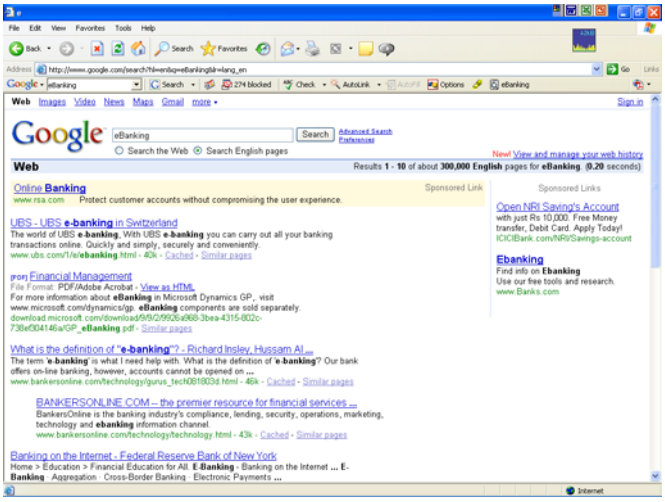
11. ผลกระทบของอินเทอร์เน็ตด้านธนาคารในประเทศไทย

11.1 บริการธนาคารทางอินเทอร์เน็ต

ธนาคารผ่านอินเทอร์เน็ตหรือ “อีแบงค์กิ้ง (eBanking)” มาจากคำว่า “ธนาคารออนไลน์ (Online Banking)” หรือ “ธนาคารอินเทอร์เน็ต (Internet Banking)” หมายถึง การนำเอาอินเทอร์เน็ตเข้ามาประยุกต์ใช้กับกระบวนการของทางธนาคาร อาทิ การติดต่อทางธุรกิจ การจ่ายเงิน เป็นต้น ซึ่งอินเทอร์เน็ตอาจจะอยู่ในรูปแบบต่าง ๆ อาทิ ระบบการให้บริการของธนาคารทางโทรศัพท์ (Banking Telephone System) เครื่องกดเงินอัตโนมัติหรือ “เอทีเอ็ม (ATM = Automatic Teller Machine)” เครื่องโอนเงินอัตโนมัติหรือ “อีเอฟที (EFT = Electronic Fund Transfer)” และบัตรอัจฉริยะหรือ “สมาร์ทการ์ด (Smart Card)” เป็นต้น อีแบงค์กิ้งจะช่วยเพิ่มความสะดวกสบายให้แก่ผู้ใช้บริการโดยผู้ที่ต้องการจะใช้บริการของธนาคารสามารถกระทำธุรกรรมดังกล่าวได้จากที่ใดก็ได้ โดยไม่ต้องเดินทางมาที่ธนาคารและเวลาใดก็ได้ โดยไม่ต้องคำนึงถึงเวลาเปิดทำการของธนาคาร เพียงแค่มีเครื่องคอมพิวเตอร์ที่เชื่อมต่ออินเทอร์เน็ตเท่านั้น [157] หากจะค้นหาความหมายของ “อีแบงค์กิ้ง (eBanking)” จากเว็บกูเกิล จะได้ผลลัพธ์ 300,000 รายการ ดังแสดงในรูปที่ 11.1

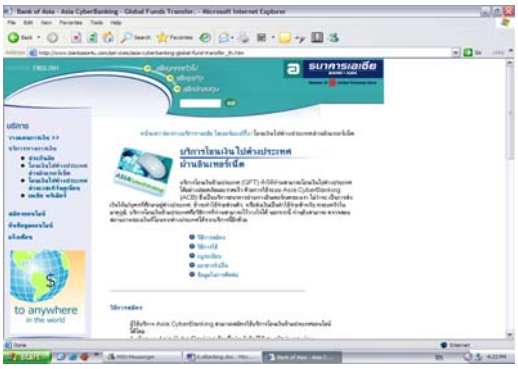


รูปที่ 11.1 ค้นหาความหมายของ “อีแบงค์กิ้ง (eBanking)” ได้ผลลัพธ์ 300,000 รายการ

อีแบงค์กิ้งมีบริการต่าง ๆ มากมาย อาทิ บริการโอนเงินระหว่างบัญชีของผู้ใช้บริการเองหรือการโอนเงินไปยังบุคคลอื่น (Transfer to owner or other account) บริการสอบถามสถานะเช็ค (Cheque status Inquiry) บริการอายัดเช็ค (Stop cheque) บริการสอบถามรายการเคลื่อนไหวในบัญชี (Statement Inquiry) บริการสอบถามยอดคงเหลือในบัญชี (Balance Inquiry) บริการสอบถามรายการชำระปัจจุบัน (Payment Online Inquiry) บริการสอบถามประวัติการชำระเงิน (Payment History Inquiry) บริการของสินเชื่อ (Loan Application) บริการชำระค่าสินค้าหรือบริการ (Payment) บริการชำระค่าบัตรเครดิต (Credit Card Payment) เป็นต้น

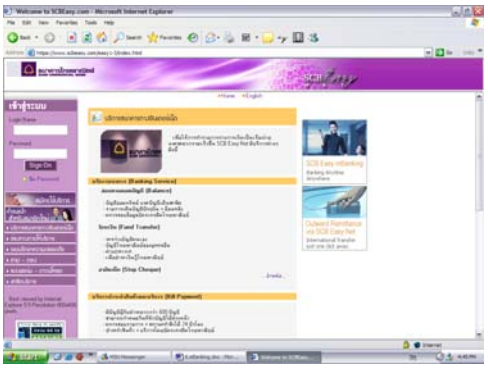
ตัวอย่างธนาคารในประเทศไทยที่ให้บริการผ่านทางอินเทอร์เน็ต มีดังต่อไปนี้

- ธนาคารเอเชีย จำกัด (มหาชน) เปิดให้บริการผ่านทางอินเทอร์เน็ตภายใต้ชื่อว่า “เอเชีย ไซเบอร์แบงค์กิ้ง (ASIA Cyber Banking)” ซึ่งเน้นให้บริการทางด้านการโอนเงินไปต่างประเทศผ่านอินเทอร์เน็ต ดังแสดงในรูปที่ 11.2



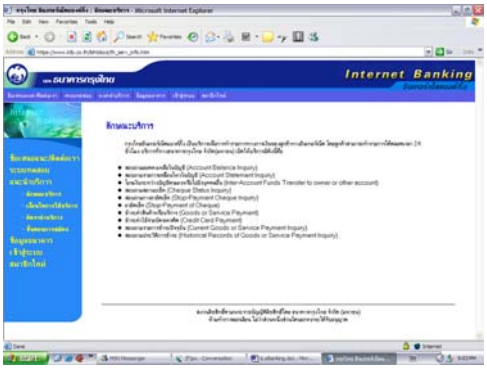
รูปที่ 11.2 บริการเอเซีย ไซเบอร์แบงค์กิ้ง
(ASIA Cyber Banking)

- ธนาคารไทยพาณิชย์ จำกัด (มหาชน) เปิดให้บริการผ่านทางอินเทอร์เน็ตภายใต้ชื่อว่า “เอสซีบี อีซี (SCB Easy)” ดังแสดงในรูปที่ 11.3 ซึ่งให้บริการเกี่ยวกับการทำธุรกรรมทางการเงินมากมาย อาทิ บริการสอบถามยอดบัญชี บริการโอนเงิน บริการอายัดเช็ค บริการชำระค่าสินค้าและบริการ บริการซื้อ-ขายกองทุนเปิดไทยพาณิชย์ และบริการซื้อสินค้าหรือบริการผ่านระบบอินเทอร์เน็ต เป็นต้น



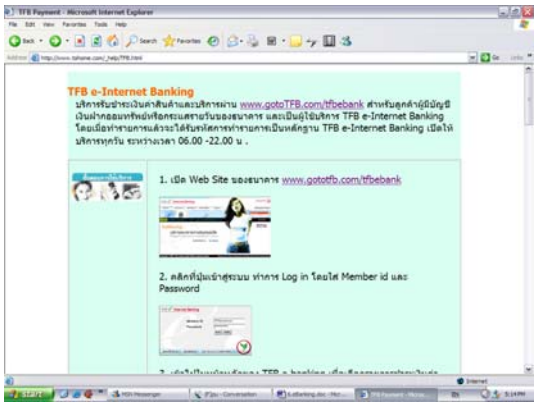
รูปที่ 11.3 บริการเอสซีบี อีซี
(SCB Easy)

- ธนาคารกรุงไทย จำกัด (มหาชน) เปิดให้บริการเพื่อทำรายการทางการเงินของลูกค้าทางอินเทอร์เน็ตภายใต้ชื่อว่า “กรุงไทยอินเทอร์เน็ตแบงค์กิ้ง (KrungThai Internet Banking)” ลูกค้าสามารถทำรายการได้ตลอด 24 ชั่วโมง มีบริการ อาทิ บริการสอบถามยอดคงเหลือในบัญชี บริการสอบถามรายการเคลื่อนไหวในบัญชี บริการโอนเงินระหว่างบัญชีของลูกค้าเองหรือโอนไปยังบุคคลอื่น บริการสอบถามสถานะเช็ค บริการสอบถามรายการชำระปัจจุบันและบริการสอบถามประวัติการชำระ เป็นต้น ดังแสดงในรูปที่ 11.4



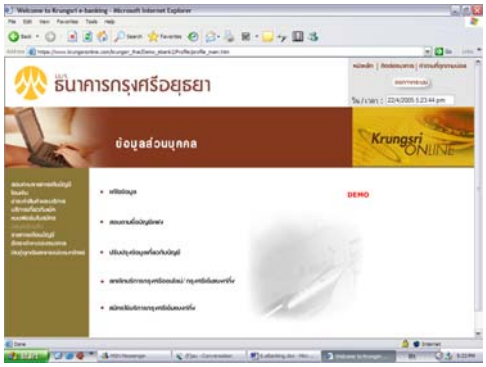
รูปที่ 11.4 บริการกรุงไทยอินเทอร์เน็ตแบงค์กิ้ง
(KrungThai Internet Banking)

- ธนาคารกสิกรไทย จำกัด (มหาชน) เปิดให้บริการผ่านทางอินเทอร์เน็ตภายใต้ชื่อว่า “ทีเอฟบีอินเทอร์เน็ตแบงค์กิ้ง (TFB Internet Banking)” ซึ่งให้บริการรับชำระเงินค่าสินค้าและบริการผ่านทางเว็บ ดังแสดงในรูปที่ 11.5



รูปที่ 11.5 บริการทีเอฟบีอินเทอร์เน็ตแบงค์กิ้ง
(TFB Internet Banking)

- ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) เปิดให้บริการผ่านทางอินเทอร์เน็ตภายใต้ชื่อว่า “กรุงศรีออนไลน์ (KrungSri Online)” ซึ่งให้บริการมากมาย เช่น บริการสอบถามรายการ เดินบัญชี บริการโอนเงิน บริการชำระค่าสินค้าและบริการ และบริการเกี่ยวกับเช็ค เป็นต้น ดังแสดงในรูปที่ 11.6
-



รูปที่ 11.6 บริการกรุงศรีออนไลน์
(KrungSri Online)

ธนาคารที่ให้บริการผ่านสื่ออิเล็กทรอนิกส์อื่น ๆ คือ การให้บริการเกี่ยวกับการทำธุรกรรมด้านการเงินผ่านทางสื่ออิเล็กทรอนิกส์แบบออนไลน์ผ่านระบบเครือข่ายภายในของธนาคารเองโดยตรง ดังจะยกตัวอย่างดังต่อไปนี้

- บริการ “เอทีเอ็ม (ATM = Automatic Teller Machine)” เป็นบริการที่ลูกค้าจะต้องเปิดบัญชีกับธนาคารใดธนาคารหนึ่งไว้ โดยที่ธนาคารนั้น ๆ จะออกบัตรใบหนึ่งหรือที่เรารู้จักกันในชื่อว่า “บัตรเอทีเอ็ม” ให้ลูกค้าพร้อมทั้งรหัสประจำบัตร ลูกค้าสามารถเปลี่ยนรหัสเป็นรหัสอะไรก็ได้ตามต้องการ หลังจากนั้นลูกค้าสามารถใช้บริการต่างของธนาคารผ่านทางตู้เอทีเอ็ม ดังแสดงในรูปที่ 11.7 โดยใช้บัตรและหมายเลขรหัสเป็นตัวนำเข้าไปสู่ระบบการให้บริการต่าง ๆ ของธนาคาร อาทิ บริการฝาก/ถอนเงินสด บริการสอบถามยอดคงเหลือในบัญชี และบริการชำค่าสินค้าและบริการ เป็นต้น ดังแสดงในรูปที่ 11.8 ซึ่งธนาคาร ไทยพาณิชย์ จำกัด (มหาชน) เป็นธนาคารแรกที่เปิดให้บริการเอทีเอ็ม โดยมีนายบรรณวิทย์ บุญรัตน์ ซึ่งศึกษาปริญญาโทที่จุฬาลงกรณีมหาวิทยาลัย ในสาขาวิชาการจัดการสารสนเทศสำหรับธนาคาร โดยมี ศ. ศรีศักดิ์ เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์

รูปที่ 11.7 ตู้เอทีเอ็ม (ATM)

รูปที่ 11.8 การใช้บัตรเอทีเอ็ม

- บริการ “เอสวีซี (SVC = Store Value Card)” เป็นบัตรที่สามารถเก็บข้อมูลด้านการเงินของผู้ใช้ไว้บนบัตรได้ เช่น บัตรอัจฉริยะหรือที่เรียกกันว่า “สมาร์ทการ์ด (Smart Card)” ดังแสดงในรูปที่ 11.9 เป็นต้น

รูปที่ 11.9 บัตรสมาร์ทการ์ด (Smart Card)

- บริการ “ธนาคารทางโทรศัพท์ (Tele-Banking)” เป็นการใช้บริการของธนาคารผ่านทางโทรศัพท์โดยลูกค้าจะต่อสายมายังหมายเลขที่ธนาคารกำหนดไว้ให้บริการ ลูกค้าสามารถสอบถามข้อมูลต่าง ๆ เกี่ยวกับการทำธุรกรรมทางการเงินของตัวเองได้ผ่านทางโทรศัพท์ โดยธนาคารจะจัดหาพนักงานตอบ-รับไว้เพื่ออำนวยความสะดวกให้แก่ลูกค้า ข้อมูลทั้งหมดของลูกค้าจะถูกเก็บไว้ในฐานข้อมูลลูกค้าส่วนกลางซึ่งพนักงานตอบ-รับสามารถเรียกใช้

ได้ตลอดเวลา บริการที่ลูกค้าสามารถใช้ได้ผ่านทางโทรศัพท์มีมากมาย อาทิ บริการรับฟังข้อมูลด้านการเงิน บริการโอนเงิน และบริการชำระค่าสินค้าและบริการ เป็นต้น [147]

11.2 การขโมยข้อมูลบัตรเครดิต

บัตรเครดิต (Credit Card) หมายถึง บัตรพลาสติกขนาดเล็กที่ผู้ใช้สามารถจ่ายเงินในการชำระค่าสินค้า บริการ และอื่น ๆ ได้จากบัตรนี้โดยไม่ต้องใช้เงินสด บัตรเครดิตจะแตกต่างจากบัตรเดบิต (Debit Card) ตรงที่บัตรเครดิตไม่สามารถโอนเงินจากบัญชีของผู้ใช้ภายหลังจากการทำธุรกรรมนั้น ๆ บัตรเครดิตจะอนุญาตให้ผู้ใช้สามารถจัดการกับยอดการใช้ในแต่ละเดือนได้ด้วยตัวของผู้ใช้เอง [145]

จากการที่มีผู้ใช้บัตรเครดิตเพิ่มขึ้นสูงมาก เนื่องจากใช้ง่าย สมัครง่าย และไม่ยุ่งยากในการชำระเงินคืนธนาคาร จึงมีกลุ่มมิจฉาชีพที่วางแผนร่วมมือกันปลอมแปลงบัตรเครดิต ดังจะกล่าวต่อไป

11.2.1 ตร.สืบ 4 รวบแก๊งบัตรเครดิตปลอมคาห้างดัง

เมื่อวันที่ 5 เมษายน พ.ศ. 2548 พล.ต.ต. วิทยา โกสิยะสถิติ ผบก.น. 4 แถลงข่าวการจับกุมแก๊งปลอมบัตรเครดิต อันประกอบไปด้วยผู้ต้องหา 3 คน ดังนี้ นายกำธร วงส์พิภพมงคล (24 ปี) อยู่บ้านเลขที่ 25/88 หมู่ 6 แขวงทุ่งสองห้อง เขตหลักสี่ กทม. นายพุทธพงศ์ สุนันท์วิริยาภรณ์ (36 ปี) อยู่บ้านเลขที่ 104 ถนนวชิรปราการ ต.บางปลาสร้อย อ.เมือง จ.ชลบุรี และนายสมศักดิ์ พันธ์ต่วน (27 ปี) อยู่บ้านเลขที่ 12 ถนนเพชรเกษม ต.หาดใหญ่ อ.หาดใหญ่ จ.สงขลา พร้อมของกลางได้แก่บัตรเครดิตปลอมจำนวน 7 ใบ โทรศัพท์มือถือจำนวน 4 เครื่อง เงินสดจำนวน 248,000 บาท รถยนต์ฮอนด้า แจ๊ส 1 คัน แผ่นป้ายทะเบียนรถ แผ่นป้ายแสดงการเสียภาษีประจำปีรถยนต์ สมุดบัญชีเงินฝากธนาคารต่าง ๆ กุญแจรถ และบัตรเอทีเอ็มของธนาคารต่าง ๆ จำนวนมาก ดังแสดงในรูปที่ 11.10

รูปที่ 11.10 การจับกุมตัวนายกำธร วงส์พิภพมงคล (24 ปี)
นายพุทธพงศ์ สุนันท์วิริยาภรณ์ (36 ปี) และนายสมศักดิ์ พันธ์ต่วน (27 ปี)

เจ้าหน้าที่ตำรวจกล่าวว่า จากการสืบทราบพบว่า จะมีกลุ่มคนร้ายนัดกันมาใช้บัตรเครดิตปลอมที่ห้างเดอะมอลล์ สาขาบางกะปิ โดยคนร้ายทั้งหมดจะนัดพบกันที่ร้านกาแฟซูซูกิภายในห้างดังกล่าว จึงได้วางแผนจับกุม จนกระทั่งสามารถจับกุมตัวผู้ต้องหาได้ทั้ง 3 คนและนำตัวมาสอบสวน จากการสอบสวนในเบื้องต้นผู้ต้องหาทั้งหมดให้การปฏิเสธ โดยนายกำธรอ้างว่า ตนมีอาชีพรับจำนำรถเพื่อกินดอกเบี้ย นายพุทธพงศ์มีอาชีพทำนากุ้ง และนายสมศักดิ์มีอาชีพค้าขายไม้สน โดยทั้งหมดนัดกันมาเที่ยวห้างบริเวณร้านกาแฟดังกล่าว จากนั้นได้มีชายสูงอายุคนหนึ่งไม่ทราบชื่อยื่นซองบุหรี่ให้ เมื่อเปิดดูพบว่า ในซองเป็นบัตรเครดิตต่าง ๆ แล้วตำรวจก็เข้ามาจับกุม ทั้งหมดยืนยันว่าไม่ได้ทำผิดและไม่ทราบเรื่องการปลอมแปลงบัตรเครดิตแต่อย่างใด

อย่างไรก็ตาม จากการสืบสวนของเจ้าหน้าที่ตำรวจพบว่า ผู้ต้องหาทั้งหมดเป็นเพื่อนกัน และร่วมกันซื้อบัตรเครดิตปลอมมาอีกต่อหนึ่ง ก่อนจะนำบัตรปลอมดังกล่าวไปรูดซื้อสินค้าตามร้านค้าต่าง ๆ ซึ่งบัตรเครดิตที่ซื้อมาอยู่ในราคาประมาณ 15,000-20,000 บาท โดยบางบัตรเป็นหน้าบัตรของธนาคารในประเทศไทย

แต่ข้อมูลข้างในเป็นข้อมูลของธนาคารต่างประเทศ ทำให้สามารถมีวงเงินในการซื้อสินค้าสูงเพิ่มสูงขึ้นถึง 300,000 บาท เจ้าหน้าที่จึงแจ้งข้อหาร่วมกันนำบัตรอิเล็กทรอนิกส์ (บัตรเครดิตปลอม) เพื่อนำออกมาใช้โดยผิดกฎหมาย ส่วนนายกำธร ทางตำรวจจะแจ้งข้อหาเพิ่มอีกหนึ่งกระทงคือ ปลอมหรือใช้เอกสารราชการปลอม

ทางตำรวจกล่าวว่า ได้มีการสืบเรื่องนี้มาเป็นเวลานาน เพราะมีผู้เสียหาย อาทิ ร้านขายทองย่านบางกะปิ เป็นต้น มาแจ้งความว่าถูกหลอกซื้อสินค้าโดยใช้บัตรเครดิตปลอม จึงเร่งวางแผนจับกุมตัวผู้ต้องหาดังที่กล่าวมาแล้วนั้นโดยเร็ว เพื่อนำมาสืบสวนสอบสวนหาตัวผู้ผลิตต่อไป เพราะถือว่า เหตุการณ์นี้เป็นเหตุการณ์ที่สร้างผลกระทบต่อเศรษฐกิจของประเทศไทยเป็นอย่างมาก [40]

11.2.2 แก๊งต่างชาติปลอมบัตรเครดิตระบาดหนักในไทย

จากรายงานข่าวของทีมข่าวอาชญากรรม เว็บผู้จัดการออนไลน์ (www.manager.co.th) เมื่อวันที่ 31 พฤษภาคม พ.ศ. 2548 พบว่า มีขบวนการปลอมบัตรเครดิตต่างชาติมากมาย อาทิ มาเลเซีย สิงคโปร์ และจีน เป็นต้น กำลังเข้ามาสร้างปัญหาเรื่องการปลอมแปลงบัตรเครดิตในไทย ซึ่งจากปี พ.ศ. 2548 มีรายงานข่าวจากธนาคารไทยพาณิชย์ จำกัด (มหาชน) ว่ามียอดการทุจริตบัตรเครดิตที่ออกโดยผู้ประกอบการในประเทศไทย ซึ่งในขณะนั้นมีผู้ถือครองบัตรเครดิตปลอมอยู่กว่า 8.8 ล้านใบ และในช่วงไตรมาสแรกของปี พ.ศ. 2548 ได้สร้างความเสียหายไปแล้วคิดเป็นมูลค่ากว่า 80-90 ล้านบาท ซึ่งแสดงให้เห็นว่า ยอดการเจริญเติบโตของการทุจริตบัตรเครดิตมีอัตราเพิ่มสูงขึ้น เมื่อเปรียบเทียบกับปี พ.ศ. 2547 และในปี พ.ศ. 2546

สาเหตุหลักของการที่มีแก๊งต่างชาติเดินทางเข้ามาปลอมบัตรเครดิตในไทยน่าจะมาจากการที่ธนาคารกลางของประเทศมาเลเซียได้ออกมาตรการแก้ไขการทุจริตบัตรเครดิต ด้วยการสั่งให้ผู้ประกอบการธุรกิจบัตรเครดิตทั้งหมดในประเทศมาเลเซียออกบัตรเครดิตที่ติดแผ่นไมโครชิพแทนบัตรเครดิตที่มีแถบแม่เหล็กทั้งหมด และด้วยสาเหตุนี้ก็ส่งผลให้แก๊งปลอมบัตรเครดิตในมาเลเซีย ซึ่งถือว่าเป็นแก๊งปลอมบัตรเครดิตที่ใหญ่ที่สุดในโลกย้ายถิ่นเข้ามาทำมาหากินหลอกลวงด้วยการปลอมบัตรเครดิตในเมืองไทย

ทีมข่าวรายงานต่อว่า เมื่อพิจารณาถึงวงจรการทำงานของขบวนการปลอมบัตรเครดิตแล้วจะพบว่าเริ่มต้นที่ตัวการหลัก ๆ 2 ราย คือ ผู้ผลิตและกลุ่มนายทุน ซึ่งทั้งสองฝ่ายจะเอื้อประโยชน์ซึ่งกันและกัน โดยเริ่มที่ฝ่ายผลิตซึ่งมีกำลังและฝีมือในการปลอมแปลง จะอาศัยเงินทุนที่ได้มาจากกลุ่มนายทุนในการสนับสนุนซื้อเครื่องมือล้ำสมัยต่าง ๆ และกลุ่มนายทุนนั้นอาจจะแยกย่อยออกไปเป็นกลุ่มผู้มีอิทธิพล อาทิ นักการเมือง เป็นต้น กลุ่มมาเฟีย และกลุ่มคนมีสี อาทิ ตำรวจหรือทหาร เป็นต้น ส่วนรายได้ที่ได้มาจากการปลอมแปลงบัตรเครดิตนั้น จะถูกแบ่งออกเป็นสองส่วนตามที่ตกลงกันไว้ซึ่งอาจจะไม่เท่ากัน โดยมากแล้วจะอยู่ที่อัตรานายทุนร้อยละ 60 ของรายได้ทั้งหมด ผู้ผลิตร้อยละ 40 ของรายได้ทั้งหมด หรือบางกลุ่มอาจจะแบ่งรายได้ออกเป็นสองส่วน ส่วนละเท่า ๆ กัน

เมื่อสืบดูรายละเอียดพฤติกรรมโดยละเอียดของขบวนการดังกล่าวแล้ว จะพบว่า ในส่วนของผู้ผลิตที่มีกำลังผลิตและแรงงานคน ส่วนใหญ่จะอาศัยอยู่ตามห้องพัก คอนโด หรืออพาร์ทเมนต์ และมีการเปลี่ยนแปลงโยกย้ายที่อยู่ไปเรื่อย ๆ สามารถแบ่งแยกย่อยออกได้เป็น 3 กลุ่มใหญ่คือ แก๊งปลอมบัตรเครดิตชาวมาเลเซีย ชาวสิงคโปร์ และชาวจีน โดยส่วนใหญ่จะพักอาศัยอยู่ในพื้นที่ย่านรัชดาภิเษก ซึ่งจะใช้พื้นที่บริเวณนี้เป็นแหล่งกบดาน ผู้ผลิตจะทำบัตรเครดิตปลอมออกมาในเบื้องต้น 2 แบบ คือบัตรแบบขาว หมายถึง บัตรเครดิตปลอมที่มีการปั๊มตัวนูนเอาไว้เรียบร้อยแล้ว แต่ยังไม่มีรายละเอียดข้อมูลใด ๆ ซึ่งบัตรแบบนี้จะถูกส่งต่อไปยังร้านค้าต่าง ๆ ส่วนมากจะเป็นห้างใหญ่ ๆ และโรงแรมระดับ 5 ดาว และอีกแบบหนึ่งคือ บัตรเลียนแบบของจริง หมายถึง บัตรเครดิตที่มีรายละเอียดข้อมูลเกี่ยวกับการเงินที่สามารถนำไปรูดชำระสินค้าได้เลย ซึ่งการทำบัตรในรูปแบบนี้ต้องใช้ฝีมือในการทำเป็นอย่างมาก และเมื่อเสร็จสิ้นขั้นตอนการผลิตบัตรทั้งสองแบบแล้ว บัตรเครดิตปลอมจะถูกส่งผ่านให้กับหน้าม้าตัวกลาง หรืออาจจะเรียกว่า “ผู้จัดจำหน่าย (Distributor)” ที่ทำหน้าที่ขายบัตรปลอมให้แก่ลูกค้าต่อไป

ต่อมา ทีมข่าวได้สืบลึกเข้าไปถึงวิธีการที่กลุ่มคนร้ายเหล่านี้ใช้ในการปลอมแปลงบัตรเครดิตขึ้นมา จนได้ข้อมูลที่น่าเชื่อถือได้จากแหล่งข่าวระดับสูงภายในกองบัญชาการตำรวจนครบาล ทำให้รู้ว่าคนร้ายกลุ่มนี้สมัยก่อนจะใช้วิธีการส่งสายเข้าไปสืบหาข้อมูลในร้านค้าชื่อดัง หรือโรงแรมระดับ 5 ดาว ซึ่งสายดังกล่าว จะใช้

เครื่องมือสำหรับอ่านข้อมูลจากบัตรเครดิตหรือบัตรเอทีเอ็ม เรียกว่า “สคิมเมอร์ (Skimmer)” ในการดักเก็บข้อมูลของลูกค้าซึ่งส่วนใหญ่จะเป็นนักธุรกิจชาวต่างชาติ จากนั้นก็จะนำเอาข้อมูลที่ดักเก็บได้นั้นมาถ่ายลงสู่เครื่องคอมพิวเตอร์ ผ่านกรรมวิธีปลอมแปลงบัตรเครดิต ซึ่งบัตรที่ปลอมแปลงออกมานั้น จะเรียกว่า “บัตรหน้าไทยข้อมูลเทศ” ซึ่งความเสียหายที่เกิดขึ้นทั้งหมดจะส่งผลเสียให้กับธนาคารต่างชาติที่ผู้เสียหายเปิดทิ้งไว้ และหากทางธนาคารต่างชาติสืบค้นพบว่า เงินที่ถูกขโมยไปนั้นถูกใช้ในประเทศไทย ก็จะส่งผลเสียต่อชื่อเสียงของประเทศไทยต่อไปอีก

แหล่งข่าวภายในกองบัญชาการตำรวจนครบาลกล่าวต่อว่า แต่ในปัจจุบันนี้ กลุ่มคนร้ายได้เปลี่ยนวิธีการใหม่แล้ว เพื่อหลบหนีการจับกุมของเจ้าหน้าที่ตำรวจ ล่าสุดตรวจพบว่า มีการลักลอบเกี่ยวสายโทรศัพท์ หรือ “ไวร์แทปปิ้ง (Wire Tapping)” หรืออีกชื่อหนึ่งคือ “เทเลโฟนแทปปิ้ง (Telephone Tapping)” หมายถึง การดูแลความเป็นไปของช่องทางการติดต่อสื่อสารผ่านทางระบบของโทรศัพท์และอินเทอร์เน็ตระหว่างการสนทนาโดยบุคคลที่สาม [161] ซึ่งวิธีการดังกล่าวนี้ได้ถูกคนร้ายมาใช้ไปในทางที่ผิด นั่นคือ การลักลอกแอบดูข้อมูลของลูกค้าจากองค์การโทรศัพท์ อาทิ ขณะที่ลูกค้าให้บัตรเครดิตแก่พนักงานเพื่อชำระสินค้า ขบวนการปลอมบัตรนี้จะลักลอกดักพ่วงสายโทรศัพท์ที่ต่อตรงจากร้านค้า ผ่านชุมทางสายขององค์การโทรศัพท์ไปยังธนาคารของลูกค้า และทางแหล่งข่าวภายในเชื่อว่า อาจจะมีการลักลอบเกี่ยวสายจากทางธนาคารเช่นเดียวกัน ซึ่งเชื่อได้ว่าวิธีนี้อาจจะมีเจ้าหน้าที่พนักงานภายในขององค์การโทรศัพท์รู้เห็นด้วย

เครือข่ายของการทำงานของคนร้ายกลุ่มนี้สามารถแยกย่อยออกไปได้ดังนี้ ฝ่ายลักลอบเก็บข้อมูลบัตรเครดิตของผู้เสียหาย ฝ่ายผลิตบัตรเครดิต บัตรเอทีเอ็ม และบัตรประชาชนปลอม ฝ่ายถือบัตรที่ถูกทำขึ้นเพื่อนำไปส่งขายต่อ และฝ่ายรับจ้างนำบัตรปลอมนั้นไปรูดชำระสินค้า

จากการรวบรวมข้อมูลการจับกุมตัวคนร้ายทั้งหมดแล้วนั้น พบว่า เจ้าหน้าที่ตำรวจสามารถตามจับกุมตัวคนร้ายใน 2 ประเภทหลังได้มากที่สุด แต่ต้นตอของกระบวนการผลิตนั้นค่อนข้างจะเป็นเรื่องที่ยากลำบาก เพราะคนร้าย 2 ประเภทนี้จะไม่ทราบหรือรู้จักฝ่ายอื่น ๆ เลย อย่างไรก็ตามจากการสอบสวนคนร้ายรายย่อยที่สามารถจับกุมได้แล้ว ส่งผลให้ทางเจ้าหน้าที่ตำรวจสืบทราบว่า แหล่งผลิตบัตรเครดิตและบัตรเอทีเอ็มปลอมมีขบวนการใหญ่อยู่ที่ประเทศมาเลเซียและสิงคโปร์ ซึ่งทางเจ้าหน้าที่ตำรวจจะได้ติดตามจับกุมต่อไป

การกระทำความผิดเกี่ยวกับการปลอมแปลงบัตรเครดิตสร้างความเสียหายให้กับประเทศชาติเป็นอย่างมาก และกระทบถึงกลไกทางเศรษฐกิจของประเทศ ซึ่งทางสำนักงานตำรวจแห่งชาติได้ออกกฎหมายที่ใช้ลงโทษผู้กระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายวิธีพิจารณาความอาญา สำนักงานตำรวจแห่งชาติ มาตรา 269/1 ผู้ใดทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับ หรือแม้แต่ส่วนใดส่วนหนึ่ง เติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใด ๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นและประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริง หรือเพื่อประโยชน์อย่างใดอย่างหนึ่ง ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ต้องระวางโทษจำคุกตั้งแต่หนึ่งถึงห้าปี และปรับตั้งแต่สองหมื่นถึงหนึ่งแสนบาท

มาตรา 269/2 ยังกำหนดบทลงโทษอีกว่า หากผู้ใดทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงสิ่งใด ๆ ซึ่งระบุไว้ในมาตรา 265/1 หรือมีเครื่องมือ หรือวัตถุเช่นว่านั้น เพื่อใช้ หรือให้ได้ข้อมูลในการปลอมหรือแปลง ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท รวมไปถึงมาตรา 269/4 ที่กำหนดโทษว่า หากผู้ใดใช้หรือมีไว้ใช้ซึ่งสิ่งใด ๆ ตามมาตรา 269/1 อันได้มาโดยรู้ว่าเป็นของที่ทำปลอมหรือแปลงขึ้น ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี หรือปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ

นอกเหนือจาก 2 มาตราที่กล่าวมาแล้วนั้น ผู้ที่กระทำความผิดฐานปลอมหรือแปลงบัตรเครดิตยังต้องได้รับโทษตามมาตรา 269/5 ที่ระบุว่า ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นและประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ มาตรา 269/6 ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ และยังต้องรับโทษตามมาตรา

269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นและประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ นอกจากนี้ ในมาตรา 269/7 ยังกำหนดบทลงโทษอีกว่า ถ้าการกระทำดังกล่าวในหมวดนี้เป็นการกระทำที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้ที่มีสิทธิใช้ เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ผู้กระทำความผิดต้องระวางโทษหนักกว่าที่บัญญัติไว้ในมาตรานั้น ๆ กึ่งหนึ่ง [18]

เมื่อวันที่ 27 กรกฎาคม 2549 บริษัท ทีโอที จำกัด (มหาชน) ได้ออกมาประกาศเตือนเจ้าของร้านค้าต่าง ๆ ให้หันมาเลือกใช้เทคโนโลยีการสื่อสารแบบใหม่ที่เรียกว่า “เครือข่ายบริการสื่อสารร่วมระบบดิจิทัล” หรือ “ไอเอสดีเอ็น (ISDN = Integrated Services Digital Network)” ที่เป็นระบบเครือข่ายที่สลับวงจรในด้านการสื่อสารข้อมูลผ่านทางโทรศัพท์ ที่อนุญาตให้ส่งผ่านข้อมูลและเสียงผ่านระบบดิจิทัลไปตามเครื่องโทรศัพท์ทั่วไป [154]

นายนพณัฏฐ์ หุตะเจริญ ผู้ช่วยกรรมการผู้จัดการใหญ่ของ บริษัท ทีโอที จำกัด (มหาชน) กล่าวถึงกรณีที่มีแก๊งปลอมบัตรเครดิตใช้เครื่องเกี่ยวสายโทรศัพท์ในการขโมยข้อมูลบัตรว่า ผู้ประกอบการร้านค้ารายย่อยควรเปลี่ยนระบบสายโทรศัพท์จากเดิมให้มาเป็นเครือข่ายไอเอสดีเอ็น เพื่อให้การเกี่ยวสายทำได้ยากขึ้น โดยขอให้แจ้งแก่ผู้ให้บริการก่อนการขอเลขหมายโทรศัพท์ด้วยว่า ต้องการนำหมายเลขนี้มาใช้ส่งข้อมูลบัตรเครดิตกับธนาคาร

ด้านนาย พงษ์สิทธิ์ ชัยฉัตรพรสุข ประธานคณะทำงานป้องกันทุจริตบัตรเครดิต ชมรมธุรกิจบัตรเครดิต กล่าวว่า ในช่วงหกเดือนแรกของ พ.ศ. 2550 ประเทศไทยมีความเสียหายจากการปลอมบัตรเครดิตแล้วกว่า 300 ล้านบาท เพิ่มขึ้นจากปีที่แล้วทั้งปีที่เสียหายไป 200 ล้านบาท โดนส่วนใหญ่ธนาคารจะเป็นผู้รับผิดชอบทั้งหมด แต่หากทางธนาคารตรวจพบว่าเป็นความผิดพลาด ประมาท และทุจริตโดยร้านค้าเป็นผู้กระทำขึ้น ร้านค้าจะต้องเป็นฝ่ายรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น จึงอยากจะเตือนให้ร้านค้าระวังการซื้อสินค้าด้วยบัตรเครดิตคราวละมาก ๆ โดยสินค้าประเภทที่มีความเสี่ยงที่จะถูกซื้อจากบัตรเครดิตปลอมมากที่สุดคือ สินค้าประเภทโทรศัพท์มือถือ [153]

11.2.3 แก๊งปลอมบัตรเครดิตข้ามชาติ

เมื่อวันที่ 25 กรกฎาคม พ.ศ. 2549 พล.ต.ต. ปัญญา มาเม่น ผู้บังคับการตำรวจท่องเที่ยว (ผบก.ทท.) และ นายพงษ์สิทธิ์ ชัยฉัตรพรสุข ประธานชมรมธุรกิจบัตรเครดิต ร่วมแถลงข่าวการจับกุมตัว นายทศพล เชาวนวุฒิ (42 ปี) ดังแสดงในรูปที่ 11.11 อยู่บ้านเลขที่ 4 ถนนราษฎร์อุทิศ ซอย 21/1 ต.หาดใหญ่ อ.หาดใหญ่ จ.สงขลา หนึ่งในแก๊งลักลอบขโมยข้อมูลบัตรเครดิต พร้อมของกลางเป็นเครื่องแปลงสัญญาณโทรศัพท์จำนวน 4 เครื่อง ถ่านไฟฉายจำนวน 24 ก้อน และเครื่องเล่นเพลงเอ็มพีสามจำนวน 1 เครื่อง

รูปที่ 11.11 การจับกุมตัว นายทศพล เชาวนวุฒิ (42 ปี)
หนึ่งในแก๊งลักลอบขโมยข้อมูลบัตรเครดิต

ในเบื้องต้น นายทศพลให้การสารภาพว่า ตนเองมีหน้าที่เฝ้าบ้านและคอยเปลี่ยนถ่านไฟฉาย รวมทั้งเก็บข้อมูลใส่เครื่องเล่นเพลงเอ็มพีสาม หากข้อมูลในเครื่องหนึ่งเต็มก็จะนำเครื่องใหม่มาเปลี่ยน เพื่อรอให้หัวหน้าซึ่งเป็นชาวมาเลเซียมารับเอาข้อมูลไป โดยในแต่ละเครื่องสามารถเก็บข้อมูลบัตรเครดิตได้ประมาณ 100 รหัส โดยจะได้รับค่าจ้างจากหัวหน้าแก๊งในราคาที่ไม่แน่นอน แต่ถ้าหัวหน้าเดินทางมาประเทศไทยก็จะได้เงินครั้งละ 3,000–4,000 บาท

ทางเจ้าหน้าที่ตำรวจให้ข้อมูลเพิ่มเติมว่า การจับกุมนายทศพลในครั้งนี้สืบเนื่องมาจากทางเจ้าหน้าที่ตำรวจของประเทศมาเลเซียสามารถจับกุมผู้ต้องหาที่ครอบครองถือบัตรเครดิตปลอมที่เกาะปีนัง และตรวจสอบจากข้อมูลในบัตรเครดิตปลอมแล้วพบว่า เป็นข้อมูลที่ลักลอบขโมยมาจากนักท่องเที่ยวชาวต่างชาติใน จ. ภูเก็ต จึงสืบสวนแกะรอยมานานกว่า 5 เดือน จนกระทั่งสามารถจับกุมได้ในที่สุด เจ้าหน้าที่ตำรวจอธิบายว่า สาเหตุที่การจับกุมแก๊งปลอมบัตรเครดิตเป็นไปได้ยากนั้น เป็นเพราะการกระทำของแก๊งอาชญากรรมข้ามชาติที่ไม่ได้ลงมือกระทำความผิดที่ประเทศไทยเพียงที่เดียว หากแต่ลงมือวนเวียนไปในหลายประเทศ อาทิ ไทย สิงคโปร์ มาเลเซีย เกาหลีใต้ ญี่ปุ่น รวมทั้งในยุโรป และสหรัฐอเมริกา เป็นต้น นอกจากนี้ ยังมีข้อจำกัดในเรื่องของข้อมูลของคนร้าย อาทิ ทะเบียนราษฎร หมายเลขบัตรประชาชน ทะเบียนรถยนต์ เป็นต้น เพราะแก๊งคนร้ายเหล่านี้ไม่ใช่คนไทย และไม่ได้พักอาศัยอยู่ในประเทศไทยโดยถาวร

สำหรับวิธีการของแก๊งคนร้ายรายนี้ จะใช้ไวร์แทปปิ้งมาดูดข้อมูลจากชุมสายโทรศัพท์ โดยจะต้องตรวจสอบดูว่า มีข้อมูลรหัสบัตรเครดิตผ่านเข้ามาในชุมสายนั้น ๆ หรือไม่ ซึ่งวิธีการนี้ต้องอาศัยช่างเทคนิคที่มีความรู้ความเชี่ยวชาญเพื่อตรวจสอบดูว่า มีข้อมูลบัตรเครดิตไหลเข้ามาในชุมสายโทรศัพท์หรือไม่ จากนั้นก็จะทำการเกี่ยวสายดักจับข้อมูลเหล่านั้นเพื่อดักจับรหัสบัตรเครดิตที่จะไหลมาพร้อมกับรหัสลับ หรือ “ซิเคียวริตี้ โคด (Security Code)” ซึ่งเป็นระบบรักษาความปลอดภัยของทางธนาคาร และด้วยเหตุนี้ แก๊งขโมยบัตรเครดิตจึงต้องมี “โปรแกรมถอดรหัส” เพื่อหาทางถอดรหัสและสกัดเอารหัสบัตรเครดิตมาใช้ จากนั้นก็จะบันทึกข้อมูลลงในเครื่องเล่นเพลงเอ็มพีสาม ซึ่งมีคุณสมบัติเด่นคือ สามารถเก็บข้อมูลได้มากกว่าแผ่นซีดีทั่วไป [19]

11.2.4 ปลอมบัตรเครดิตและขโมยข้อมูล

จากหนังสือพิมพ์คม ชัด ลึก ฉบับวันอังคารที่ 10 กรกฎาคม พ.ศ. 2550 มีรายงานข่าวว่า นายปัญญา ไชยมงคล (58 ปี) อดีตพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟฝ.) ได้เข้าแจ้งความกับ พ.ต.ต. ปิยะชัย สะเดา พนักงานสอบสวน สภ.อ เมืองขอนแก่น โดยนายปัญญาให้การด้วยน้ำตานองหน้าว่า เงินสดในบัญชีธนาคารกรุงไทย สาขาขอนแก่น ถูกกดออกไปจากบัญชีรวมมูลค่าเป็นเงินกว่า 1,400,000 บาท ตามข่าวรายงานว่าหลังจากที่นายปัญญาได้รับเงินบำเหน็จจากการไฟฟ้าฝ่ายผลิตแห่งประเทศไทยเป็นเงินกว่า 2,000,000 บาท ก็ได้ใช้เงินดังกล่าวเดินทางไปท่องเที่ยวที่ประเทศมาเลเซียตั้งแต่วันที่ 5-8 ธันวาคม พ.ศ. 2549 ก่อนจะกลับมาปรับยอดบัญชีอีกครั้งที่ธนาคารในจ. ขอนแก่น แต่ก็พบว่าเงินในบัญชีได้หายไปอย่างไร้ร่องรอยดังข่าวที่กล่าวมา

เบื้องต้นนั้น นายปัญญาสงสัยว่าพนักงานในธนาคารอาจจะมีส่วนรู้เห็น เพราะเขาเล่าว่า เมื่อเดือนพฤศจิกายน พ.ศ. 2549 เขาเพิ่งจะไปเปลี่ยนบัตรเอทีเอ็มมาก่อนที่จะเดินทางไปประเทศมาเลเซีย และจากผลการตรวจสอบของทางธนาคารพบว่า เงินของนายปัญญาถูกกดออกไปวันละ 150,000 แสนบาท ตั้งแต่วันที่ 5-13 ธันวาคม พ.ศ. 2549 (ในขณะที่เข้าแจ้งเรื่องนั้น เป็นวันที่ 13 ธันวาคม พ.ศ. 2549 ก็ยังมีการกดเงินดังกล่าวออกไป) โดยส่วนใหญ่คนร้ายจะเลือกกดเงินจากตู้เอทีเอ็มในย่านอนุสาวรีย์ชัยฯ ในเขตกทม. แทบทั้งสิ้น

ร.ต.อ. ฉัตรมงคล วิศินอมร และ พล.ต.ต. ปัญญา มาเม่น หนึ่งในผู้เชี่ยวชาญพฤติกรรมแก๊งปลอมบัตรเครดิต สันนิษฐานว่า กรณีนี้มีความเป็นไปได้ 2 ทาง คือ 1. เป็นการกระทำของแก๊งปลอมบัตรเครดิต และ 2. เป็นการขโมยข้อมูลหรือ “แฮก (Hack)” ข้อมูลทางคอมพิวเตอร์

หากเป็นการกระทำของแก๊งปลอมบัตรเครดิต ทางตำรวจกล่าวว่า แก๊งพวกนี้จะมีนายทุนที่คอยรับซื้อข้อมูล ซึ่งเป็นคนไทย โดยจะมีเครื่องสคิมเมอร์ (Skimmer) ซึ่งแม้แต่ธนาคารชั้นนำหลายแห่งยังไม่มีเครื่องนี้ไว้ในครอบครอง เครื่องนี้จะมีการทำงานคล้ายกับเครื่องอ่านข้อมูลของลูกค้าธนาคาร และเครื่องอ่านข้อมูลของบัตรเอทีเอ็มในตู้เอทีเอ็มโดยจะมีนายทุนนำเครื่องนี้เข้ามาและนำไปแจกจ่ายให้กับเครือข่ายที่แฝงตัวเป็นพนักงานเก็บเงินตามสถานที่ต่าง ๆ นอกจากนี้ยังอาจจะมีเจ้าหน้าที่ของธนาคารบางคนอยู่ในขบวนการนี้ด้วย เมื่อผู้เสียหายชำระค่าสินค้าผ่านบัตรเครดิต บัตรเครดิตนั้นจะถูกนำไปรูดกับเครื่องดังกล่าวและบันทึกข้อมูลของผู้เสียหายไว้ จากนั้นนายทุนจะรับซื้อข้อมูลนั้นแล้วนำไปขายต่อให้กับแก๊งปลอมบัตรเครดิต ซึ่งส่วนมากจะเป็นชาวต่างชาติ อาทิ สิงคโปร์ มาเลเซีย และอินโดนีเซีย เป็นต้น แก๊งปลอมบัตรเครดิตนี้จะใช้ระยะเวลาเพียงแค่ 1-2 วัน ก็สามารถ

ลอกเลียนแบบบัตรออกมาจำหน่ายได้ในราคาเพียง 2,000-20,000 บาท โดยราคาของบัตรปลอมนี้จะถูกหรือแพงนั้นขึ้นอยู่กับสัญชาติของเจ้าของบัตร อาทิ ถ้าเจ้าของบัตรถือสัญชาติเป็นญี่ปุ่น บัตรปลอมก็จะมีราคาแพง เนื่องจากธนาคารในประเทศญี่ปุ่นจะให้วงเงินสูง

ส่วนการขโมยหรือแฮกข้อมูลจากเครื่องคอมพิวเตอร์ ทางตำรวจกล่าวเพิ่มเติมว่า คนร้ายจะมีการสร้างโปรแกรมอ่านข้อมูลบัตรเครดิตไปแอบลักลอบติดตั้งไว้ตามตู้เอทีเอ็มต่างๆ แต่กรณีนี้ทางตำรวจเชื่อว่าต้องมีการรู้เห็นจากเจ้าหน้าที่ของธนาคาร เพราะมีเพียงเจ้าหน้าที่ของธนาคารเท่านั้นที่สามารถเปิด-ปิดตู้เอทีเอ็มได้ และยังเป็นผู้ที่สามารถเปิดดูข้อมูลส่วนตัวของลูกค้าธนาคารจากบัตรเครดิตหรือบัตรเอทีเอ็มได้ จากกรณีของนายปัญญานี้ ร.ต.อ. ฉัตรมงคล วิเคราะห์ว่า การที่ผู้เสียหายเคยทำเรื่องเพื่อเปลี่ยนบัตรมาก่อนนั้นอาจจะเป็นไปได้ว่ามีเจ้าหน้าที่ของธนาคารรู้เห็น แต่ก็ต้องดูพฤติกรรมของนายปัญญาเองด้วยว่า ได้นำบัตรเครดิตดังกล่าวไปซื้อสินค้าโดยชำระเงินผ่านทางบัตรหรือไม่ หรือเคยฝากใครคนใดกดเงินผ่านบัตรเครดิตหรือไม่ เพราะคนนั้นอาจจะเอารหัสบัตรของนายปัญญาไปขายต่อให้กับแก๊งปลอมบัตรเอทีเอ็มก็เป็นได้

จากกรณีนี้ ถือว่าเป็นข้อเตือนใจให้แก่คนที่ชอบใช้บัตรเครดิตชำระสินค้าต่างๆ ให้คอยตรวจสอบดูว่าเมื่อให้บัตรเครดิตแก่พนักงานของร้านค้าแล้ว พนักงานคนนั้นเอาบัตรของตนเองไปรูดที่เครื่องรูดเงินจริงๆ ของธนาคารหรือไม่ หรือถ้ามีเหตุจำเป็นที่ไม่สามารถเดินไปดูได้ด้วยตัวเอง ก็ให้สังเกตว่าพนักงานเอาบัตรเครดิตของตนเองไปที่เครื่องรูดเงินจริงๆ หรือไม่ แต่ทางที่ดีที่สุด ควรจะนำบัตรไปกดเงินออกมาแล้วจ่ายเป็นเงินสดจะดีกว่าเพื่อความปลอดภัยจากคนร้ายกลุ่มนี้ [53]

11.2.5 จับเว็บปลอมดูดเงินเอทีเอ็ม

เมื่อวันที่ 5 มิถุนายน พ.ศ. 2550 พล.ต.ต.ชูชาติ สุวรรณาคม ผบก.ทท. พร้อม พ.ต.ท. พันธนะ นุชนารถ รองผกก. 4 บก.ทท. ร่วมกับนายพงษ์สิทธิ์ ชัยฉัตรพรสุช ผู้จัดการสายการบริหารป้องกันการทุจริตของธนาคารไทยพาณิชย์ จำกัด (มหาชน) และตัวแทนสมาคมธนาคารไทย แถลงข่าวการจับกุมตัวนายโกมา โอนานิ (40 ปี) ชาวแซมเบีย และนางสายพิณ ศรีลิขิต (34 ปี) ดังแสดงในรูปที่ 11.12 อยู่บ้านเลขที่ 291/49 ซอยแยกรัชฎภัณฑ์ แขวงมักกะสัน เขตราชเทวี กรุงเทพฯ พร้อมของกลางที่ตรวจพบคือ สมุดบัญชีของธนาคารไทยพาณิชย์ จำกัด (มหาชน) สาขาย่อยนานา สแควร์ สมุดบัญชีของธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) สาขาสะพานใหม่ดอนเมือง และสาขาสยามพารากอน บัตรเอทีเอ็มของธนาคารไทยพาณิชย์ จำกัด (มหาชน) และบัตรเอทีเอ็มของธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) โดยทั้งสองคนถูกจับกุมในข้อหาร่วมกันฉ้อโกงประชาชน และปลอมแปลงและใช้เอกสารปลอม

รูปที่ 11.12 การจับกุมตัวนายโกมา โอนานิ (40 ปี) ชาวแซมเบีย และนางสายพิณ ศรีลิขิต (34 ปี)

รายงานข่าวกล่าวว่า ทางศูนย์สืบสวนปราบปรามคนร้ายข้ามชาติและอาชญากรรมบัตรอิเล็กทรอนิกส์ของกองบัญชาการตำรวจท่องเที่ยวได้รับการประสานงานข้อมูลจากสมาคมธนาคารไทย ว่ามีกลุ่มคนร้ายได้ร่วมมือกันสร้างเว็บเลียนแบบธนาคารไทยพาณิชย์ และสถาบันทางการเงินชั้นนำของไทย โดยเพิ่มช่องให้ลูกค้าของธนาคารใส่รหัสบัตรเอทีเอ็มบนหน้าเว็บที่คัดเลือกแบบสุ่มส่งให้ลูกค้าของธนาคาร โดยแจ้งให้ลูกค้าใส่รหัสผ่านเพื่อเข้าไปแก้ไขข้อมูล ซึ่งเมื่อลูกค้าหลงเชื่อใส่รหัสผ่าน คนร้ายก็จะเก็บรวบรวมข้อมูลของลูกค้าก่อนนำรหัสผ่านนั้น

ไปเข้าเว็บตัวจริงเพื่อทำการโอนเงินหรือนำไปชำระค่าบริการโทรศัพท์มือถือในระบบเติมเงิน ซึ่งก่อให้เกิดความเสียหายให้กับลูกค้าที่ใช้บริการของธนาคารและสถาบันทางการเงินคิดเป็นมูลค่าความเสียหายหลายสิบล้านบาท

เมื่อมีการประสานงานจากทางสมาคมธนาคารไทย ทางกองบังคับการตำรวจท่องเที่ยวก็ได้ทำการสืบสวนเพื่อติดตามจับกุมตัวคนร้ายที่ก่อคดีนี้ โดยได้ตรวจสอบจากกล้องโทรทัศน์วงจรปิดบริเวณตู้เอทีเอ็มที่คนร้ายไปกดโอนเงินที่ถนนสุขุมวิท 3 แขวงคลองเตยเหนือ เขตวัฒนา จนสืบทราบว่ากลุ่มคนร้ายนี้ประกอบด้วยนายโกมาและนางสายพิณ จึงได้รวบรวมหลักฐานขออนุมัติหมายจับจากศาลอาญา ก่อนกระจายกำลังเข้าเฝ้าสังเกตการณ์บริเวณถนนสุขุมวิท ย่านซอยนานา จนกระทั่งพบนางสายพิณเดินอยู่บริเวณกลางซอยสุขุมวิท 3 จึงได้แสดงหมายจับก่อนเข้าทำการจับกุม และเมื่อสอบสวนขยายผลก็สามารถจับกุมตัวนายโกมา ได้ที่ห้องพักโรงแรมโรส อินน์ ซอยสุขุมวิท 3 จากการสอบสวนผู้ต้องหาให้การสารภาพว่าได้ลักลอบนำข้อมูลของลูกค้าไปใช้ในการโอนเงินจริง แต่ยังไม่ยอมซัดทอดไปถึงผู้ร่วมขบวนการ ซึ่งทางเจ้าหน้าที่ได้จับกุมตัวไว้เพื่อสอบสวนขยายผลเพื่อจับกุมกลุ่มคนร้ายกลุ่มนี้ต่อไป

นายพงษ์สิทธิ์ ชัยฉัตรพรสุข ประธานคณะทำงานป้องกันทุจริตบัตรเครดิต ชมรมธุรกิจบัตรเครดิต กล่าวว่า จากการตรวจสอบของข้อมูลเชื่อว่ากลุ่มคนร้ายกลุ่มนี้น่าจะเป็นคนที่มีความรู้และเชี่ยวชาญทางด้านอินเทอร์เน็ตเป็นอย่างดี โดยคนร้ายจะออกแบบเว็บเลียนแบบธนาคารหรือสถาบันการเงินที่เปิดให้บริการลูกค้าผ่านทางอินเทอร์เน็ตพร้อมการแก้ไขข้อมูลเล็กน้อยในช่องที่สำหรับใส่รหัสผ่าน จากนั้นก็สุ่มส่งหน้าเว็บที่สร้างเลียนแบบไปตามอีเมล์ของลูกค้าธนาคาร หากลูกค้าคนใดหลงเชื่อใส่รหัสผ่านไปในเว็บดังกล่าว คนร้ายก็จะนำรหัสผ่านนั้นไปเข้าเว็บจริงของธนาคารเพื่อโอนเงินในบัญชีของลูกค้าไปยังบัญชีที่คนร้ายเปิดทิ้งไว้ ซึ่งจากการสืบสวนสอบสวนพบว่า ต้นตอของการสร้างเว็บมาจากประเทศเบลเยี่ยมและฝรั่งเศส โดยพฤติกรรมของคนร้ายกลุ่มนี้ได้สร้างความเสียหายให้แก่ธนาคารไทยพาณิชย์ รวมถึงความเชื่อมั่นของลูกค้าที่มีต่อธนาคารไทยพาณิชย์หรือสถาบันการเงินชั้นนำของไทยคิดเป็นมูลค่ากว่าสิบล้านบาท และจากการตรวจสอบของสมาคมธนาคารไทย พบว่าคดีที่เกิดขึ้นในครั้งนี้ถือว่าเป็นคดีแรกในประเทศไทย [33]

11.2.6 จับแก๊งต้มตุ๋นกดเอทีเอ็ม

เมื่อวันที่ 7 มิถุนายน พ.ศ. 2550 พ.ต.ท.เศกสิทธิ์ สุภาอ้วน สว.สส.สน.ทองหล่อ ได้ทำการสืบสวนและจับกุมตัวกลุ่มคนร้ายอันประกอบไปด้วย นายศักดิ์ชัย แจ้มกระจ่าง (34 ปี) อาชีพ รปภ.ห้างเดอะมอลล์สาขาบางแค นายอนิรุทต์ แจงเอี่ยมเอก (30 ปี) อาชีพ รปภ.ห้างเดียวกัน นายอนุรักษ์ แจงเอี่ยมเอก (31 ปี) อาชีพขับรถแท็กซี่ ซึ่งเป็นพี่ชายของนายอนิรุทต์ นายนัทธี พิทักษ์ธรรม (44 ปี) อาชีพ ขับรถแท็กซี่ และนายพรรษา พัวพันธ์ (42 ปี) อาชีพ พนักงานบริษัท ดังแสดงในรูปที่ 11.13 ในข้อหาร่วมกันฉ้อโกงทรัพย์ ในขั้นแรกผู้ต้องหาทั้งหมดยังให้การปฏิเสธ

จากการแจ้งความดำเนินคดีของนายชัยยุทธ ศรีวิชัย (27 ปี) อาชีพ รปภ.ของอาคารมาลีนนท์ ที่ สน. ทองหล่อ ว่าถูกคนร้ายใช้กลอุบายหลอกลวงด้วยการโทรศัพท์มาแจ้งว่าได้รับรางวัลใหญ่เป็นเงินสดมูลค่ากว่าหนึ่งแสนบาท แล้วหลอกให้ไปตรวจสอบยอดเงินจากบัตรเอทีเอ็ม แต่ต้องสูญเงินในบัญชีทั้งหมดเป็นเงินกว่า 32,000 บาท ชุดสืบสวนจึงได้ติดตามเก็บหลักฐานจนสืบทราบว่า เงินของนายชัยยุทธ ผู้เสียหายถูกโอนไปที่บัญชีของธนาคารกรุงเทพ สาขาย่อยเดอะมอลล์บางแค เลขที่บัญชี 2384225153 ชื่อเจ้าของบัญชี คือ นายศักดิ์ชัย แจ้มกระจ่าง ทางตำรวจจึงเชิญตัวมาสอบปากคำ นายศักดิ์ชัยอ้างว่ามีเพื่อนที่เป็นรปภ. ชื่อ นายอนิรุทต์ มาว่าจ้างให้เปิดบัญชีและนำสมุดบัญชีพร้อมกับบัตรเอทีเอ็มกลับไปด้วย เมื่อสืบสวนขยายผลไปเรื่อย ๆ ทางตำรวจจึงทราบว่ามีนายอนุรักษ์และนายนัทธี รวมถึงนายพรรษาน่าจะมีส่วนเกี่ยวข้องด้วย จึงเชิญตัวผู้ต้องหาทั้งหมดมาสอบปากคำและแจ้งข้อกล่าวหาดังกล่าว

รูปที่ 11.13 การจับกุมนายพรรษา พัวพันธ์ (42 ปี)
หัวหน้ากลุ่มคนร้ายหลอกต้มตุ๋นกดเอทีเอ็ม

ชุดสืบสวนได้นำหมายค้นศาลอาญากรุงเทพใต้ เข้าตรวจค้นบริษัทจัดหางานชื่อ บริษัทโคราช เอสเอส เซอร์วิส จำกัด เลขที่ 100/40 ตลาดเสริมเพิ่มพูน ซอยเปรมประชา ถนนวิภาวดีรังสิต แขวงสีกัน เขตดอนเมือง กทม. และจากการเข้าตรวจค้นโต๊ะทำงานของนายพรรษา ซึ่งทำงานเป็นพนักงานในบริษัทดังกล่าว พบสมุดบัญชีธนาคารต่าง ๆ โดยมีชื่อของนายพรรษาเป็นเจ้าของบัญชีรวม 17 เล่ม สมุดบัญชีธนาคารของผู้อื่นอีก 18 เล่ม พร้อมบัตรเอทีเอ็มอีกจำนวนหนึ่ง ก่อนจะยึดเป็นของกลางมาตรวจสอบ รวมทั้งชิ้นส่วนหน่วยความจำของเครื่องคอมพิวเตอร์บนโต๊ะทำงานของนายพรรษาด้วย

รายงานข่าวกล่าวถึงวิธีการของคนร้ายกลุ่มนี้ว่า คนร้ายจะสุ่มหมายเลขโทรศัพท์ของผู้เสียหายแล้วโทรศัพท์ผ่านทางอินเทอร์เน็ต เมื่อผู้เสียหายรับสายก็จะใช้โปรแกรมดัดแปลงเสียงให้กลายเป็นเสียงผู้หญิงหรือเสียงคนแก่ ออกอุบายว่าหมายเลขโทรศัพท์ของผู้เสียหายเป็นหมายเลขที่ถูกรางวัลเป็นเงินสดจำนวนมาก จากนั้นจะเกลี้ยกล่อมให้ผู้เสียหายเอาบัตรเอทีเอ็มไปตรวจสอบว่าได้รับเงินรางวัลหรือยัง โดยให้กดเลือกรายการแบบเป็นภาษาอังกฤษพร้อมออกคำสั่งให้กดหมายเลขต่าง ๆ อ้างว่าเป็นรหัสผ่านเพื่อตรวจสอบว่าเงินเข้าไปในบัญชีของผู้เสียหายหรือยัง โดยเลขต่าง ๆ ที่หลอกให้กดไปนั้น แท้ที่จริงแล้วคือหมายเลขบัญชีของคนร้ายและจำนวนเงินที่กดดูนั้นคือจำนวนเงินที่โอนไปให้คนร้ายนั่นเอง สำหรับกลุ่มผู้ต้องหากลุ่มนี้ ทางตำรวจเชื่อว่าจะมีนายพรรษาเป็นหัวหน้ากลุ่มโดยใช้วิธีการว่าจ้างบุคคลอื่นให้เปิดบัญชีฝากกันเป็นทอด ๆ

แต่นายพรรษาให้การปฏิเสธ โดยอ้างว่ามีนายเฉิน ไม่ทราบนามสกุล ชาวไต้หวัน เป็นผู้ว่าจ้างให้กระทำความผิดดังกล่าว แต่ทางตำรวจไม่ปักใจเชื่อ เพราะเมื่อตรวจสอบเส้นทางของเงินผู้เสียหาย ส่วนใหญ่ปลายทางจะมาสุดที่นายพรรษา นอกจากนี้ ยังมีพยานระบุว่า นายพรรษาเคยว่าจ้างให้ไปกดเงินที่ตู้เอทีเอ็มแห่งหนึ่ง โดยจะแบ่งเงินให้คิดเป็นร้อยละ 7 ของจำนวนเงินทั้งหมดที่กดมา แต่มีข้อแม้ว่าต้องสวมหมวกอำพรางใบหน้าไม่ให้กล้องโทรทัศน์วงจรปิดจับภาพได้ หลังจากการสืบสวนสอบสวนทั้งหมดแล้ว เจ้าหน้าที่ตำรวจนำตัวผู้ต้องหาทั้งหมดพร้อมของกลางส่ง พ.ต.ท. คงเดช สายยางหล่อ พงส. (สบ3) สน.ทองหล่อ ดำเนินคดีต่อไป [32]

11.2.7 กลวิธีของคนร้ายในการขโมยข้อมูลจากบัตรเครดิต

หากสังเกตเครื่องเอทีเอ็มที่ประสบปัญหาการถูกขโมยข้อมูลบัตรเครดิตส่วนใหญ่แล้วจะพบว่า เครื่องเอทีเอ็มจะมีลักษณะแตกต่างไปจากเครื่องเอทีเอ็มปกติ ดังแสดงในรูปที่ 11.14 กล่าวคือจะมีลักษณะของที่เสียบบัตรยื่นออกมาจากตัวเครื่องเยอะเกินไป โดยคนร้ายจะนำเครื่องอ่านข้อมูลซ่อนไว้ในชิ้นส่วนที่ทำเตรียมไว้แล้วนำไปติดตั้งเสริมเข้าไปในเครื่องเอทีเอ็ม โดยจะมีช่องให้สอดบัตรตามปกติ แต่จะมีข้อสังเกตว่าเมื่อเสียบบัตรเข้าไปในเครื่องเอทีเอ็มที่มีการติดตั้งเครื่องอ่านข้อมูลนั้น บัตรจะรู้สึกแน่นกว่าปกติ และเวลาที่เครื่องคืนบัตรออกมาจะผิดไปจากที่เคยเป็น เพราะมีเครื่องอ่านข้อมูลแอบซ่อนอยู่ในช่องเสียบบัตรอยู่ก่อนแล้ว

รูปที่ 11.14 ลักษณะของเครื่องอ่านข้อมูล และการติดตั้งเข้ากับเครื่องเอทีเอ็ม

รูปที่ 11.15 ลักษณะของเครื่องเอทีเอ็ม ที่มีการติดตั้งเครื่องอ่านข้อมูล

ดังแสดงในรูปที่ 11.15 คือหน้าตาของเครื่องเอทีเอ็มที่มีการติดตั้งเครื่องอ่านข้อมูลเสร็จเรียบร้อยแล้ว หากมีผู้ที่ไม่รู้หลงมาใช้เครื่องเอทีเอ็มตู้นี้ ข้อมูลของผู้ใช้ก็จะถูกคัดลอกไว้ในแผ่นแม่เหล็กที่อยู่ในเครื่องอ่านข้อมูล และรอเวลาให้คนร้ายมาถอดเอาชิ้นส่วนนี้ออกไปทำการถ่ายโอนข้อมูลลงไปในบัตรเปล่า ๆ ซึ่งมีราคาไม่แพง และหาซื้อได้ง่าย ดังนั้น หากจะเข้าไปกดเงินตามเครื่องเอทีเอ็มควรจะสังเกตให้ดีว่าเครื่องที่จะกดนั้นผิดปกติอะไรหรือไม่ บัตรที่เสียบเข้าไปแน่นเกินไปหรือไม่ หากผิดสังเกตก็ให้เปลี่ยนเครื่องเอทีเอ็มดีกว่า

หลายท่านอาจสงสัยว่า เมื่อคนร้ายได้ข้อมูลไปแล้ว หากไม่รู้รหัสผ่านของบัตรเครดิต คนร้ายก็ไม่สามารถลักลอบกดเงินออกมาได้แล้ว แต่หารู้ไม่ว่า คนร้ายพวกนี้ฉลาดแกมโกงมากกว่าที่เราจะคาดคิดได้ คนร้ายจะทำการขโมยรหัสผ่านของเราโดยที่เราเองอาจจะไม่รู้ตัวด้วยซ้ำ หากสังเกตเครื่องเอทีเอ็มที่ผิดปกติจะพบกับกล่องที่ใส่โฆษณาข้าง ๆ ตู้ ดังแสดงในรูปที่ 11.16

รูปที่ 11.16 กล่องที่ใส่โฆษณาข้าง ๆ ตู้เอทีเอ็ม ที่คนร้ายอาจจะซ่อนกล้องไว้ข้างใน

รูปที่ 11.17 ภายในของกล้องที่แอบซ่อน เพื่อดูรหัสผ่านของผู้ที่มากดเงินที่เครื่องเอทีเอ็ม

กล่องใส่โฆษณาดังกล่าวอาจจะถูกดัดแปลงจากคนร้ายให้ซ่อนกล้องขนาดเล็กแบบไร้สายไว้ด้านใน เพื่อลักลอบดูรหัสผ่านจากคนที่มากดเงินจากเครื่องเอทีเอ็ม ภายในกล้องไร้สายนั้นจะมีแบตเตอรี่ไว้คอยจ่ายไฟเพื่อที่จะได้สามารถเฝ้าติดตามดูคนที่มากดเงินที่เครื่องได้ตลอดทั้งวัน ดังแสดงในรูปที่ 11.17 กล้องชนิดนี้จะมีรัศมีการส่งประมาณ 100-200 เมตร ซึ่งมีราคาไม่สูงมากนัก [7]

11.3 ข้อปฏิบัติในการเก็บรักษาบัตรและข้อมูลในบัตรเครดิตและบัตรเอทีเอ็ม

การทุจริตผ่านบัตรเครดิตสามารถกระทำได้หลายรูปแบบ อาทิ การลักลอบคัดลอกข้อมูลในบัตรเครดิตโดยคนร้ายอาจจะแอบคัดลอกข้อมูลส่วนตัวที่เก็บบันทึกไว้ในแถบแม่เหล็กโดยใช้อุปกรณ์ล้ำสมัย จากนั้นจึงถ่ายโอนข้อมูลเหล่านั้นลงบนบัตรปลอมที่ทำขึ้นมา แล้วนำบัตรนั้นไปใช้ซื้อสินค้าเสมือนเป็นเจ้าของบัตร

ตัวจริง นอกจากนี้ มิจฉาชีพบางรายอาจจะมุ่งความสำคัญไปที่เครื่องเอทีเอ็มเพื่อลักลอบขโมยข้อมูลบัตรเอทีเอ็ม โดยแอบดูรหัสของผู้ใช้บัตรผ่านกล้องตัวเล็กที่แอบติดตั้งไว้ตามเครื่องเอทีเอ็ม

ด้วยเหตุนี้ ผู้ใช้บัตรเครดิตจึงควรเก็บรักษาบัตรเช่นเดียวกับที่เก็บรักษาเงินสด ซึ่งมีข้อควรปฏิบัติ ดังนี้

11.3.1 ทันทีที่ได้รับบัตรใหม่

- เซ็นชื่อลงบนแถบแม่เหล็กทันที
- จดหมายเลขบัตรเครดิตและหมายเลขโทรศัพท์สำหรับแจ้งบัตรหาย และเก็บไว้ในที่ที่ปลอดภัย และหาได้ง่ายในยามฉุกเฉิน
- ไม่ควรตั้งรหัสบัตรเอทีเอ็มโดยใช้ข้อมูลส่วนตัวที่สามารถคาดเดาได้ง่าย อาทิ ชื่อ หมายเลขโทรศัพท์ วันเดือนปีเกิด เป็นต้น
- ควรจำรหัสบัตรเครดิตให้ได้ หากจำเป็นต้องจดรหัสก็ไม่ควรเก็บไว้ในกระเป๋าเงิน กระเป๋าถือ หรือเก็บไว้ที่เดียวกับบัตรเครดิต
- ไม่ควรบอกรหัสบัตรให้บุคคลอื่นทราบ

11.3.2 เมื่อใช้บัตรเครดิต

- โทรแจ้งธนาคารที่ออกบัตรทันทีที่บัตรสูญหาย เพื่อทำการระงับการใช้บัตรนั้น และแจ้งความที่สถานีตำรวจและเก็บหลักฐานการแจ้งความไว้เป็นหลักฐาน
- ก่อนเซ็นชื่อลงบนสลิป ควรตรวจสอบจำนวนเงินว่าตรงกับราคาของสินค้าและบริการให้ถูกต้อง เพื่อป้องกันไม่ให้ผู้อื่นนำข้อมูลในสลิปไปใช้ในทางที่มิชอบและเก็บสลิปไว้เพื่อตรวจสอบความถูกต้องในภายหลังอีกครั้ง
- ตรวจสอบยอดค่าใช้จ่ายในใบแจ้งบัญชีบัตรเครดิตประจำเดือนว่ามีจำนวนเงินตรงกับที่ใช้ไปหรือไม่ โดยเฉพาะอย่างยิ่งเมื่อกลับมาจากเดินทางไปต่างประเทศ
- ไม่ควรบอกหมายเลขบัตรเครดิตแก่บุคคลอื่นทางโทรศัพท์ นอกจากว่ากำลังติดต่อกับองค์กรที่มีความน่าเชื่อถือหรือเป็นฝ่ายเริ่มการติดต่อด้วยตัวเอง
- หากมีความจำเป็นต้องบอกหมายเลขบัตรเครดิตผ่านทางโทรศัพท์ ต้องตรวจสอบให้แน่ใจว่าการติดต่อนั้นมาจากบริษัทที่ไว้ใจได้ และขอเอกสารยืนยันการซื้อขายที่เป็นลายลักษณ์อักษรจากพนักงานขายทุกครั้ง
- พยายามชำระสินค้าที่ใช้บัตรเครดิตด้วยตัวเอง อย่าให้พนักงานนำบัตรไปในที่ที่มองไม่เห็น
- หลีกเลี่ยงการใช้เครื่องเอทีเอ็มในที่เปลี่ยว หรือมีลักษณะที่ผิดปกติ ขณะใช้บริการเอทีเอ็มควรสำรวจรอบ ๆ ตัว เพื่อสังเกตพฤติกรรมต้องสงสัยของคนที่ยืนอยู่ข้างหลัง และเพื่อป้องกันไม่ให้คนที่ยืนอยู่ข้างหลังแอบมองรหัสบัตรเอทีเอ็ม
- ติดตั้งระบบรักษาความปลอดภัยพร้อมด้วยซอฟต์แวร์ที่ป้องกันไวรัสของเครื่องคอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน เพื่อป้องกันการโจรกรรมข้อมูล
- ซื้อสินค้าและบริการแบบออนไลน์จากเว็บที่มีชื่อเสียงและเชื่อถือได้เท่านั้น
- ใช้รหัสผ่านยาว ๆ เพื่อคุ้มครองข้อมูลบัญชีธนาคารและบัญชีการซื้อสินค้าผ่านทางอินเทอร์เน็ต [20]

11.4 การเงินผ่านอินเทอร์เน็ต

อีแบงค์กิ้งหรือบริการธนาคารอิเล็กทรอนิกส์เป็นการนำคอมพิวเตอร์เข้ามามีส่วนร่วมในการทำงานจากเดิมที่ใช้คนเป็นหลักในการปฏิบัติงานในทุก ๆ ด้าน ดังต่อไปนี้

11.4.1 การใช้คอมพิวเตอร์ด้านการฝากถอนเงิน ถือเป็นจุดเปลี่ยนแปลงจากบริการด้านการเงินของธนาคารแบบเดิม คือ เมื่อลูกค้าต้องการฝาก-ถอนเงิน ลูกค้าจะต้องเดินทางไปฝาก-ถอนเงิน ณ ที่ทำการธนาคาร มาเป็นการให้บริการรูปแบบใหม่ คือ ธนาคารนำคอมพิวเตอร์เข้ามาช่วยในการฝาก-ถอนเงิน ทำให้ลูกค้าสามารถใช้บริการฝาก-ถอนเงิน ณ สาขาใดของธนาคารนั้นก็ได้ นอกจากนี้พนักงานของธนาคารเองก็สามารถใช้คอมพิวเตอร์นำยอดเงินเข้าบัญชีในกรณีฝากเงินและตัดบัญชีในกรณีถอนเงินต่างสาขาได้ในทันที การฝาก-ถอนเงินสดถือเป็นบริการประเภทเดียวที่ไม่สามารถให้บริการผ่านทางเว็บได้ แต่ถ้าฝากเงินโดยโอนเงินจากบัญชีอื่นหรือถอนเงินโดยส่งไปเข้าบัญชีอื่นก็ทำผ่านเว็บได้ทันที ในปัจจุบันลูกค้าสามารถฝากเงินผ่านเครื่องรับฝากเงินและสามารถถอนเงินผ่านเครื่องถอนเงินได้แล้ว

11.4.2 การใช้คอมพิวเตอร์ช่วยตรวจสอบหรือสอบถามยอดบัญชี เป็นบริการที่ลูกค้าสามารถใช้บริการผ่านทางเว็บของธนาคารโดยที่ธนาคารจะใช้หมายเลขบัญชีเป็นเลขประจำตัวผู้ขอรับบริการและให้ผู้ขอรับบริการเป็นผู้กำหนดรหัสผ่านด้วยตนเอง ลูกค้าหรือผู้ใช้บริการสามารถตรวจสอบรายการเดินบัญชีย้อนหลังและสามารถตรวจสอบข้อมูลการใช้บัตรเครดิตได้ด้วย

11.4.3 การใช้คอมพิวเตอร์ให้บริการโอนเงินภายในประเทศและระหว่างประเทศ มีหลายแบบดังต่อไปนี้

- การโอนเงินระหว่างบัญชี เป็นการโอนเงินระหว่างบัญชีของเจ้าของบัญชีคนเดียวกันผ่านทางอินเทอร์เน็ต ผู้ใช้บริการต้องไปลงทะเบียนกับทางเว็บของธนาคารก่อนโดยการใช้งานใช้ได้อย่างจำกัด อาทิ ผู้ใช้บริการหนึ่งคนสามารถเปิดบัญชีได้ไม่เกิน 6 บัญชีในวงเงินไม่เกิน 500,000 บาทต่อวันซึ่ง เงื่อนไขต่าง ๆ ขึ้นอยู่กับธนาคารผู้ให้บริการ เป็นต้น
- การโอนเงินไปบัญชีบุคคลอื่น เป็นการโอนเงินผ่านทางอินเทอร์เน็ตเช่นเดียวกับการโอนเงินระหว่างบัญชี จะแตกต่างกันตรงที่ผู้ใช้บริการมีความต้องการที่จะโอนเงินไปเข้าบัญชีบุคคลอื่นแทนที่จะโอนเข้าบัญชีตัวเอง ในบริการนี้ผู้ใช้บริการต้องไปลงทะเบียนกับทางเว็บของธนาคารก่อนโดยผู้ใช้บริการสามารถเป็นเจ้าของบัญชีได้ไม่เกิน 10 บัญชีในวงเงินไม่เกิน 50,000 บาทต่อบัญชีต่อวันแต่ถ้าหากผู้ใช้บริการมีความจำเป็นที่จะต้องใช้เงินเพิ่มก็สามารถขออนุมัติเพิ่มวงเงินได้แต่ก็ไม่เกิน 500,000 บาทต่อบัญชีต่อวันขึ้นอยู่กับธนาคารผู้ให้บริการด้วย
- การโอนเงินไปต่างประเทศผ่านทางคอมพิวเตอร์มีบริการหลายอย่าง เช่น บริการโอนเงินไปต่างประเทศเพื่อการศึกษา บริการโอนเงินไปต่างเทศจากนักท่องเที่ยวหรือชาวต่างชาติที่อยู่ในประเทศไทยแต่ต้องการโอนเงินกลับไปประเทศของตัวเอง เป็นต้น ผู้ใช้สามารถใช้บริการนี้ได้ในเวลาทำการปกติของธนาคาร คือ 8.30-16.30 น. ถึงแม้ว่าจะเป็นการโอนเงินผ่านทางอินเทอร์เน็ตก็ตาม แต่ถ้าลูกค้าทำการโอนเงินหลังจากเวลาทำการไปแล้วระบบจะเก็บข้อมูลเอาไว้แล้วจะทำรายการโอนเงินให้ในวันทำการถัดไป ส่วนอัตราแลกเปลี่ยนที่ใช้โอนจะเป็นอัตราที่ธนาคารประกาศไว้ ณ ขณะนั้นซึ่งผู้ใช้บริการสามารถตรวจสอบได้ผ่านทางคอมพิวเตอร์ มีค่าธรรมเนียมในการโอนครั้งละ 300 บาทซึ่งจะหักจากบัญชีโดยอัตโนมัติ

11.4.4 การอายัดเช็คผ่านคอมพิวเตอร์ ผู้ใช้สามารถทำได้โดยระบุหมายเลขเช็คและจำนวนเงินที่สั่งจ่ายซึ่งบริการนี้จะมีผลทันทีที่กดยืนยันการอายัด

11.4.5 การชำระค่าสินค้าและบริการต่าง ๆ ผ่านทางคอมพิวเตอร์หรือการชำระเงินออนไลน์นั่นเอง เป็นการให้บริการที่ช่วยเพิ่มความสะดวกสบายให้ลูกค้าเป็นอย่างมากซึ่งจากเดิมลูกค้าต้องไปใช้บริการที่ธนาคารแต่ปัจจุบันลูกค้าสามารถใช้บริการผ่านคอมพิวเตอร์ได้แล้วแถมยังมีบริการเสริมอีกหลายอย่างให้บริการอีกด้วย การชำระเงินออนไลน์มีหลายแบบดังตัวอย่างต่อไปนี้

- การชำระเงินแบบเงินออนไลน์แบบเงินสดดิจิทัล (Digital Cash) เป็นการนำข้อมูลดิจิทัลมาใช้แทนเงินสดซึ่งเหมาะสำหรับการซื้อขายที่มีมูลค่าน้อยและเหมาะสำหรับการซื้อขายที่สามารถรับสินค้าบนอินเทอร์เน็ตได้ทันที เช่น การซื้อขายข่าวสารหรือซอฟต์แวร์ เป็นต้น ทุกครั้งที่ลูกค้า

ใช้บริการธนาคารจะทำการตรวจสอบจำนวนเงินที่สามารถใช้ได้จริงเพื่อความถูกต้องในการชำระเงินโดยธนาคารจะส่งข้อมูลที่ตรวจสอบได้ไปยังเครื่องพีซีของลูกค้าผ่านทางอินเทอร์เน็ต นอกจากนี้ลูกค้าสามารถปกปิดการซื้อขายโดยใช้ระบบ “ลายเซ็นลับ (Blind Signature)” ซึ่งธนาคารจะไม่เปิดเผยข้อมูลของลูกค้าหากลูกค้าใช้ระบบลายเซ็นลับ

- การชำระเงินโดยใช้อีเช็คหรือเช็คอิเล็กทรอนิกส์ (eCheck) ขั้นตอนการให้บริการเหมือนกับการชำระเงินด้วยเช็คที่เป็นกระดาษ คือ ผู้สั่งจ่ายจะส่งข้อมูลการซื้อสินค้าหรือโอนเงินไปให้ผู้รับเงิน จากนั้นผู้รับเงินส่งข้อมูลไปยังธนาคารแล้วธนาคารจะส่งข้อมูลกลับไปยังผู้จ่ายเพื่อแจ้งการโอนเงิน การโอนเงินโดยใช้เช็คอิเล็กทรอนิกส์มีข้อดีหลายประการ อาทิ สามารถป้องกันการปลอมเช็คได้ระดับหนึ่ง ผู้รับเงินไม่รู้เลขที่บัญชีธนาคารของผู้จ่ายเงิน และร้านค้าไม่รู้เลขที่บัญชีธนาคารของผู้จ่ายเงิน เป็นต้น
- การชำระเงินผ่านบัตรเครดิตบนอินเทอร์เน็ต มีรูปแบบการใช้เช่นเดียวกับบัตรเครดิตที่เป็นพลาสติก คือ เมื่อลูกค้าใช้บัตรเครดิตร้านค้าจะตรวจสอบกับธนาคารว่าข้อมูลของลูกค้าถูกต้องหรือไม่ก่อนที่จะออกใบสลิปเพื่อให้ลูกค้าเก็บเป็นหลักฐานการชำระเงิน ร้านค้าจะนำหลักฐานการจ่ายเงินซื้อสินค้าหรือบริการไปเรียกเก็บจากธนาคารหรือบริษัทบัตรเครดิต

11.4.6 การซื้อสินค้าทางอินเทอร์เน็ต เป็นบริการที่ลูกค้าสามารถเลือกซื้อสินค้าและบริการจากเว็บที่เชื่อมต่อระบบการชำระเงินของธนาคาร เมื่อลูกค้าสั่งซื้อสินค้าหรือบริการผ่านเว็บระบบจะหักบัญชี เป็นค่าสินค้าหรือบริการได้ทันที ข้อดีของการซื้อสินค้าทางอินเทอร์เน็ตมีมากมาย เช่น ลูกค้าสามารถซื้อสินค้าได้วันละ 24 ชั่วโมงทุกวัน ลูกค้าสามารถตรวจสอบรายการสั่งซื้อสินค้าได้ ช่วยลดต้นทุนการรับชำระ ค่าสินค้าและบริการและช่วยเพิ่มช่องทางการซื้อสินค้า เป็นต้น [147]