต่อทั่วโลกว่าได้ประสบกับปัญหาไวรัสคอมพิวเตอร์ อันมีสาเหตุมาจากการบุกรุกเข้าไปในคอมพิวเตอร์ หรือที่เรียกกันว่าการเข้าถึง (Access) โดยบุคคลที่ปราศจากอำนาจ ทำให้หน่วยงานต่างๆ ไม่สามารถใช้คอมพิวเตอร์ของตนได้ตามปกติ

ไวรัสคอมพิวเตอร์เป็นชุดคำสั่งหรือโปรแกรม ซึ่งสามารถแก้ไขดัดแปลงข้อมูลหรือทำลายข้อมูลได้ทันที และไวรัสคอมพิวเตอร์ยังสามารถอยู่ในเครื่องคอมพิวเตอร์ ทำการทำลายข้อมูลตามเงื่อนไขหรือเงื่อนเวลาที่กำหนด อีกทั้งยังสามารถแพร่พันธุ์ อันมีลักษณะคล้ายคลึงกับไวรัสในตัวมนุษย์ โดยวัตถุประสงค์หลักของผู้กระทำก็เพื่อที่จะทำลายข้อมูลในคอมพิวเตอร์

ความเสียหายที่เกิดขึ้นนั้นอาจจะเกิดขึ้นกับข้อมูลเพียงบางส่วนหรือทั้งหมดก็ได้ ขึ้นอยู่กับว่าไวรัสคอมพิวเตอร์ที่อยู่ในเครื่องเป็นไวรัสคอมพิวเตอร์ชนิดใด โดยทั่วไปจะแบ่งความเสียหายออกเป็น 3 ระดับ คือระดับแรกข้อมูลไม่เสียหายเลย เพียงแต่เครื่องนั้นใช้งานไม่ได้ชั่วคราว อันเนื่องมาจากการเกิดไวรัสคอมพิวเตอร์ชนิดที่มีการเติมขยะลงไป คำว่า "ขยะ" หมายถึงข้อมูลที่ระบบคอมพิวเตอร์ไม่ต้องการแต่ผู้ก่อให้เกิดข้อมูลประเภทนี้ใส่ไว้ในเครื่องเป็นจำนวนมาก อันทำให้เครื่องคอมพิวเตอร์นั้นไม่สามารถทำงานต่อไปได้ เพราะไม่มีหน่วยความจำหรือเนื้อที่พอที่จะทำงาน ระดับที่สองคือการก่อให้เกิดความเสียหายแก่ข้อมูลที่เป็นการบอกตำแหน่งที่อยู่ของแฟ้ม

ข้อมูลต่างๆ โดยปกติคอมพิวเตอร์จะทำงานกับแฟ้มข้อมูลได้ จะต้องมีตารางบอกตำแหน่งเนื้อที่ของแฟ้มข้อมูลนั้นๆ เพื่อคอมพิวเตอร์จะได้เข้าถึงข้อมูลในตำแหน่งที่เก็บข้อมูลได้อย่างถูกต้องและรวดเร็ว แต่ไวรัสคอมพิวเตอร์ประเภทนี้จะสร้างความสับสนให้กับตารางบอกตำแหน่ง แต่จะไม่ทำลายข้อมูลที่เก็บอยู่ในคอมพิวเตอร์นั้นๆ ดังนั้นถ้าสามารถแก้ไขตารางให้บอกตำแหน่งที่ถูกต้องได้ก็สามารถนำข้อมูลกลับมาใช้ได้ และระดับสุดท้ายอันก่อให้เกิดความเสียหายอย่างมากคือการทำลายข้อมูลในคอมพิวเตอร์และจัดรูปแบบ (Format) เพื่อใช้ในการเก็บข้อมูลใหม่ ความเสียหายระดับนี้ โดยทั่วไปไม่สามารถที่จะนำข้อมูลกลับมาใช้ได้อีก เว้นแต่จะมีการทำการสำรอง (Backup) ข้อมูลไว้ในสื่อต่างๆ

สำหรับมูลเหตุจูงใจในการก่อให้เกิดไวรัสคอมพิวเตอร์ การศึกษาถึงมูลเหตุจูงใจของผู้สร้างโปรแกรมไวรัสคอมพิวเตอร์ก็เพื่อจะได้วิเคราะห์ถึงวัตถุประสงค์ และอาจจะนำไปใช้เป็นแนวทางในการบัญญัติกฎหมาย ซึ่งมูลเหตุจูงใจมีหลายสาเหตุ ดังนี้

1. เพื่อแสดงความสามารถ โดยมากแล้วจะเป็นการกระทำของนักคอมพิวเตอร์รุ่นหนุ่มสาว จะไม่มีเจตนาที่ชั่วร้ายมากนัก แต่ถือว่าเป็นการทดลองความสามารถเพื่อสร้างความตื่นเต้นให้กับชีวิต บางครั้งถ้ากระทำการได้สำเร็จก็จะได้รับคำชมเชยจากพรรคพวกของตนเอง

2. เพื่อการลงโทษผู้ละเมิด ผู้กระทำมีมูลเหตุจูงใจเพื่อที่จะลงโทษบุคคลที่ไม่ได้ซื้อซอฟต์แวร์มาด้วยความถูกต้อง ผู้ใช้ซอฟต์แวร์เหล่านี้ควรที่จะมาซื้อจากผู้เป็นเจ้าของในราคาตามท้องตลาด แต่กลับไปซื้อจากที่อื่นที่มีการปลอมแปลง หรือบางกรณีใช้วิธีการคัดลอกหรือทำสำเนาจากต้นฉบับจริงและทำต่อๆ กันไป ผู้เขียนซอฟต์แวร์จึงขาดประโยชน์จากรายได้ในส่วนนี้ อันเป็นมูลเหตุจูงใจในการสร้างโปรแกรมไวรัสคอมพิวเตอร์ติดไปกับซอฟต์แวร์ที่ได้มาโดยไม่ถูกต้อง

3. เพื่อการแก้แค้น ผู้กระทำจะมีเจตนาเพื่อการแก้แค้น อันสืบเนื่องมาจากการบุกรุกเข้าไปในระบบคอมพิวเตอร์ บางกรณีก่อให้เกิดความเสียหาย จึงคิดว่าการป้องกันเพียงอย่างเดียวไม่สามารถยับยั้งผู้บุกรุกได้หรืออาจจะไม่สาสมต่อการกระทำ จึงสร้างโปรแกรมไวรัสคอมพิวเตอร์เพื่อที่จะแก้แค้นผู้บุกรุกนั้น (พรชัย เหลียวพัฒนพงศ์, 2537 : 47)

จะเห็นได้ว่าการก่อให้เกิดไวรัสคอมพิวเตอร์เป็นสิ่งที่เลวร้าย เพราะโดยมากจะก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ แต่ก็มีไวรัสคอมพิวเตอร์บางชนิดที่เกิดขึ้นในปัจจุบันไม่ได้ก่อให้เกิดความเสียหาย โดยไม่ได้ไปทำลายข้อมูลต่างๆ ในระบบคอมพิวเตอร์ ยกตัวอย่าง เช่น ไวรัสกลอนหรือเนื้อเพลงสดุดีเจ้าหญิงไดอาน่า เกิดขึ้นที่กรุงแมดดริด ประเทศสเปน ได้มีไวรัสคอมพิวเตอร์ประหลาดชนิดหนึ่งกำลังเข้ามาในเครื่องคอมพิวเตอร์ต่างๆ ของประเทศ โดยการมี

กลอนหรือเนื้อเพลงของนายเอลตัน จอห์น (Elton John) ที่ทำขึ้นเพื่อสดุดีเจ้าหญิงไดอาน่า ปรากฏอยู่เต็มหน้าจอเครื่องคอมพิวเตอร์ต่างๆ ของประเทศ ตามคำกล่าวของผู้เชี่ยวชาญทางด้านคอมพิวเตอร์ทั้งหลายเป็นไปในแง่ที่ดี อีกทั้งยังกระจายไปตามเครือข่ายอินเตอร์เน็ต และก็ได้รับการคุ้มกันในทางตอนเหนือของประเทศแล้ว นายเฟอร์แนนโด (Fernando) ที่ปรึกษาของบริษัทแพนด้าซอฟต์แวร์ (Panda Software) ทางด้านโปรแกรมกำจัดไวรัส (Anti-virus) กล่าวว่าเป็นไวรัสคอมพิวเตอร์ชนิดหนึ่งของโลกที่เป็นไปในแง่ดี เพราะไม่ได้ทำลายหรือโจมตีสิ่งใดทั้งสิ้น สำหรับกลอนหรือเนื้อเพลงแคนเดิ้ลอินเดอะวิน (Candle in the Wind) นั้นเป็นเนื้อเพลงที่ดัดแปลงมาจากเพลงยอดนิยมของมาริลีน มอนโร (Marilyn Monroe) และเนื้อเพลงนี้ก็เป็นเนื้อเพลงที่เอลตัน จอห์น ได้ร้องเมื่อวันที่ฌาปนกิจพระศพของเจ้าหญิง เมื่อเดือนกันยายน 1997 เนื่องมาจากการสิ้นพระชนม์ จากอุบัติเหตุทางรถยนต์เมื่อวันที่ 31 สิงหาคม 1997

(Http://www.fm97.ksc.net/it_talk/970831/newstalk.html, 11 June 1998)