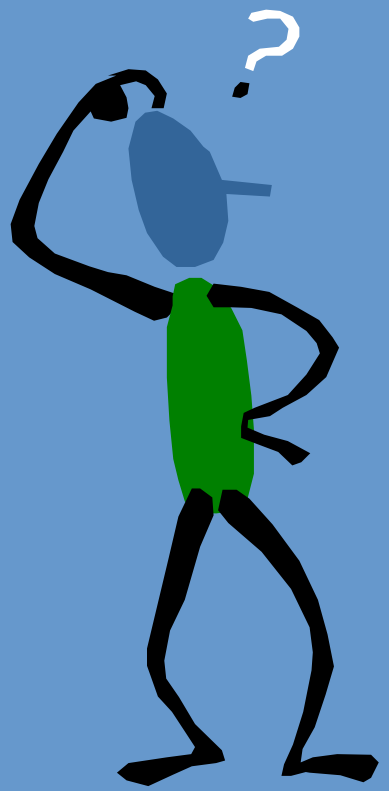
การพาณิชย์อิเล็กทรอนิกส์

บทที่ 7

ระบบการรักษาความปลอดภัย

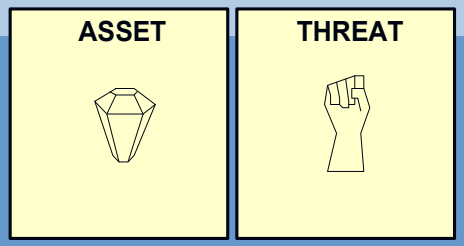
และการเข้ารหัส



ทำไมต้องมีการรักษาความปลอดภัย ???

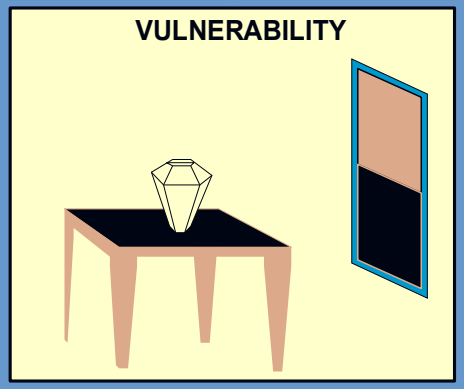
Assets, Threats, Vulnerabilities, Risks, and Protective Measures

ทรัพย์สิน

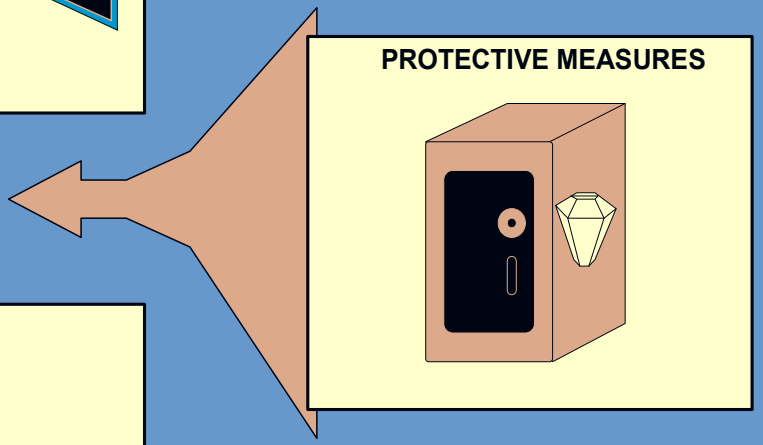


คุกคาม

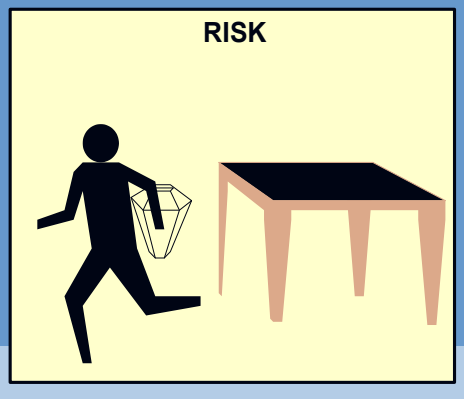
จุดอ่อน



ป้องกัน



ความเสี่ยง



Online Shopping จะไหวเรอะ

???


Important Dates:
This Month's Newsletter
I'm from

การสร้างความเชื่อมั่นในการทำธุรกรรมบน Internet

Cryptography **เป็นกลไกหลักในแต่ละ** Application

General Security Issues at EC

Web Browser

Internet

Web Server

CGI Programs

Server-Side

Scripts, ColFusion ,

Other components

Database

Authentication

ID/Password

Biometric

Privacy/

Integrity

การรหัส

Digital

Signature

Non-Repudiation

Digital Signature

Authentication

Authorization

Audit

Privacy/

Integrity

Barcode

Digital

Signature

หลักการรักษาความปลอดภัยของข้อมูล

1. การระบุตัวบุคคล และอำนาจหน้าที่ (Authentication & Authorization)
2. การรักษาความลับของข้อมูล (confidentiality)
3. การรักษาความถูกต้องของข้อมูล (Integrity)
4. การป้องกันการปฏิเสธ หรืออ้างความรับผิดชอบ (Non-repudiation)
5. สิทธิส่วนบุคคล (Privacy)

1.การระบุตัวบุคคล (Authentication)

- การแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ
- การล็อคซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจเท่านั้น หรือ
- บัตรเข้าออกอาคาร, เจ้าหน้าที่รักษาความปลอดภัย

ป้องกันโดย

- ID + Password
- Biometric (Fingerprint, Face, etc.)
- Encryption การเข้ารหัส
- Digital Signature
- Digital Certificate

การอนุมัติ – อำนาจในการอนุมัติ(Authorization)

- อำนาจในการจ่ายเงิน เช่น วงเงินบัตรเครดิต
- การอนุมัติวงเงินที่จะเรียกเก็บจากธนาคารที่ออกบัตรเครดิต
- ตรวจสอบวงเงินในบัญชีว่ามีเพียงพอไหม ???

2.การรักษาความลับของข้อมูล (Confidentiality)

- การรักษาความลับของข้อมูลที่เก็บไว้ หรือส่งผ่านทางเครือข่าย
- ป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้
- เปรียบเหมือนการปิดผนึกซองจดหมาย หรือ
- การใช้ซองจดหมายที่ทึบแสง หรือ
- การเขียนหมึกที่มองไม่เห็น

ป้องกันโดย การเข้ารหัส, การใช้บาร์โค้ด, การใส่รหัสผ่าน (password), กำแพงไฟ (Firewall)

3.การรักษาความถูกต้องของข้อมูล (Integrity)

- การป้องกันไม่ให้ข้อมูลถูกแก้ไข
- เปรียบเหมือนกับการเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบ
- หรือ การใช้โฮโลแกรมกำกับบนบัตรเครดิต
- หรือ ลายน้ำบนธนบัตร

ป้องกันโดย Digital Signature

4. การป้องกันการปฏิเสธ หรืออ้างความรับผิดชอบ (Non-repudiation)

- การป้องกันการปฏิเสธว่าไม่ได้มีการส่งหรือรับข้อมูลจากฝ่ายต่าง ๆ ที่เกี่ยวข้อง
- การป้องกันการอ้างที่เป็นเท็จว่าได้รับ หรือส่งข้อมูล
- เช่นในการขายสินค้า เราต้องมีการแจ้งให้ลูกค้าทราบถึงขอบเขตของการรับผิดชอบที่มีต่อสินค้า หรือระหว่างการซื้อขาย โดยระบุไว้บน web
- หรือการส่งจดหมายลงทะเบียน

ป้องกันโดย Digital Signature

5. สิทธิส่วนบุคคล (Privacy)

- การรักษาสิทธิส่วนตัวของข้อมูลส่วนตัว
- เพื่อปกป้องข้อมูลจากการลอบดูโดยผู้ที่ไม่มีสิทธิ์ในการใช้ข้อมูล
- ข้อมูลที่ส่งมาถูกดัดแปลงโดยผู้อื่นก่อนถึงเราหรือไม่

ป้องกัน โดยการเข้ารหัส

การเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต

- Passive Unauthorized Access = ลอบฟังข้อมูลที่ส่งผ่านเครือข่าย
- Active Unauthorized Access = คุกคามเพื่อเปลี่ยนแปลง

  - **Hacker**
    - » **white hat hacker**
  - **Cracker**
    - » **black hat hacker**
  - **Script Kiddy**
    - » ไม่เก่งเหมือนแครกเกอร์ แต่สามารถใช้โปรแกรมที่โหลดมาเจาะระบบ

แฮกเกอร์ (Hacker)

- คือ ผู้เชี่ยวชาญที่มีความรู้ความสามารถในการถอดรหัส หรือเจาะระบบรักษาความปลอดภัยเครื่องคอมฯ อื่น โดยมีวัตถุประสงค์
  - ทดสอบความปลอดภัยของระบบ
  - ทดสอบความสามารถของตนเอง

แครกเกอร์ (Cracker)

- คือ ผู้เชี่ยวชาญที่มีความรู้ความสามารถในการถอดรหัส หรือเจาะระบบรักษาความปลอดภัยเครื่องคอมฯ อื่น โดยมีวัตถุประสงค์
  - บุกรุก ทำลายข้อมูลของคู่แข่ง
  - ขโมยข้อมูลจากคู่แข่ง หรือนำไปขายให้กับคู่แข่ง เช่น ด้านการค้า หรือการทหาร ความสนุกสนาน คึกคะนอง

การคุกคาม-การบุกรุก

วิธีการ

- การเข้ามาทำลายเปลี่ยนแปลงหรือขโมยข้อมูล
- ขโมย หลอกลวง โกง (Theft / fraud)
- เปลี่ยนแปลงข้อมูล / ทำให้เสีย (Data alteration / contamination)
- ยักยอก (Misappropriation)
- บริการล่าช้า (Degrading service / delay)
- ข้อมูลสูญหาย ถูกปฏิเสธ (Data loss / denial attack)
- ปลอมตัวเข้ามาใช้ระบบและทำรายการปลอม
- การเข้าถึงระบบเครือข่ายของผู้ไม่มีสิทธิ์

แก้ปัญหาโดย

การเข้ารหัสข้อมูล

ลายเซ็นดิจิตอล

Firewall

ชนิดของการบุกรุกระบบเครือข่าย

1. Non-Technical
2. Technical Use Software and technology
   - Dos Attack = mail bomb
   - DDos Attack
   - Malicious Code
     - Virus
     - Worm
     - Trojan Horse

Spam Mail

DDos

Mail

Mail Bomb

A lot of Mail

Dos A

Malware หรือ Malicious Code

ไวรัส

หนอน (worm)

I LOVE YOU, Mellissa, MyDoom

ม้าโทรจัน (Trojan)

Malware ที่แพร่ระบาดทั่วไป
และเหมือนจะสร้างความ
เสียหายให้กับระบบเศรษฐกิจ
มากที่สุดก็คือ worm

โค้ดอันตราย (Malicious Code)

Malware

- **Malware** ย่อมาจาก Malicious Software หมายถึงโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย หรือเป็นคำที่ใช้เรียกโปรแกรมที่มีจุดประสงค์ร้ายต่อ ระบบคอมพิวเตอร์ทุกชนิดแบบรวมๆ โปรแกรมพวกนี้ก็เช่น virus, worm, trojan, spyware, keylogger, hack tool, dialer, phishing, toolbar, BHO, etc

  แต่เนื่องจาก virus คือ malware ชนิดแรกที่เกิดขึ้นและอยู่มานาน ดังนั้นโดยทั่วไปก็จะใช้คำว่า virus แทนคำว่า malware แต่ถ้าจะคิดถึงความจริงแล้วไม่ถูกต้อง malware แต่ละชนิดไม่เหมือนกัน

ประเภทของไวรัส

1. ไวรัสพาราสิต (Parasitic Virus) เริ่มงานและจำลองตัวเมื่อมีการเรียกใช้งานไฟล์ที่ติดไวรัส
2. ไวรัสบูตเซกเตอร์ (Boot Sector Virus) ฝังตัวเองอยู่ในบูตเซคเตอร์ แทนที่คำสั่งที่ใช้ในการเริ่มต้นการทำงานเครื่องคอมฯ เมื่อเปิดเครื่องคอมฯ ไวรัสนี้จะโหลดตัวเองไปที่หน่วยความจำก่อนที่จะโหลดระบบปฏิบัติการ หลังจากนั้นจะสำเนาตัวเองฝังอยู่กับไฟล์อื่นๆ
3. ไวรัสสเตลท์ (Stealth Virus) สามารถเปลี่ยนแปลงให้อยู่ในรูปแบบที่โปรแกรมป้องกันไวรัสตรวจไม่พบ เมื่อติดกับโปรแกรมได้แล้วจะทำให้โปรแกรมนั้นมีขนาดใหญ่ขึ้นเรื่อย ๆ
4. ไวรัสโพลีมอร์ฟิค (Polymorphic Virus) ไวรัสประเภทนี้มีการเปลี่ยนแปลงตัวเองทุกครั้งที่ติดต่อไปยังเครื่องคอมพิวเตอร์ ซึ่งยากต่อการตรวจสอบ

5. ไวรัสมาโคร (Macro Virus) มีผลกับ Macro Application มักพบในโปรแกรม Word / Excel เมื่อผู้ใช้งานเรียกใช้ไฟล์ที่ติดมา ทำให้ไวรัสฝังตัวเองที่หน่วยความจำทำให้คอมฯ ทำงานช้าลง

6. หนอนอินเทอร์เน็ต (Worms) ติดต่อทางอินเทอร์เน็ต สามารถแพร่กระจายรวดเร็วโดยการคัดลอกตัวเองและใช้เครือข่ายเป็นช่องทางการกระจาย

7. ม้าโทรจัน (Trojan Horse) โครงสร้างไม่เหมือนไวรัสอื่น ๆ โดยสามารถหลบการตรวจจับ และเมื่อเราเรียกใช้โปรแกรมต่าง ๆ ตัวมันเองจะเริ่มทำงานด้วยการดักจับรหัสผ่านต่าง ๆ และส่งกลับไปยังผู้สร้าง

ตัวอย่างไวรัสมาโคร

ความแตกต่างระหว่าง Virus, Worm, Trojan

- Virus = แพร่เชื้อไปติดไฟล์อื่นๆในคอมพิวเตอร์โดยการแนบตัวมันเองเข้าไป มันไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ ต้องอาศัยไฟล์พาหะ สิ่งที่มันทำคือสร้างความเสียหายให้กับไฟล์

- Worm = คัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้อย่างอิสระ โดยอาศัยอีเมล์หรือช่องโหว่ของระบบปฏิบัติการ มักจะไม่แพร่เชื้อไปติดไฟล์อื่น สิ่งที่มันทำคือมักจะสร้างความเสียหายให้กับระบบเครือข่าย

- Trojan = ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ต้องอาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเองหรือด้วยวิธีอื่นๆ สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อ จากระยะไกล ซึ่งจะทำอะไรก็ได้ และโทรจันยังมีอีกหลายชนิด

Malware อื่นๆ

- Spyware = ไม่แพร่เชื้อไปติดไฟล์อื่นๆ ไม่สามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆได้ ต้องอาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเองหรืออาศัยช่องโหว่ของ web browser ในการติดตั้งตัวเองลงในเครื่องเหยื่อ สิ่งที่มันทำคือรบกวนและละเมิดความเป็นส่วนตัวของผู้ใช้ เช่น ส่งโฆษณา pop-up มาให้

- Zombie Network = เครื่องคอมพิวเตอร์จำนวนมากๆ จากทั่วโลกที่ตกเป็นเหยื่อของ worm, trojan และ malware อย่างอื่น ซึ่งจะถูก attacker/hacker ใช้เป็นฐานปฏิบัติการในการส่ง spam mail, phishing, DoS หรือเอาไว้เก็บไฟล์หรือซอฟต์แวร์ที่ผิดกฎหมาย

การหลอกลวงผ่านเน็ต (PHISHING attack)

- การหลอกลวงทางอินเทอร์เน็ตผ่านทาง email ที่ปลอมให้ดูเหมือนว่าถูกส่งมาจากหน่วยงานให้บริการ on-line ที่ดูแล้วน่าจะเชื่อถือได้
- ทำให้แฮกเกอร์ได้ข้อมูล username และ password ของผู้ใช้อย่างง่ายและสามารถที่จะยึด account ของเรา เรียกว่าเป็นการขโมยความ เป็นตัวตนของเราไปเลย (Identity Theft)
- เมื่อแฮกเกอร์ยึด account เราได้ แล้วจะLog-in เป็นตัวของผู้ใช้ใน web site จริง และทำการใช้จ่ายเงินหรือทำธุรกรรมอย่างอื่นเพื่อเป็นประโยชน์แก่แฮกเกอร์ในนามของผู้ใช้

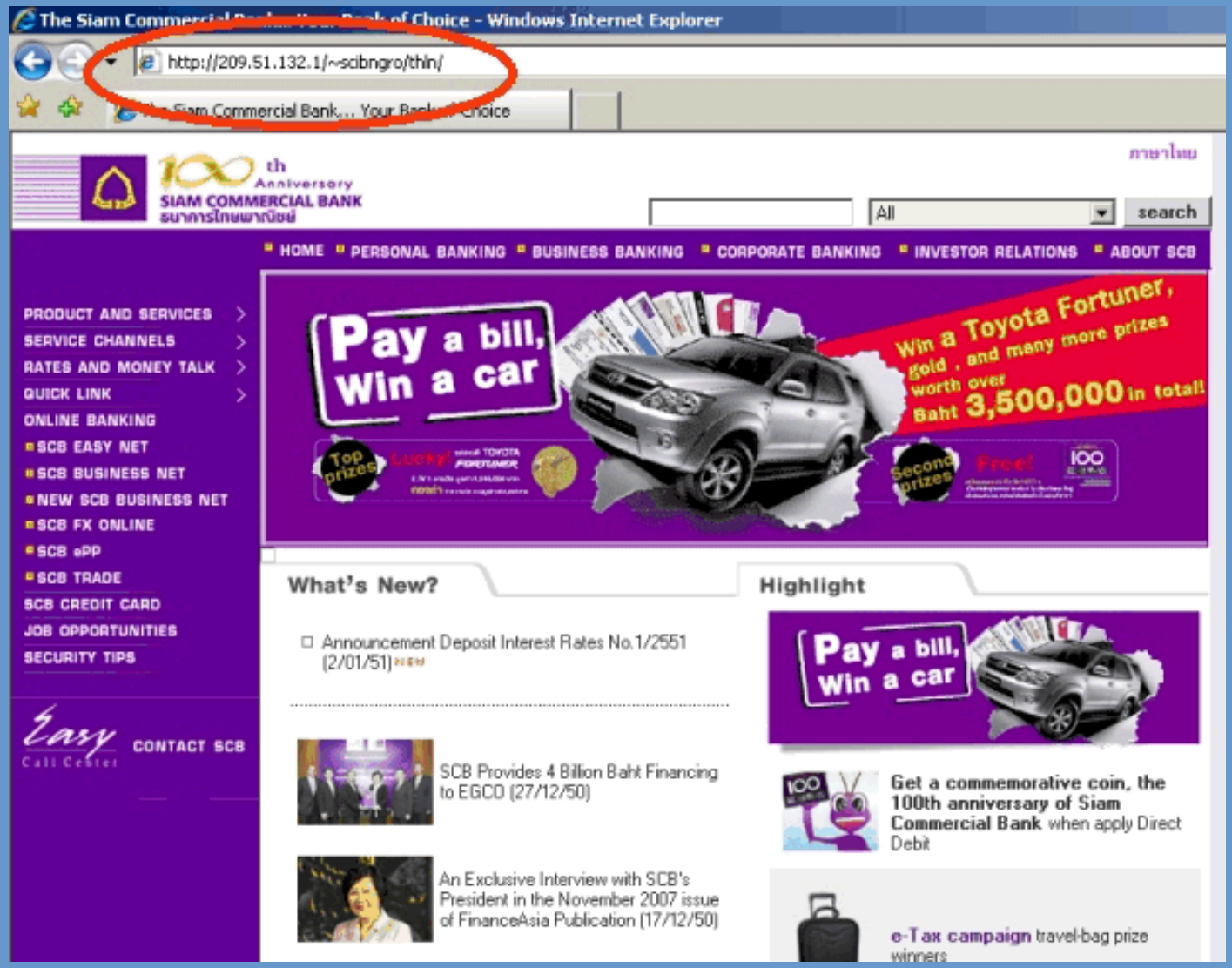
ตัวอย่าง

- เช่น อินเทอร์เน็ตแบงค์กิ้ง
- หรือการซื้อขายของผ่านอินเทอร์เน็ต (ยกตัวอย่างเช่น ebay) เพื่อจะหลอกให้ผู้ใช้บริการหลงเข้าไปใน Web site ที่ถูกจัดทำปลอมขึ้นมาให้ใกล้เคียงของจริงมากถ้าไม่สังเกตให้ดี
- จุดมุ่งหมายของแฮกเกอร์ก็คือหลอกให้เราใส่ username และpassword ในการเข้าระบบ on-line ดังกล่าว

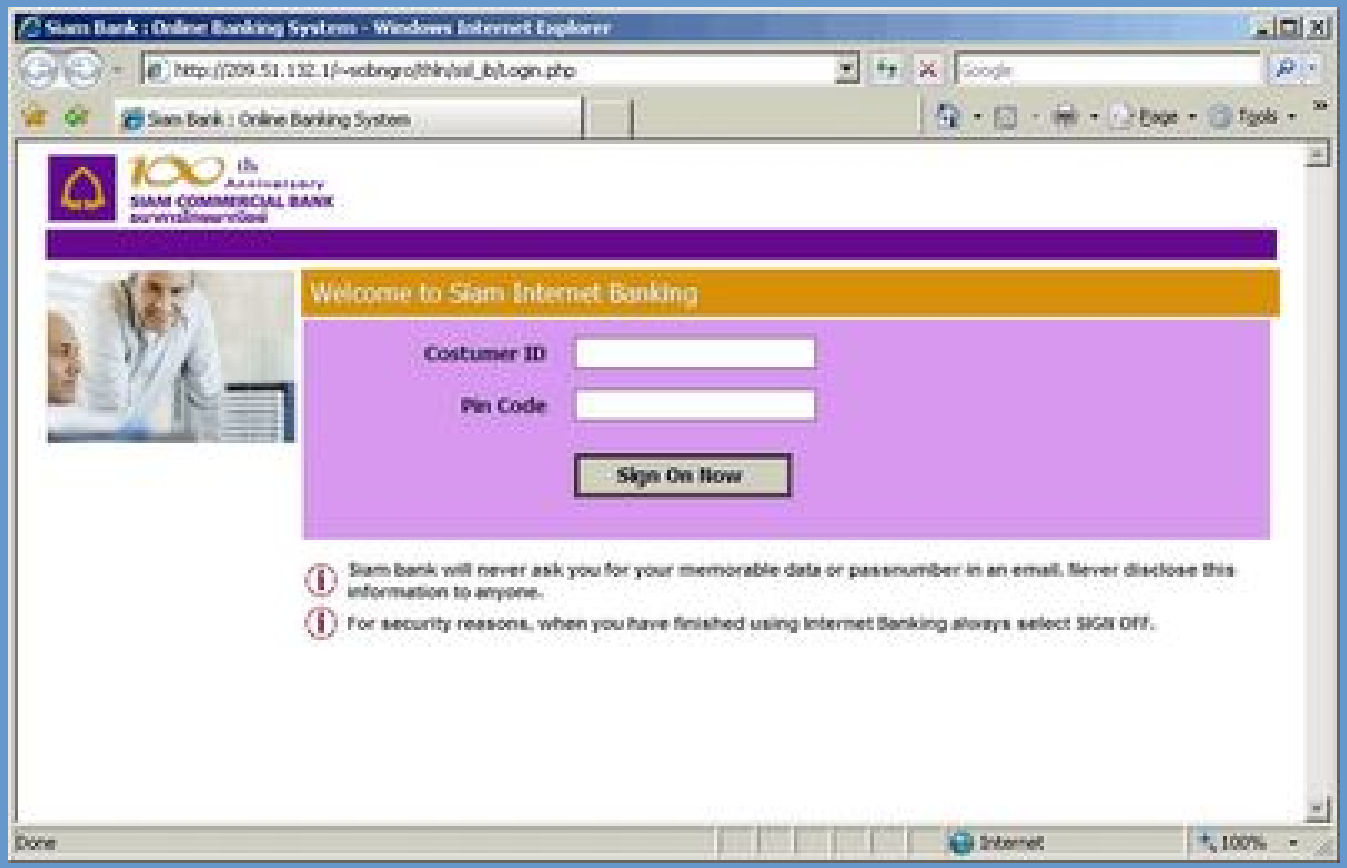
วิธีการแก้ไขปัญหา

- คอยระมัดระวังเรื่องการรับ email คือ ต้องตรวจดูให้ดีเสียก่อนที่จะตกเป็นเหยื่อภัยจากการจู่โจมด้วยวิธี “PHISHING”
- การฝึกอบรม Security Awareness Training ผู้ใช้งานคอมพิวเตอร์ทั่วไปให้มีความรู้ความเข้าใจภัยจาก “PHISHING”

ตัวอย่าง Phishing



ตัวอย่าง Phishing



ตัวอย่าง Phishing: จดหมายแจ้งเตือนจากธนาคาร

ที่ สปทส. 02-510158 5 มีนาคม 2551

เรื่อง แจ้งเตือนเรื่อง Phishing อีเมล์ และ เว็บไซต์ที่ปลอมลูกค้าของธนาคารไทยพาณิชย์

เรียน พนักงานธนาคารทุกท่าน

เนื่องจากสายความปลอดภัยเทคโนโลยีสารสนเทศได้รับแจ้งว่ามีการ ส่ง Email ในลักษณะ Phishing ไปยังกลุ่มลูกค้าของธนาคาร ซึ่งมีเนื้อความล่อลวงให้ลูกค้าของธนาคารเข้าไปทำการ Login เข้าสู่ระบบที่ใช้ชื่อเดียวกับระบบงานบริการลูกค้าของธนาคารหลายๆระบบ โดยกลุ่มผู้ไม่ประสงค์ดีได้ออกเลียนแบบ หน้า Webpage ของธนาคาร(http://www.scb.co.th/ - SCB Web portal) ซึ่งในหน้า webpage เลียนแบบ (http://209.51.132.1/~scibugnx/thai/) จะมี Link ไปยังระบบงานบริการลูกค้าของธนาคาร ซึ่งหากลูกค้าหลงเชื่อใช้ Link จากหน้า Webpage ดังกล่าวระบบจะเชื่อมต่อไปยังหน้า Login ที่ผู้ไม่ประสงค์ดีได้จัดเตรียมเอาไว้ (http://209.51.132.1/~scibugnx/thai/scbl_th/Login.php) โดยมีจุดมุ่งหมายที่จะดักไขมอ User Password ของลูกค้าธนาคารไปใช้งาน โดยไม่ได้รับอนุญาต ซึ่งผู้ไม่ประสงค์ดีได้ดำเนินการส่ง Email ออกไปยัง Internet โดยทั่วไปซึ่งหากลูกค้าหลงเชื่อ และปฏิบัติตาม Email ดังกล่าวข้างต้น ผู้ไม่ประสงค์ดี อาจทราบ User Password ของลูกค้าและสามารถนำไปใช้งาน ซึ่งอาจก่อให้เกิดความเสียหายแก่ลูกค้าและธนาคารได้(รายละเอียดเพิ่มเติมตามเอกสารแนบ)

ดังนั้น สายความปลอดภัยเทคโนโลยีสารสนเทศจึงใคร่ขอแจ้งให้พนักงานทุกท่านรับทราบถึงข้อมูลดังกล่าว เพื่อใช้ประกอบกับการแจ้งเตือนหรือให้ข้อมูลกับลูกค้า เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับลูกค้าของธนาคาร ต่อไป

จึงเรียนมาเพื่อโปรดทราบ

(นายชุติพัฒน์ บันทศิริศรณ์)
ผู้จัดการความปลอดภัยเทคโนโลยีสารสนเทศ
สายความปลอดภัยเทคโนโลยีสารสนเทศ

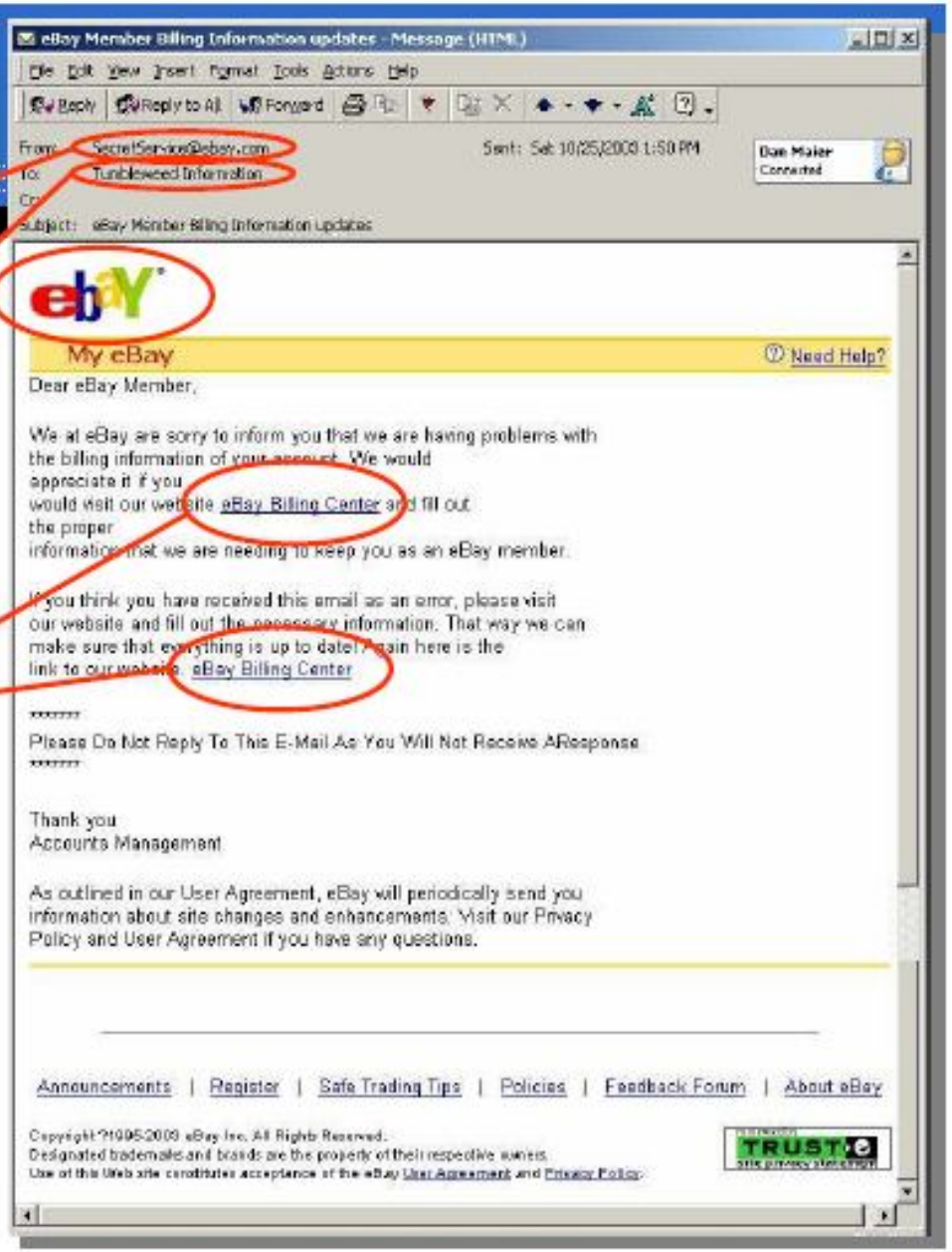
Phishing Attacks

Spoofed Email Address
(SecretService@ebay.com)

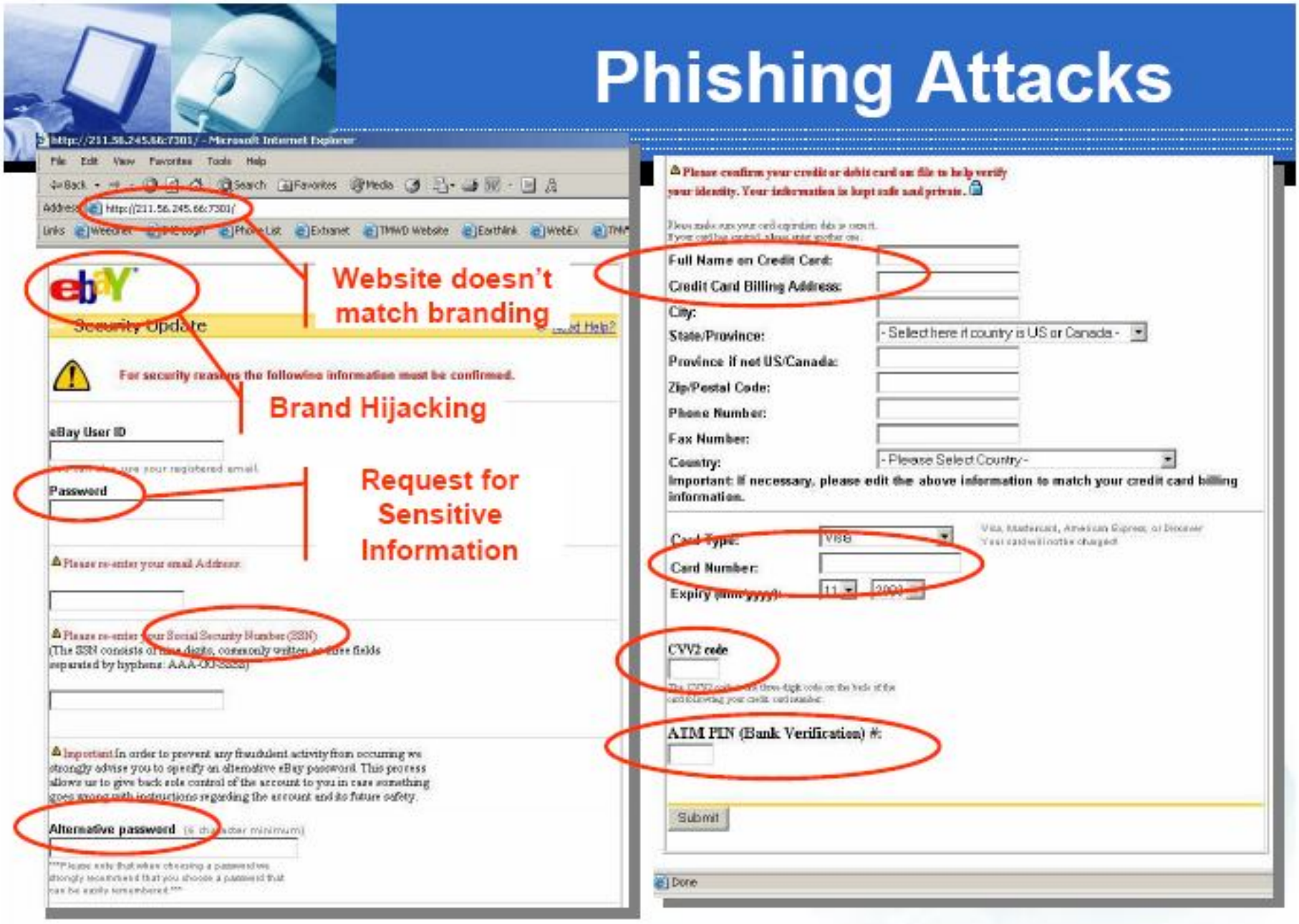
Spam Mass Mailing

Brand Hijacking

Disguised Link to Phisher Site
href="http://www.ebay.com:tkbm6Yjkimgd234d
gdfhfnbjghuiiqrfgfdhgjgtWdfdbhjiuEbnkuod5fEtn
uo3243h*@211.56.245.66:7301/"



Phishing Attacks



บทลงโทษ

กรณี Hack ข้อมูลอย่างเดียว

- จำคุกไม่เกิน 6 เดือน หรือ ปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำและปรับ

กรณี Hack ข้อมูลแล้วเอาไปเผยแพร่

- จำคุกไม่เกิน 1 ปี หรือ ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำและปรับ

มีผลตั้งแต่ 18 กรกฎาคม 2550

กฎหมายไอซีที

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

ผู้ประกาศ สำนักงานปลัดกระทรวง

พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ
- การเปิดเผยข้อมูลมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ
- การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ชอบ
- การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่น
- การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยไม่ชอบ
- การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ
- การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่นโดยปกติสุข
- การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด
- การใช้ระบบคอมพิวเตอร์ทำความผิดอื่น ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด
- การตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล

ความปลอดภัยของการทำธุรกรรมและการสื่อสาร EC (Securing EC Communication)

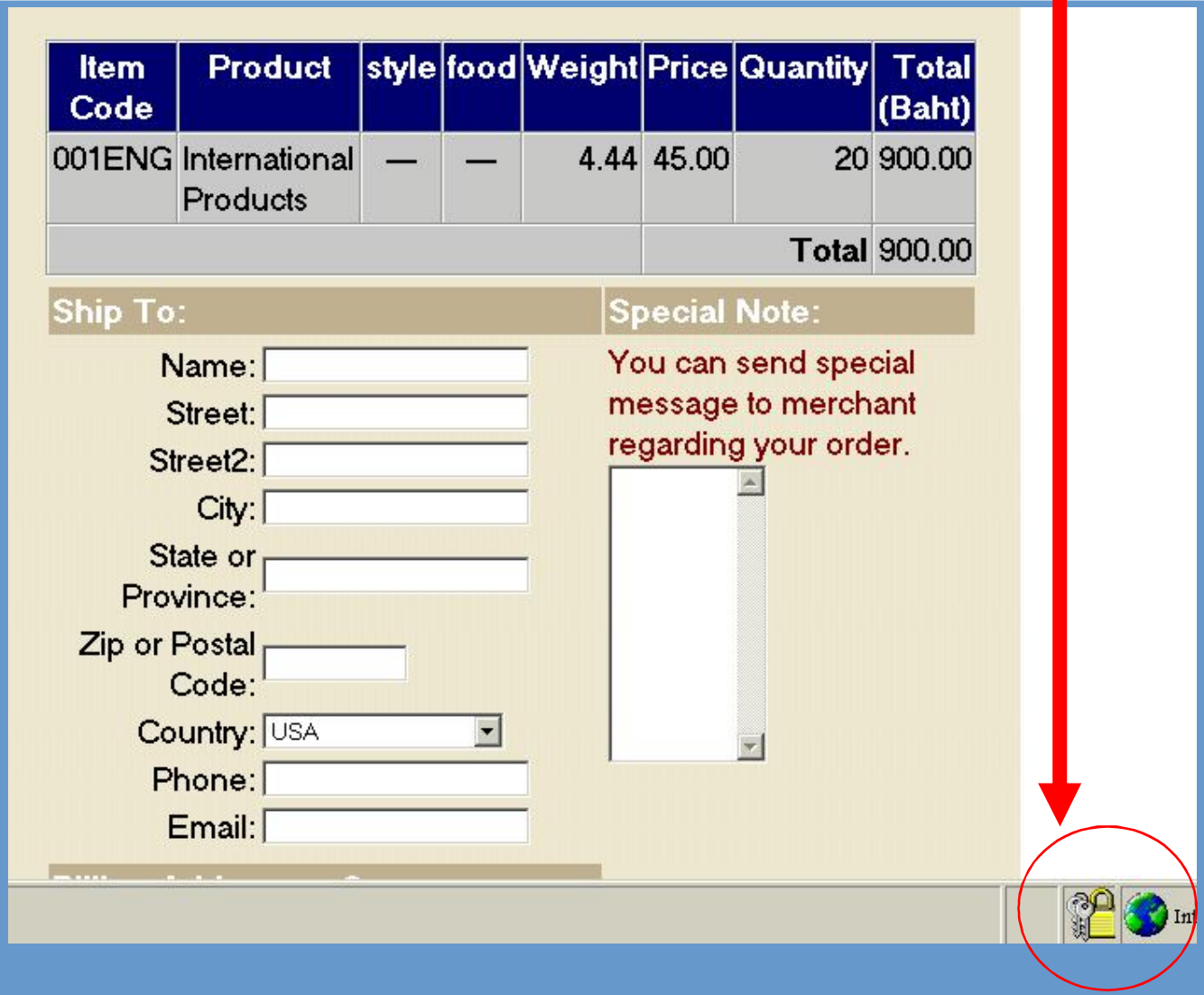
1. การระบุตัวบุคคล

Authentication

- User + Password
- Biometric System
  - Physical
  - Behavior

2. การรหัส (Cryptography)

สัญลักษณ์รูปการทำธุรกรรมที่มีการรักษาความปลอดภัย (PADLOCK)



Item Code	Product	style	food	Weight	Price	Quantity	Total (Baht)
001ENG	International Products	—	—	4.44	45.00	20	900.00
						Total	900.00

Ship To:

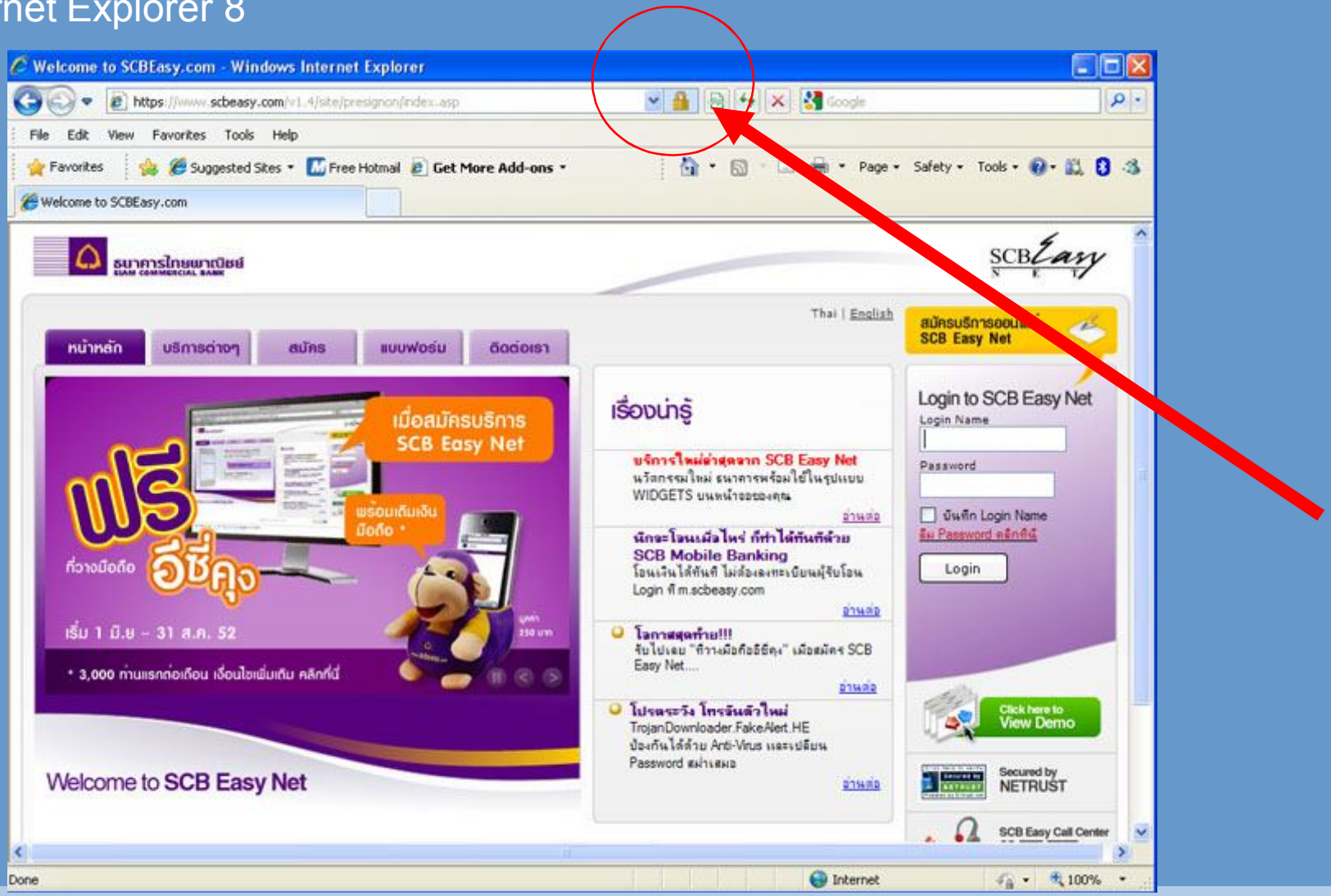
Name:
Street:
Street2:
City:
State or Province:
Zip or Postal Code:
Country: USA
Phone:
Email:

Special Note:

You can send special message to merchant regarding your order.

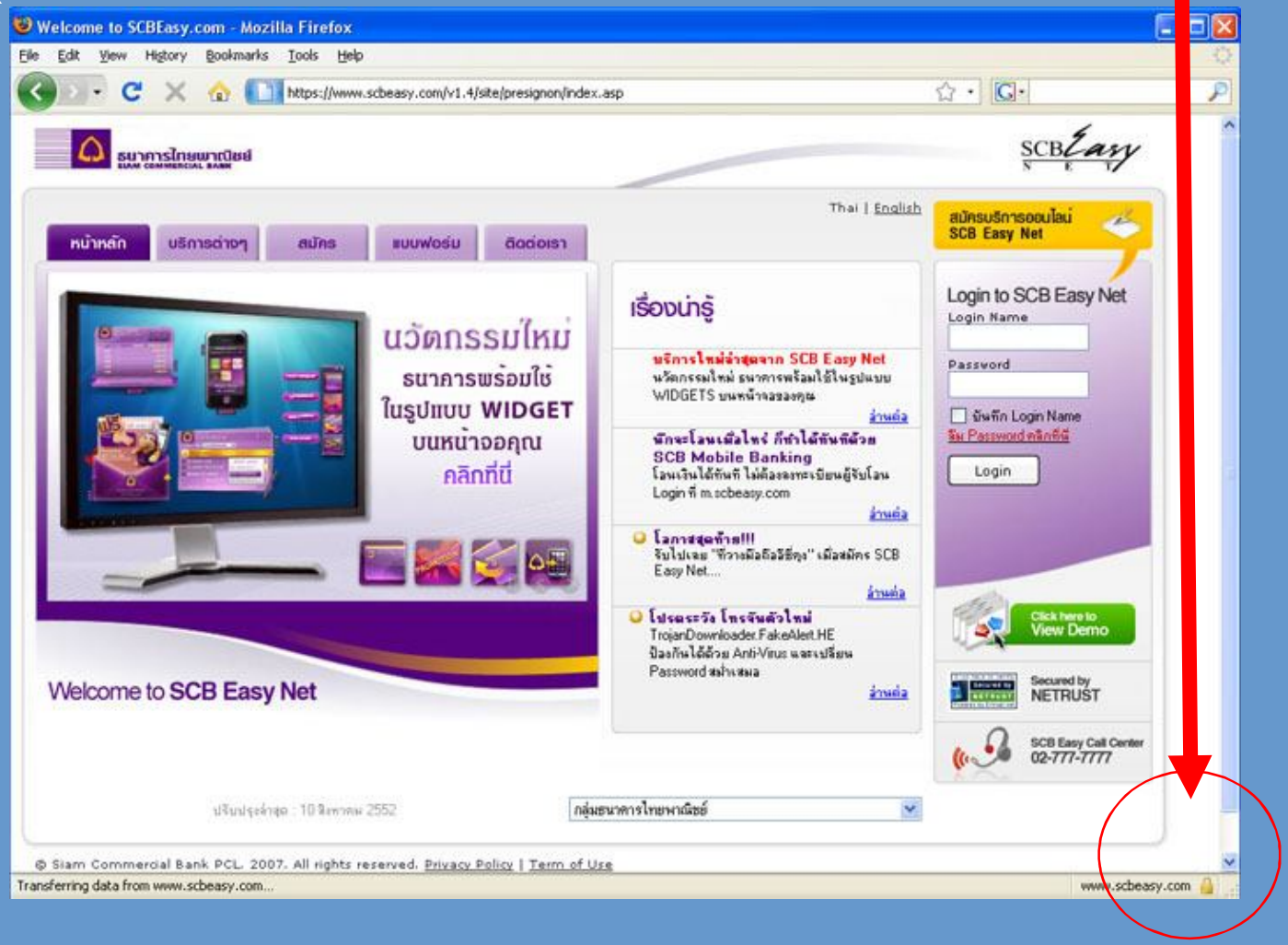
สัญลักษณ์รูปการทำธุรกรรมที่มีการรักษาความปลอดภัย (PADLOCK)

Internet Explorer 8

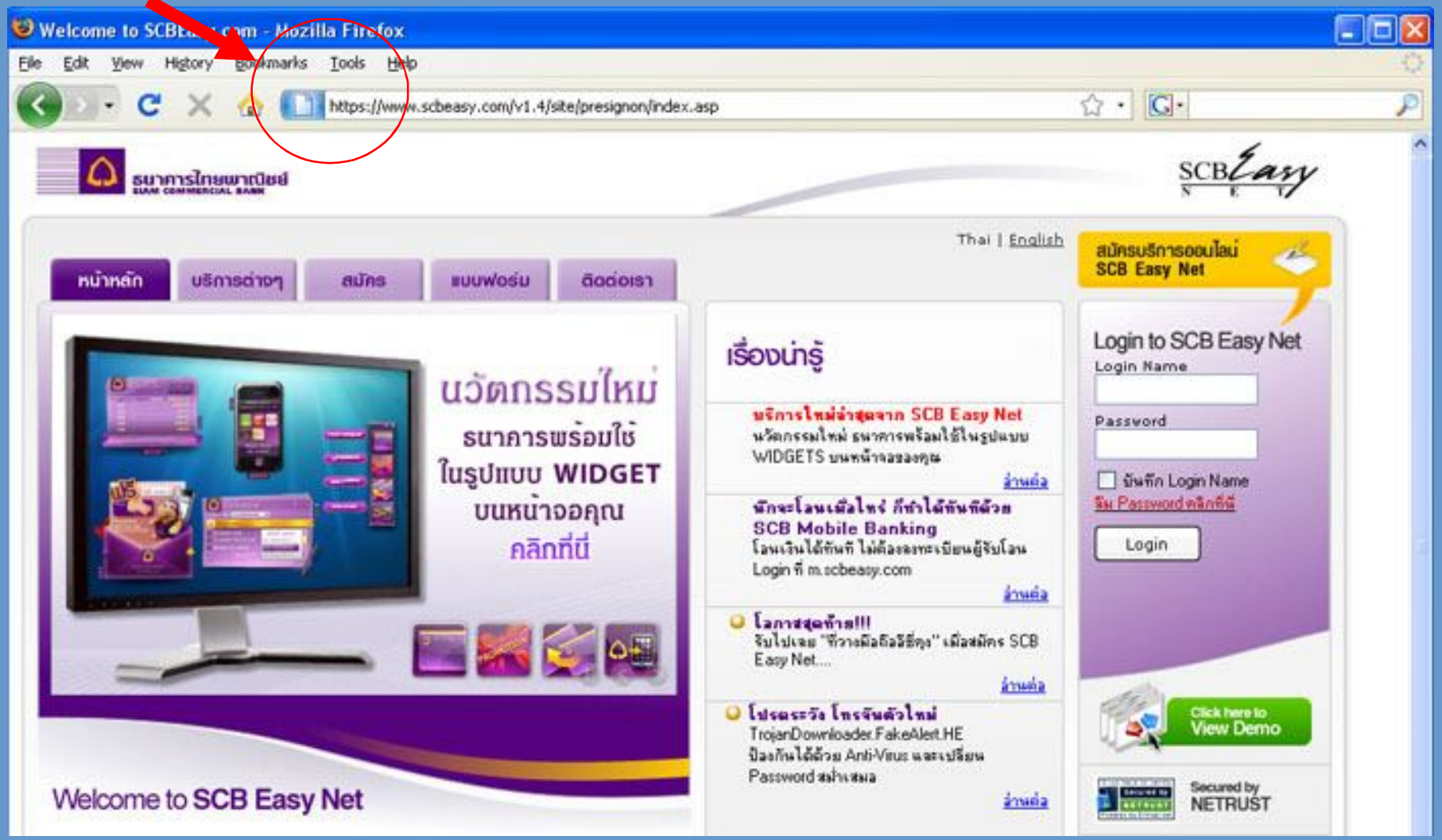


สัญลักษณ์รูปการทำธุรกรรมที่มีการรักษาความปลอดภัย (PADLOCK)

Firefox



- **HTTPS** (HyperText Transmission Protocol, Secure)



การเข้ารหัส (Cryptography)

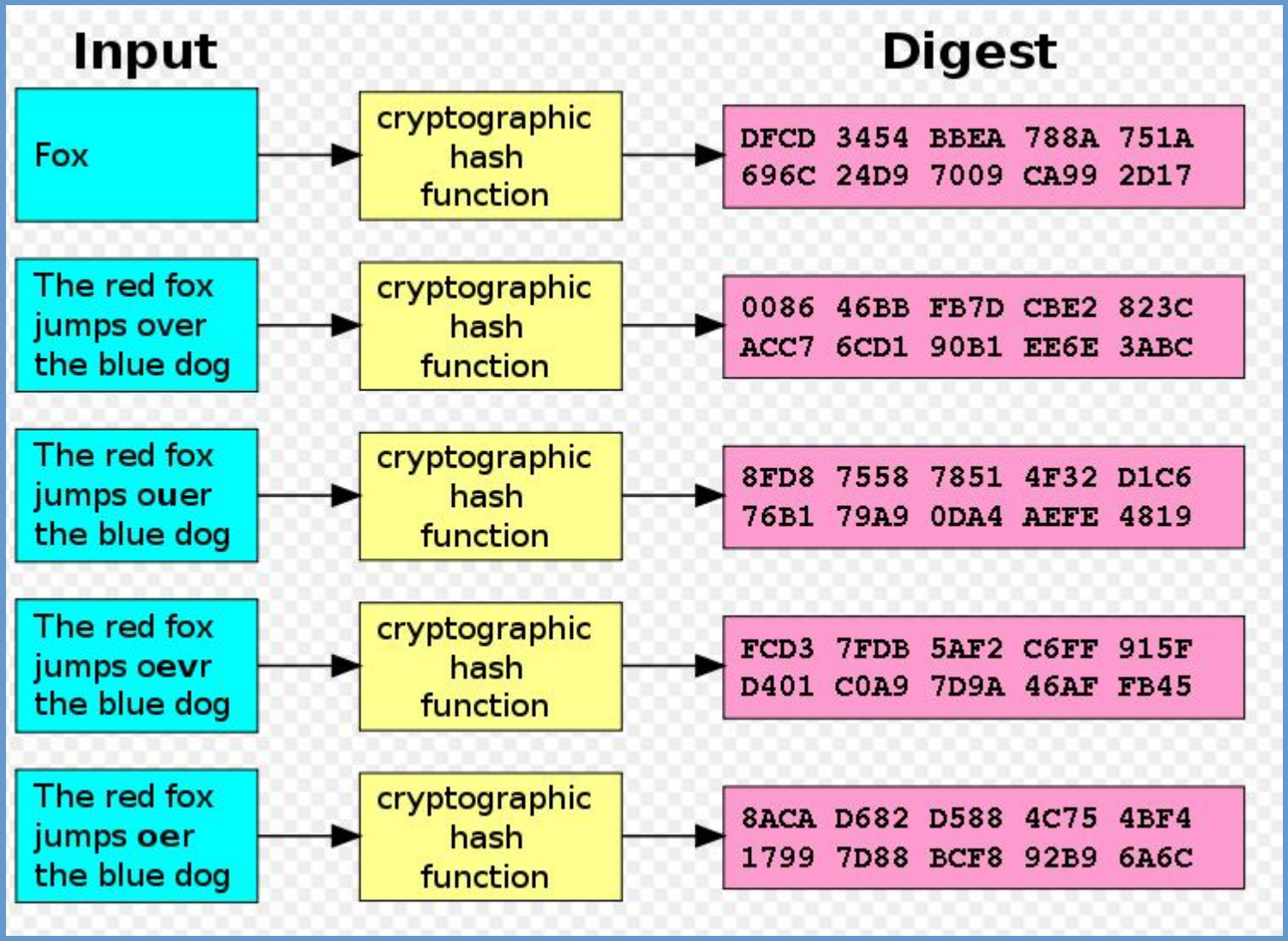
- การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ
- ผู้มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได้ด้วยการถอดรหัส **(Decryption)**

1. ใช้สมการทางคณิตศาสตร์ (อัลกอริทึม)
2. ใช้กุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้ (มีความยาวเป็นบิต โดยยิ่งกุญแจมีความยาวมาก ยิ่งปลอดภัยมาก เพราะต้องใช้เวลานานในการคาดเดากุญแจของผู้คุกคาม)

การเข้ารหัส (Encryption)

- ประกอบด้วยฝ่ายผู้รับ และฝ่ายผู้ส่ง
- ตกลงกฎเกณฑ์เดียวกัน ในการเปลี่ยนข้อความต้นฉบับให้เป็นข้อความอ่านไม่รู้เรื่อง (cipher text)
- ใช้สมการ หรือสูตรทางคณิตศาสตร์ที่ซับซ้อน
- กฎการเพิ่มค่า 13
- แฮชฟังก์ชัน (Hash function)

Hash Function



ส่วนประกอบของการเข้ารหัส

ขั้นตอนการเข้ารหัส

1. ใช้ฟังก์ชั่นการคำนวณทางคณิตศาสตร์ (Algorithm)
2. คีย์ที่ใช้ในการเข้ารหัส หรือ ถอดรหัส

- เป็นชุดตัวเลข หรือ อักขระที่นำมาเข้ารหัส มีหน่วยเป็นบิต (8 บิต = 1 ไบต์ = 1 อักขระ)

เช่น 00000001 = 1

00000010 = 2

สูตรคือ 2^n ; n คือ จำนวนบิต (อย่างต่ำ 8 บิต)

เช่น หาจำนวนบิต

- 2^8 = 256 คีย์ (2 คูณกัน 8 ครั้ง = 256 ชุดข้อมูล)

หรือ

- 2^{128} = ??? คีย์

(2^{128} เป็นคีย์ของโปรโตคอล SSL ที่ใช้อยู่ในปัจจุบัน)

ระยะเวลาใช้ในการถอดรหัส

- ถ้าคีย์ยาว 2^{40} บิต เวลาถอดรหัส 8 ปี
- ความยาว 2^{128} บิต เวลาถอดรหัส ล้านล้าน ปี

*****

จำนวนบิตมากเท่าไหร่ ความปลอดภัยของข้อมูลยิ่งมากขึ้น

เนื่องจากผู้บุกรุกต้องใช้เวลาเดาคีย์มากยิ่งขึ้น

ตัวอย่างโปรแกรมการเข้ารหัส โดยใช้กฎ 13[1]

การเข้ารหัสจะทำโดยการเปลี่ยนตัวอักษร จากตำแหน่งเดิมเป็นตัวอักษรตำแหน่งที่ 13 ของชุดตัวอักษรนั้น เช่น

A	B	C	D	E	F	G	H	I	G	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

....

....

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	G	K	L	M

เช่น เข้ารหัส I LOVE YOU ----> **V YBIR LBH**

1.การเข้ารหัสแบบสมมาตร (Symmetric encryption)

- ผู้รับและผู้ส่งข้อความจะมีคีย์เดียวกันในการรับส่งข้อความ

ข้อดี

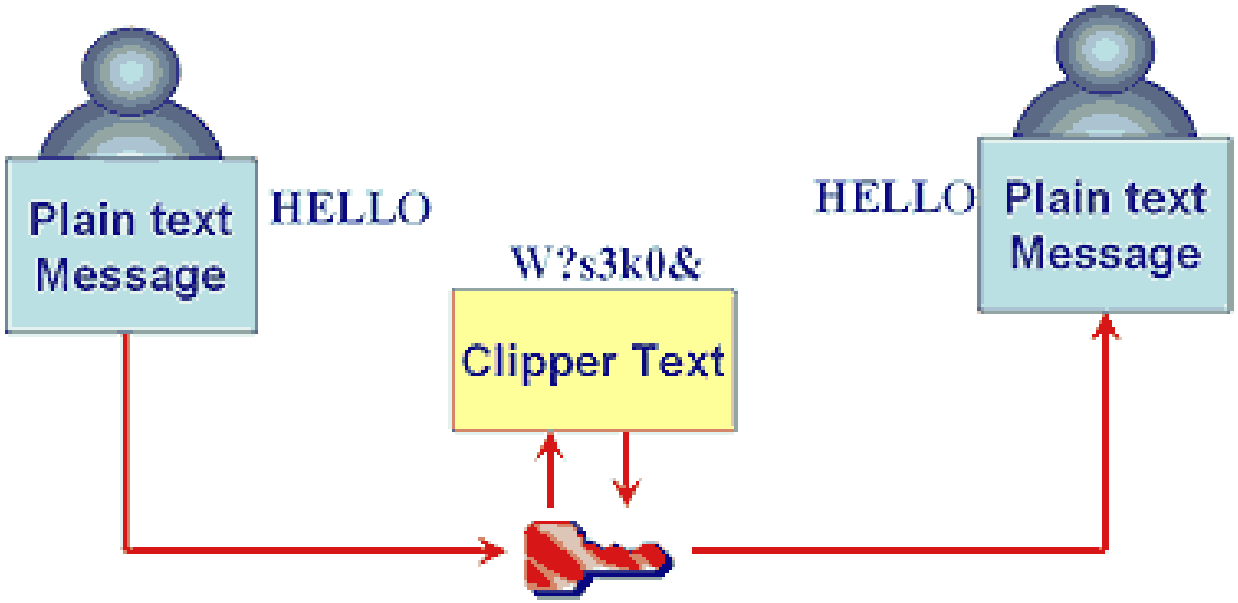
- มีความรวดเร็วเพราะใช้การคำนวณที่น้อยกว่า
- สามารถสร้างได้ง่ายโดยใช้ฮาร์ดแวร์

ข้อเสีย

- ไม่สามารถตรวจสอบว่าเป็นผู้ส่งข้อความจริง ถ้ามีผู้ปลอมตัวเข้ามาส่งข้อความ
- ไม่มีหลักฐานที่จะพิสูจน์ได้ว่าผู้ส่งหรือผู้รับกระทำรายการจริง
- การบริหารการจัดการกุญแจทำได้ยากเพราะกุญแจในการเข้ารหัส และถอดรหัส เหมือนกัน

Symmetric Encryption

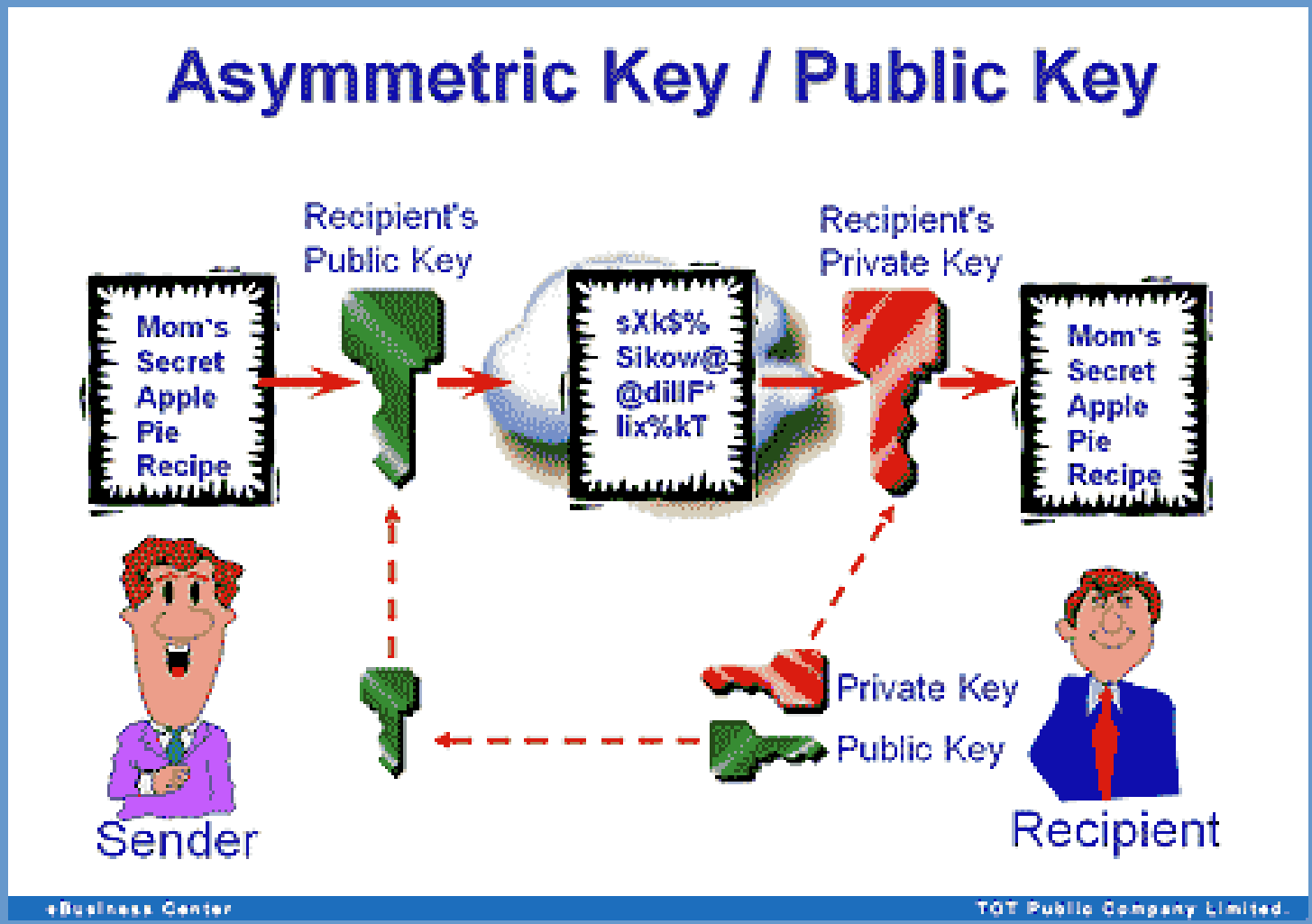
- Symmetric Key / Secret Key



2. การเข้ารหัสแบบอสมมาตร (Asymmetric encryption)

- ใช้เทคนิคของการมีคีย์เป็นคู่ๆ
- กุญแจส่วนตัว (private key) เป็นคีย์เฉพาะเจ้าของคีย์
  - ใช้ถอดรหัสและอ่านข้อความ เช่น รหัสผ่าน (password)
- กุญแจสาธารณะ (Public key) เป็นคีย์ที่ส่งให้ผู้อื่นใช้
  - แจกจ่ายให้ผู้ที่ต้องการส่งข้อความถึงเรา เช่น e-mail
- ใช้รักษาความลับของข้อความที่เราจัดส่งโดยใช้คีย์สาธารณะของผู้รับในการเข้ารหัส
- เป็นการระบุบุคคลผู้เป็นเจ้าของ (Authenticate) เพื่อตรวจสอบว่าบุคคลที่ส่งข้อความเข้ามานั้นเป็นตัวผู้ส่งเองจริง ๆ

Asymmetric Encryption



การเข้ารหัสแบบอสมมาตร

ข้อดี

- การบริหารการจัดการกุญแจทำได้ง่ายกว่า เพราะกุญแจในการเข้ารหัส และถอดรหัส ต่างกัน
- สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์

ข้อเสีย

- ใช้เวลาในการเข้า และถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก

- บน web จะใช้กุญแจสาธารณะ และกุญแจส่วนตัว
- เบราเซอร์ใช้กุญแจสาธารณะเพื่อเข้ารหัสรายการข้อมูลบนเครื่องคอมพิวเตอร์ลูกค้า (Client)
- เว็บเซิร์ฟเวอร์เท่านั้นมีกุญแจส่วนตัว

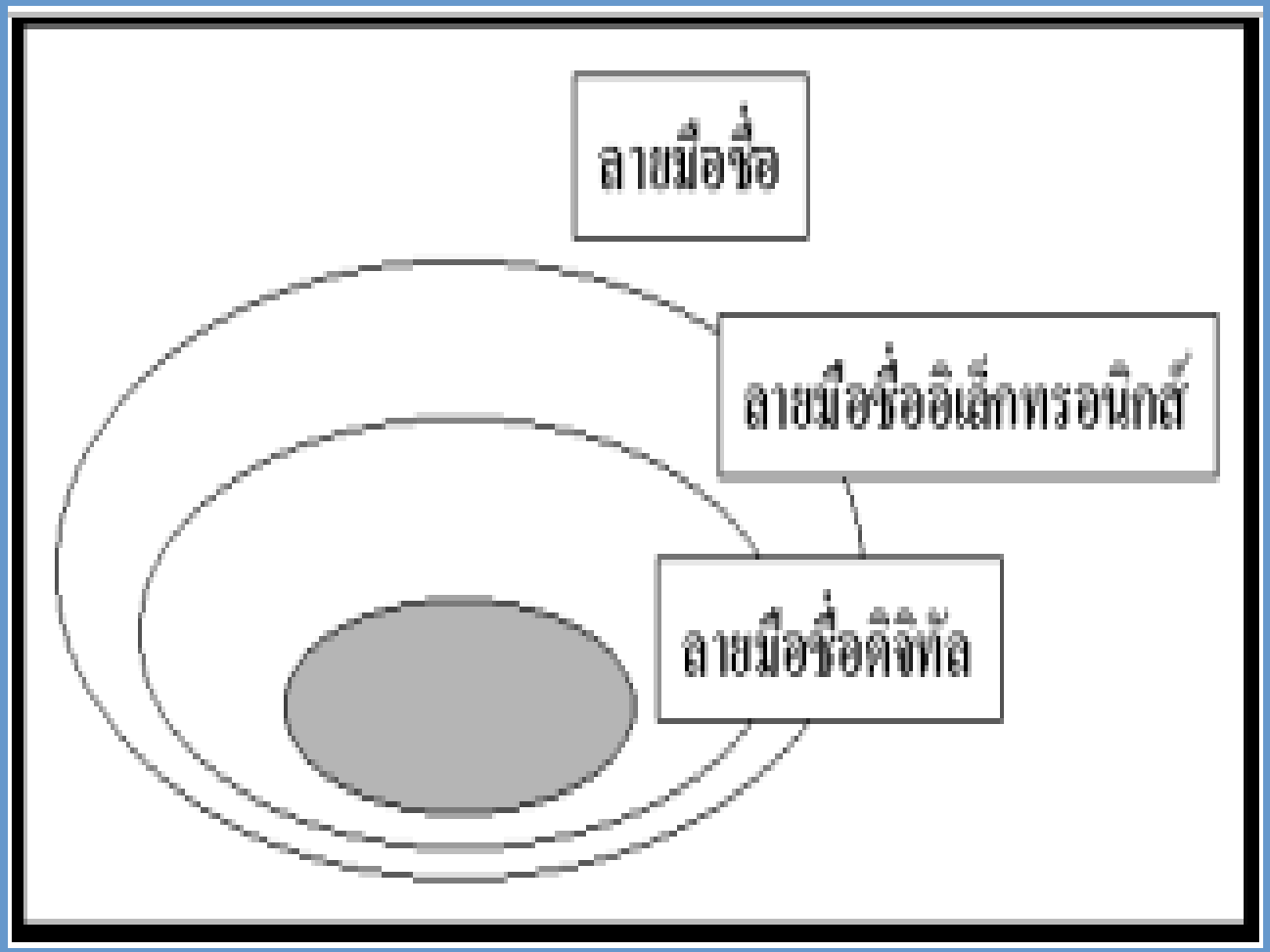
เทคโนโลยีที่สำคัญสำหรับการรักษาความปลอดภัยบนระบบ e-commerce

1. ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

- ลายมือชื่อดิจิทัล (Digital Signature)
  - ใช้ระบบรหัสแบบอสมมาตร (private key & public key)
- รหัสประจำตัว (ID) , รหัสผ่าน (Password)
- E-Mail Address
- Biometrics

2. ใบรับรองดิจิตอล (Digital Certificate)

3. องค์กรรับรองความถูกต้อง(Certification Authority ; CA)


ลายมือชื่อ
ลายมือชื่ออิเล็กทรอนิกส์
ลายมือชื่อดิจิทัล

1. ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

- **หมายถึง** อักขระ ตัวเลข เสียง หรือสัญลักษณ์อื่นใด ที่สร้างขึ้นโดยวิธีทางอิเล็กทรอนิกส์
- **วิธีการ** นำมาประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์
- **วัตถุประสงค์**
  - เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ (Authentication)
  - เพื่อแสดงว่าบุคคลยอมรับและผูกพันกับข้อมูลอิเล็กทรอนิกส์ หรือเพื่อป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation)

ลายมือชื่ออิเล็กทรอนิกส์

ปัญหา ?

- คู่สัญญาไม่เคยเห็นหน้ากันมาก่อน
- ไม่แน่ใจว่าใช่นาย Tom หรือไม่
- ใครจะเป็นผู้รับผิด หากผิดสัญญา

มั่นใจเพราะยืนยันได้ว่าผู้ที่ติดต่อคือใคร

ตรวจสอบได้ว่าสัญญามีการเปลี่ยนแปลง

มีผู้รับผิดตามสัญญา

ตัวอย่างลายมือชื่ออิเล็กทรอนิกส์

- รหัสประจำตัว (ID) , รหัสลับ (Password)
- Biometrics
- E-Mail Address
- ลายมือชื่อดิจิทัล (Digital Signature)
  - ใช้ระบบรหัสแบบอสมมาตร (private key & public key)

รหัสผ่าน (Password)

- ปิด-เปิด mailbox
- เก็บรักษากุญแจส่วนตัว
- ข้อจำกัด
  - ไม่สามารถนำไปใช้แนบท้ายข้อมูลอิเล็กทรอนิกส์
  - ไม่สามารถนำไปลงในหนังสือ
  - ควรปกปิดไว้เป็นความลับ

Biometrics

- ลักษณะทางชีวภาพ
  - สแกนม่านตา
  - จดจำเสียง
  - เครื่องอ่านลายนิ้วมือ

จดหมายอิเล็กทรอนิกส์ (E-mail)

- To : gentleman@npru.ac.th
- from : lady@hotmail.com
- message : ขอซื้อรถยนต์ที่คุณประกาศ

ขายราคา 50,000 บาท

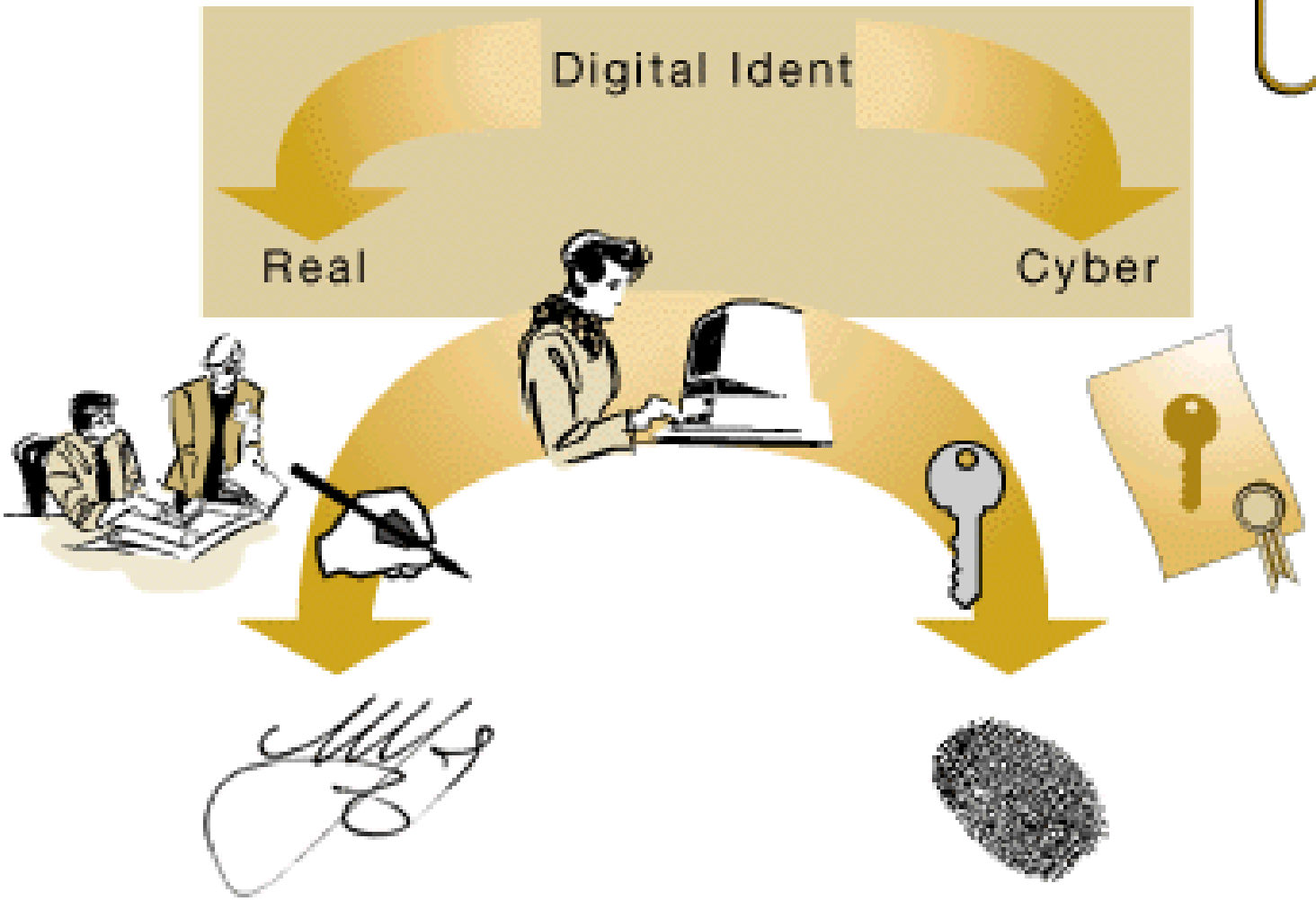
จากลำใย

ลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่อดิจิตอล (Digital Signature)

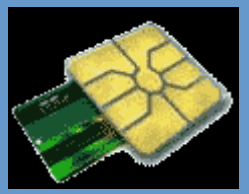
- ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัว (Private key) ของผู้ส่ง เปรียบเสมือนลายมือชื่อของผู้ส่ง
- ถอดรหัสด้วยกุญแจสาธารณะของผู้ส่ง (Public key)
- เพื่อระบุตัวบุคคล
- กลไกการป้องกันการปฏิเสธความรับผิดชอบ
- ป้องกันข้อมูลไม่ให้ถูกแก้ไข
- สามารถที่จะทราบได้ หากถูกแก้ไข

Digital Signature



สมาร์ทการ์ด

สมาร์ทการ์ด คือ บัตรพลาสติกที่มีช่องขนาดเล็ก (Microchip) เป็นที่เก็บข้อมูลจำนวนมากซึ่งเป็น จุดที่แตกต่างจากบัตรแถบแม่เหล็กธรรมดา ข้อมูลบนบัตรสมาร์ทการ์ดสามารถมีได้มากกว่าบนบัตรแถบแม่เหล็กธรรมดาถึง 100 เท่า ส่วนใหญ่เป็นข้อมูลส่วนตัวของเจ้าของบัตร เช่น เงินสดในบัญชีธนาคาร เบอร์บัญชีเงินฝาก หมายเลขบัตรเครดิต หรือรายละเอียดเกี่ยวกับการเงินต่าง ๆ เป็นต้น บางครั้งถูกเรียกว่า บัตรสะสมมูลค่า (Store - Valued Card) สมาร์ทการ์ดบางประเภทสามารถประมวลผลข้อมูลได้ด้วย ซึ่งจะใช้ในการเข้ารหัสและถอดรหัสของเจ้าของบริการ ซึ่งทำให้สมาร์ทการ์ดมีความเป็นส่วนตัว และปลอดภัยมากเป็นพิเศษ และยังสามารถใช้จ่ายเงินผ่านทางอินเทอร์เน็ตได้อีกด้วย



2. ใบรับรองดิจิตอล Digital Certificate

- ออกแบบโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority)
- เลขประจำตัวดิจิทัลที่รับรองความเป็นเจ้าของ web site
- เมื่อเริ่มการเชื่อมต่อที่มีระบบรักษาความปลอดภัยกับ web site
- เบราเซอร์ที่ใช้จะเรียกสำเนาของใบรับรองดิจิทัลจาก web server
- มีกุญแจสาธารณะเพื่อเข้ารหัสข้อมูลที่ส่งผ่านไซต์นั้น
- ให้ความมั่นใจว่าติดต่อกับ web site นั้นจริง
- ป้องกันการขโมยข้อมูลลูกค้าจากไซต์อื่น (spoofing)
- เช่น บ.verisign, ในไทยมี TOT

- ยืนยันในการทำธุรกรรมว่าเป็นบุคคลจริง
- ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อองค์กร ที่อยู่
- ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรองหมายเลขประจำตัวของผู้ออกใบรับรอง
- กุญแจสาธารณะของผู้ที่ได้รับการรับรอง
- วันหมดอายุของใบรับรองดิจิทัล
- ระดับชั้นของใบรับรองดิจิทัลซึ่งมี 4 ระดับ ระดับที่ 4 จะมีกระบวนการตรวจสอบเข้มงวดที่สุด และต้องการข้อมูลมากที่สุด
- หมายเลขประจำตัวของใบรับรองดิจิทัล

ประเภทของใบรับรองดิจิตอล

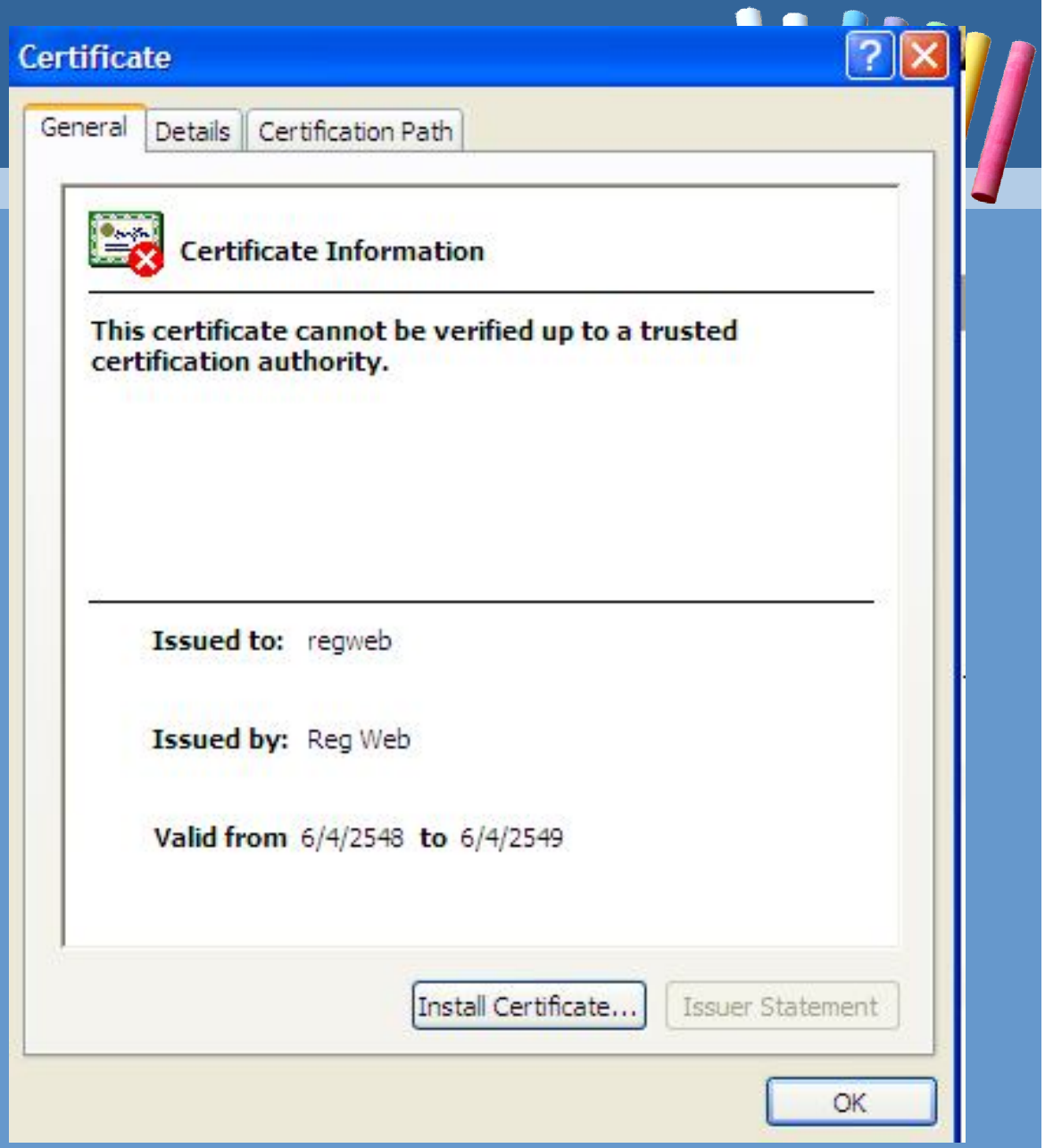
1. ใบรับรองตัวบุคคล
2. ใบรับรองโปรแกรม
3. ใบรับรองเว็บไซต์

BBBOnLine

หรือ

TRUSTe

ตย.ใบรับรองเว็บไซต์



TOT CA – Digital Certificate Properties

TOT CA (X.509 v.3)

Serial Number : ef96cd0b6379afg

Validity : 17 Feb 06 13.31.40 - 17 Feb 07 13.31.40

Signature Algorithms : sha1RSA-1024 bits
Issued Subject : Name /Organization / email

Holder's Public Key : RSA
ie86502hhd0vidywfoofkrtgfgdserth,jpdml4554r3df3ddkas
736ed5vidywfoofkk5qwfgk98dszbvcqm85k309nvidywjbkh

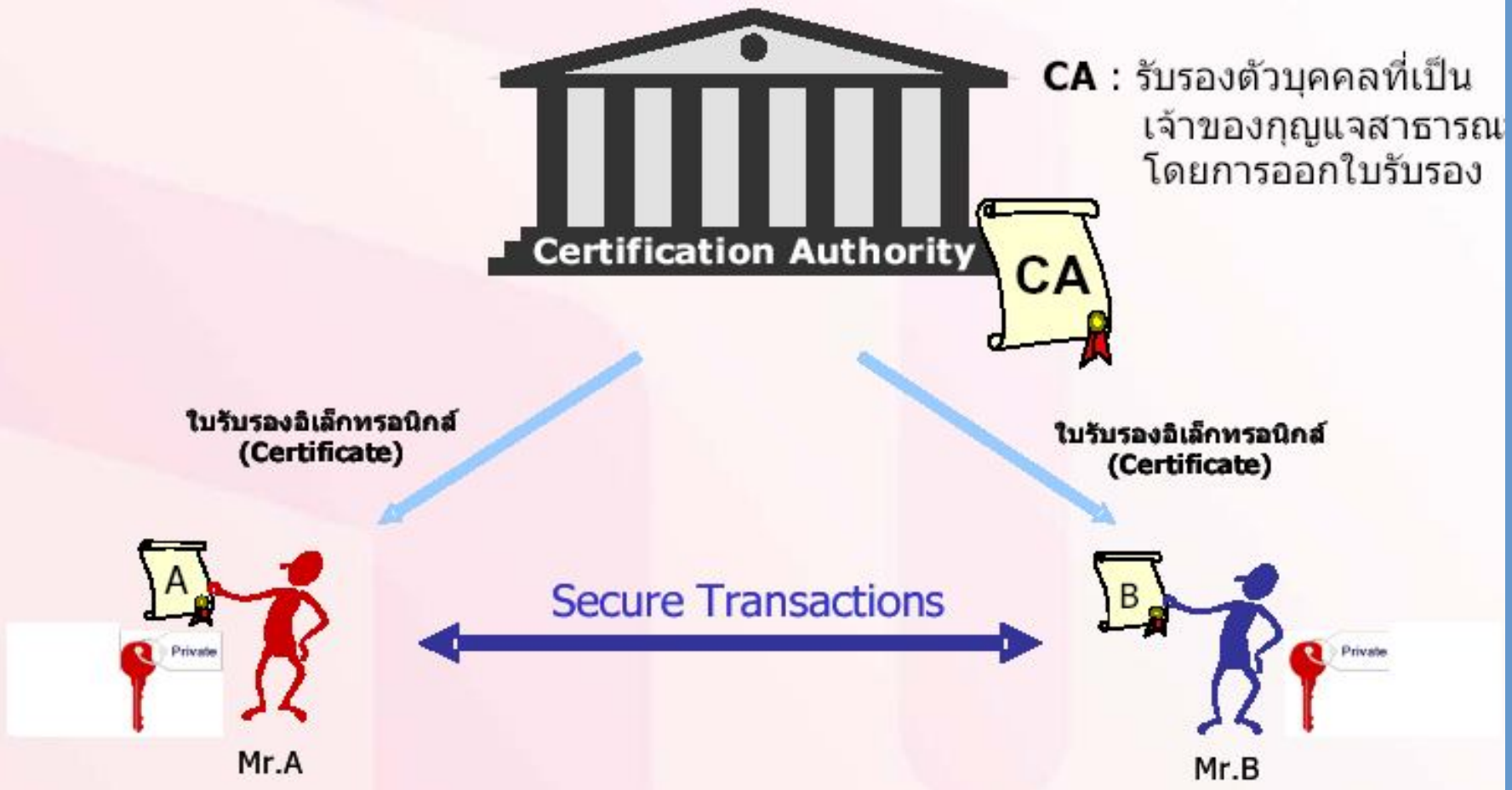
Signed by TOT CA
kdiowuriwi495729fd654df5648df3fgh6fgh153h3f1hshsg0925
h309afhwa09721h481903207akndnxnzkjpsioeru1069132by5

Other Extension

3. องค์กรรับรองความถูกต้อง (Certification Authority CA)

- หน้าที่ของ CA
- การให้บริการเทคโนโลยีการเข้ารหัส ได้แก่ การสร้างกุญแจสาธารณะและกุญแจลับสำหรับผู้จดทะเบียน การส่งมอบกุญแจลับ การสร้างและการรับรองลายมือชื่อดิจิทัล
- การให้บริการเกี่ยวกับใบรับรอง ได้แก่ การออกแบบการเก็บรักษา การยกเลิก การตีพิมพ์เผยแพร่ใบรับรองดิจิทัลรวมทั้งการกำหนดนโยบายการออกและอนุมัติใบรับรอง
- บริการเสริมอื่น ๆ ได้แก่ การตรวจสอบสัญญาต่าง ๆ การทำทะเบียน การกู้กุญแจ

Certification Authority (CA) : Trusted third party



รายนามผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (CA) ในประเทศไทย

Public CAs in Thailand

- สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.)
- CAT Telecom Public Company Limited(CAT)
- TOT Public Company Limited (TOT)
- ThaiDigital ID
- บริษัท Maxsavig จำกัด

e- payment

- ธนาคารแห่งประเทศไทย

e-Government

- กระทรวงมหาดไทย
- กระทรวงการต่างประเทศ
- กรมสรรพากร
- กรมศุลการกร
- กรมการประกันภัย
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- สำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นต้น

เทคโนโลยี และ มาตรการการรักษาความปลอดภัยของข้อมูล

มาตรการ/ เทคโนโลยี	การรักษาความลับ	การระบุตัวบุคคล	การรักษาความถูกต้อง	การป้องกันการปฏิเสธความรับผิดชอบ
การเข้ารหัส	หลัก	รอง		
ลายมือชื่อดิจิตอล		รอง 1	รอง 2	หลัก
ใบรับรองดิจิตอล และ องค์กรรับรองความถูกต้อง		หลัก		

โปรโตคอลระบบความปลอดภัยการชำระเงินออนไลน์

1. S-HTTP ตรวจสอบความมีสิทธิจริงของผู้ใช้ระหว่าง Browser และ Server
2. SSL ตรวจสอบสิทธิทั้งสองฝ่าย และมีการเข้ารหัสด้วยกุญแจคู่ (Public and Private key)
3. SET รับรองตัวตนที่แท้จริงของผู้ซื้อ-ผู้ขาย ด้วยการรับรองดิจิทัล เช่น ลายมือชื่อดิจิทัล

Secure Socket Layers : SSL

ตรวจสอบสิทธิทั้งสองฝ่าย และมีการเข้ารหัสด้วยกุญแจคู่ (Public and Private key)

- มีได้ 2 แบบ คือ การเข้ารหัสแบบ 40 bits กับการเข้ารหัส แบบ 128 bits
- ระบบระบุแค่ฝั่งผู้ขาย (ร้านค้า) ว่าเป็นใคร
- ไม่สามารถระบบผู้ถือบัตรได้ว่าเป็นตัวจริงหรือไม่

หลักการ

- ข้อมูลจากไคลเอนต์ที่จะส่งไปเซิร์ฟเวอร์จะถูกเข้ารหัส
- เว็บเบราเซอร์จะเป็นตัวเข้ารหัสให้
- โดยเว็บเบราเซอร์จะเอา Public Key จากเซิร์ฟเวอร์มาเข้ารหัสกับ Master key ที่เบราเซอร์สร้างขึ้นมา
- เซิร์ฟเวอร์จะมีหน้าที่ในการถอดรหัสกลับมาเป็นข้อมูลปกติ

- HTTP (HyperText Transmission Protocol) เป็นมาตรฐาน เช่น

  http://www.ktb.co.th

- ถ้าเว็บใดมีการใช้เทคโนโลยีรักษาความปลอดภัยแบบ SSL มาตรฐานที่ใช้จะเปลี่ยนเป็น
- **HTTPS** (HyperText Transmission Protocol, Secure)

  https://www.ktbonline.ktb.co.th

- **HTTPS** (HyperText Transmission Protocol Secure)

Secure Electronic Transaction : SET

- ปัจจุบันมีใช้กันอยู่ใน 34 ประเทศ มีความปลอดภัยกว่าระบบ SSL
- SET จะมีหน่วยงานกลางที่ถูกจัดตั้งขึ้นมาเพื่อยืนยันการทำธุรกรรม (Certification Authority : CA)
- ระบุตัวจริงได้ทั้งผู้ถือบัตร ร้านค้า และธนาคารโดยการรับรองจาก CA
- มี Private key และ Public key โดยที่ Public key นั้นทาง CA จะเป็นผู้เก็บไว้เพื่อทำการตรวจสอบ
- เมื่อมีการสั่งซื้อสินค้า ร้านค้าจะได้รับข้อมูลเฉพาะใบสั่งซื้อส่วนหมายเลขบัตรเครดิตทางร้านค้าไม่สามารถเรียกดูได้ แต่จะส่งไปยังธนาคารเพื่อเรียกเก็บเงิน
- ต้นทุนสูง

tion	Secure Site SSL Certificates	Secure Site Pro True 128-Bit SSL	Commerce Site SSL Certificates	Commerce Site Pro True 128-bit SSL	Managed PKI for SSL Standard Edition	Managed PKI for SSL Premium Edition	Managed PKI for Intranet SSL Standard Edition	Managed PK Intranet SS Premium Editi
ew Product scription	Product Info	Product Info	Product Info	Product Info	Product Info	Product Info	Product Info	Product Inf
ady to Buy?	Buy Now	Buy Now	Buy Now	Buy Now	Contact Sales	Contact Sales	Contact Sales	Contact Sal
ice: 2-Year rtificate	$598	$1,790	$1,798	$2,795	Contact Sales	Contact Sales	Contact Sales	Contact Sale
ice: 1-Year rtificate	$349	$995	$949	$1,495	$249/certificate for 10	$695/certificate for 10	$179/certificate for 10	$489/certificate 10
mber of rtificates	Single	Single	Single	Single	5, 10, 25, 50, 100, more	5, 10, 25, 50, 100, more	5, 10, 25, 50, 100, more	5, 10, 25, 50, more
ee SSL Trial	Free SSL Trial	-	-	-	-	-	-	-
nimum SSL cryption	40-bit	128-bit	40-bit	128-bit	40-bit	128-bit	40-bit	128-bit
suance	Standard	Express delivery	Express delivery	Express delivery	Instant issuance by authenticated administrators	Instant issuance by authenticated administrators	Instant issuance by authenticated administrators	Instant issuanc authenticate administrato
line Payment ocessing	-	-	Payflow Pro	Payflow Pro	-	-	-	-
riSign NetSure otection rranty	$100,000	$250,000	$100,000	$250,000	$100,000	$250,000	$100,000	$250,000
alys Guard	-	Free	-	Free	-	-	-	-
tcraft	-	Free *$1,000 value*	Free *$1,000 value*	Free *$1,000 value*	-	-	-	-
ynote Red Alert	-	Free	Free	Free	-	-	-	-
riSign Secured al	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSig Secur
thentication	2 factor authentication	2 factor authentication	2 factor authentication	2 factor authentication	Class 3 organizational authentication	Class 3 organizational authentication	Class 3 organizational authentication	Class 3 organization authenticatic

e-Commerce Payment Security

- แนวทางการแก้ไขปัญหาการชำระเงินออนไลน์ในปัจจุบัน
  - ความพยายามของธนาคาร
    - การตรวจสอบที่อยู่ที่แท้จริง (AVS)
    - การพัฒนาระบบการชำระเงิน ePay โดยใช้บัตรสมาร์ทการ์ดทำ ธุรกรรมผ่านเครือข่ายอินเทอร์เน็ตของบริษัท PCC เป็นธุรกรรมคล้าย ATM pool ที่สนับสนุนการโอนเงินระหว่างผู้ซื้อและผู้ขายต่างธนาคารได้ แต่ด้านผู้ขายหรือร้านค้าจะต้องลงทุนในเครื่องอ่านบัตรสมาร์ทการ์ด
    - อนุญาตให้ผู้ถือบัตร ATM สร้างเลขบัญชีเสมือนเพื่อทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์ได้

ปัจจุบันมี Visa Electron ที่อำนวยความสะดวกในการชำระเงินผ่านระบบ e-Commerce ได้ทั่วโลก

e-Commerce Payment Security

- ความพยายามของธนาคาร
  - CVV2 หลังบัตรเครดิต กรอกลงไปในเว็บไซต์
  - บัตร VISA Electron
  - บัตร MasterCard Electronic

e-Commerce Payment Security

- ***Verified by VISA***
  - เป็นระบบชำระเงินชนิดใหม่ที่คิดค้นโดย VISA เพื่อลดความเสี่ยงจากการทำธุรกรรมทางการเงินบนอินเทอร์เน็ต
  - ผู้ถือบัตรเครดิตจะต้องทำการขอรหัสผ่านจากธนาคารผู้ออกบัตรก่อนชำระค่าสินค้าในเว็บไซต์ที่มี Verified by VISA เมื่อถึงขั้นตอนการชำระเงินจะมีหน้าจอให้กรอกข้อมูลรหัสผ่านในหน้าดังกล่าว ผู้ซื้อจะปลอดภัยจากการที่ร้านค้านี้ได้รับการระบุตัวตนที่แท้จริง และมั่นใจได้ว่าจะไม่ถูกนำข้อมูลไปใช้ในทางมิชอบ
  - ร้านค้าก็มั่นใจเพราะมีการยืนยันตัวผู้ซื้อชัดเจน เพราะหากเกิดการปฏิเสธการชำระเงินธนาคารที่ออกบัตร Visa จะเป็นผู้รับผิดชอบการชำระเงินนั้น
  - ด้วยระบบการชำระเงินที่ดี จะทำให้การซื้อขายสินค้าบนระบบพาณิชย์อิเล็กทรอนิกส์เป็นไปได้ นับเป็นการเปิดโอกาสแก่ผู้ประกอบการไทยที่จะใช้ช่องทางนี้พัฒนาการค้าต่างประเทศได้มากขึ้นด้วย

e-Commerce Payment Security

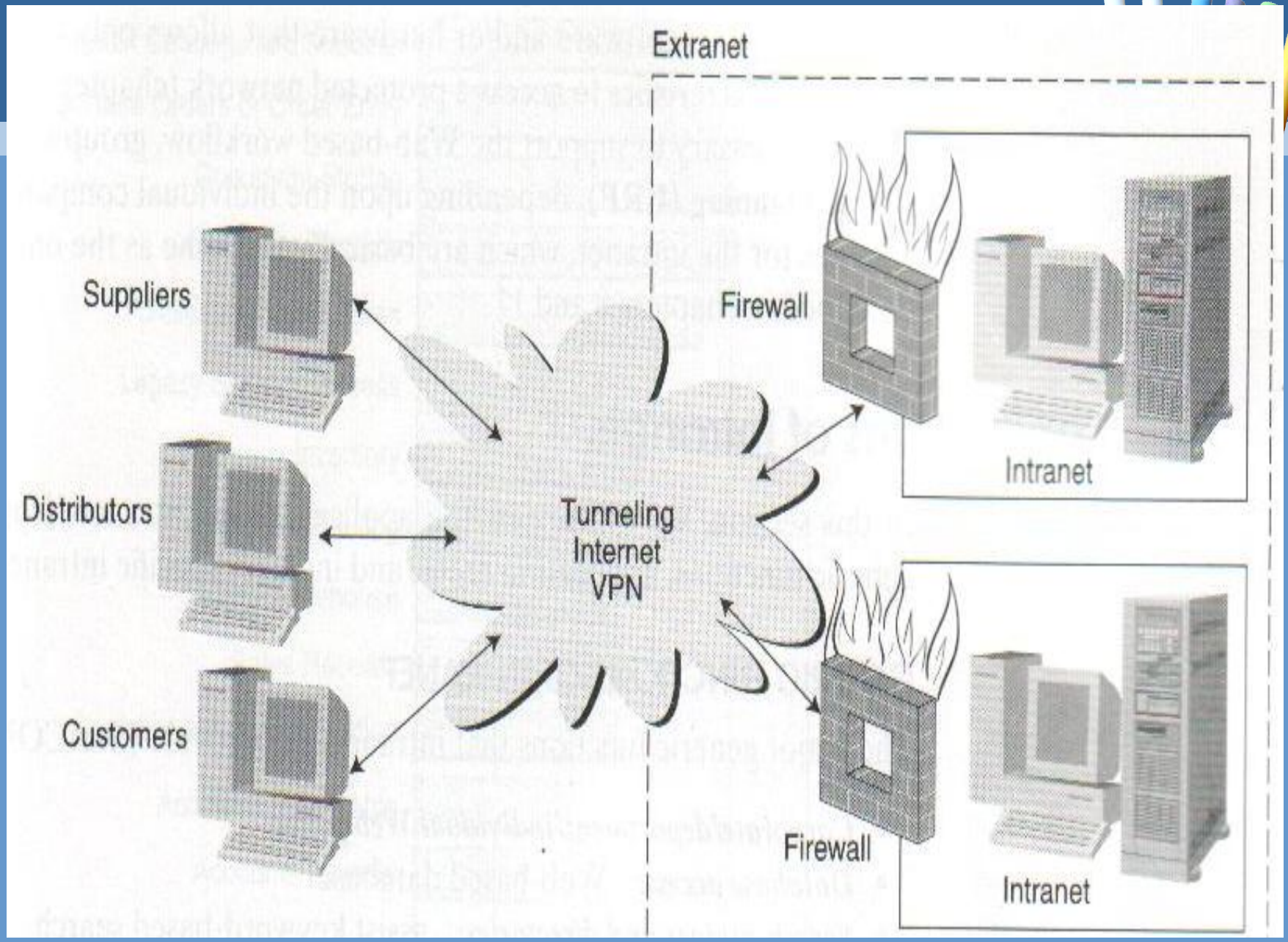
- ***MasterCard SecureCode***
  - ลักษณะเดียวกันกับ VBV แต่เป็นของ MasterCard
  - เพื่อเพิ่มความปลอดภัยของการชำระค่าสินค้าและบริการผ่านบัตรเครดิตทางอินเทอร์เน็ต ด้วยระบบการสอบถามรหัสผ่านส่วนตัว (SecureCode Password) และระบบการแสดงคำทักทายส่วนตัว (Personal Greeting) ในทุกครั้ง ที่มีการทำรายการชำระค่าสินค้า และบริการผ่านบัตรเครดิตทางอินเทอร์เน็ต

MasterCard® SecureCode™

2. การรักษาความปลอดภัยของเครือข่าย (Network Security)

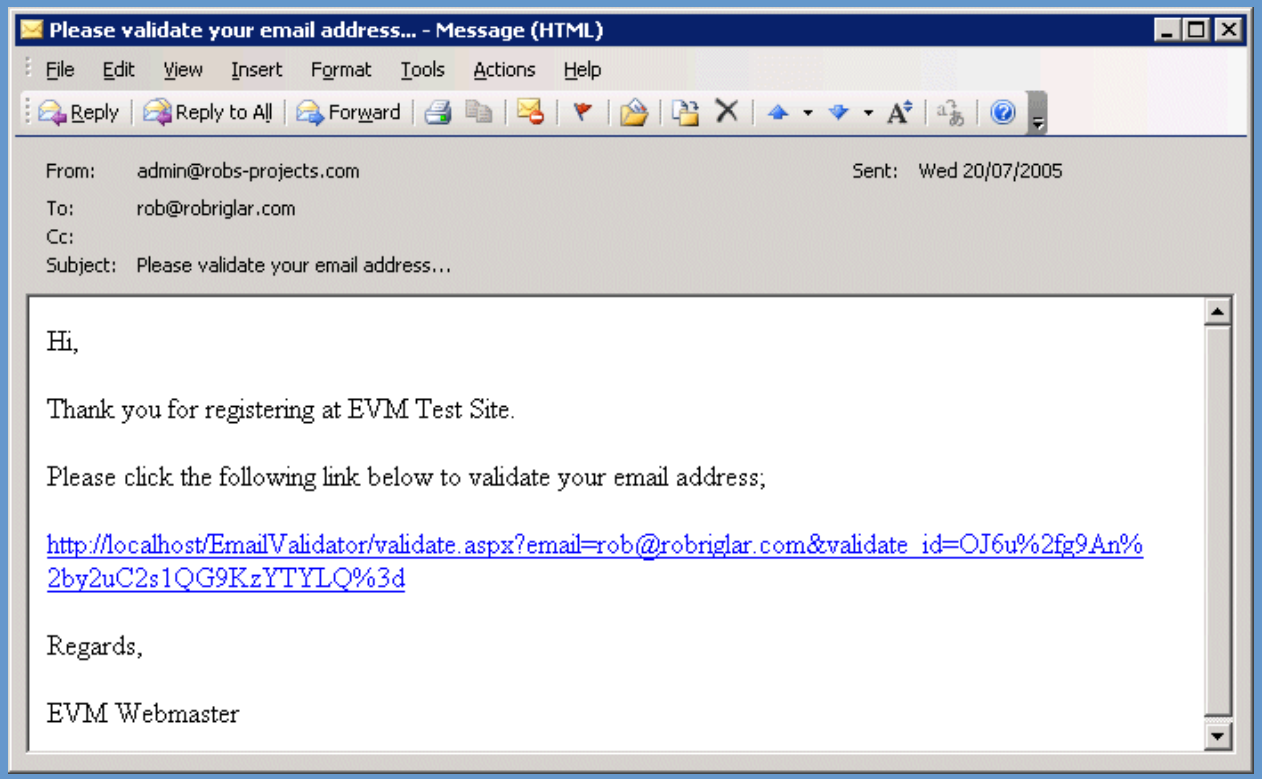
กำแพงไฟ (Firewall)

- เป็นฮาร์ดแวร์ และซอฟต์แวร์ที่ใช้สำหรับป้องกันการบุกรุกของระบบเครือข่าย
- ระบบกั้นการติดต่อภายนอก
- จุดสำคัญคือ ควบคุมทางเข้าออกของข้อมูล
- ตรวจสอบจาก packet ข้อมูลที่ส่งผ่านอุปกรณ์สื่อสารหรือคอมพิวเตอร์ในเครือข่ายกับอินเทอร์เน็ต


Extranet
Suppliers
Distributors
Customers
Tunneling
Internet
VPN
Firewall
Intranet
Firewall
Intranet

- สกัดกั้นการบุกรุกได้ไม่ถึง100%
- สถิติพบว่า 80% ของการบุกรุกระบบเกิดจากคนในองค์กร
- แฮกเกอร์จากภายนอก อาจเข้ามาใช้คอมพิวเตอร์โน้ตบุ๊คต่อเข้ากับเครือข่ายด้วยเหตุผลง่ายๆ เช่น ตรวจโทรศัพท์ หรือ ตรวจระบบสาย แล้วสร้างเส้นทางเชื่อมต่อทะลุไฟร์วอลล์
- Spoofing คือ การแอบเข้ามาใช้ระบบโดยปลอมเป็นผู้อื่น

ตัวอย่างการรักษาความปลอดภัยบนเว็บเพิ่มเติม

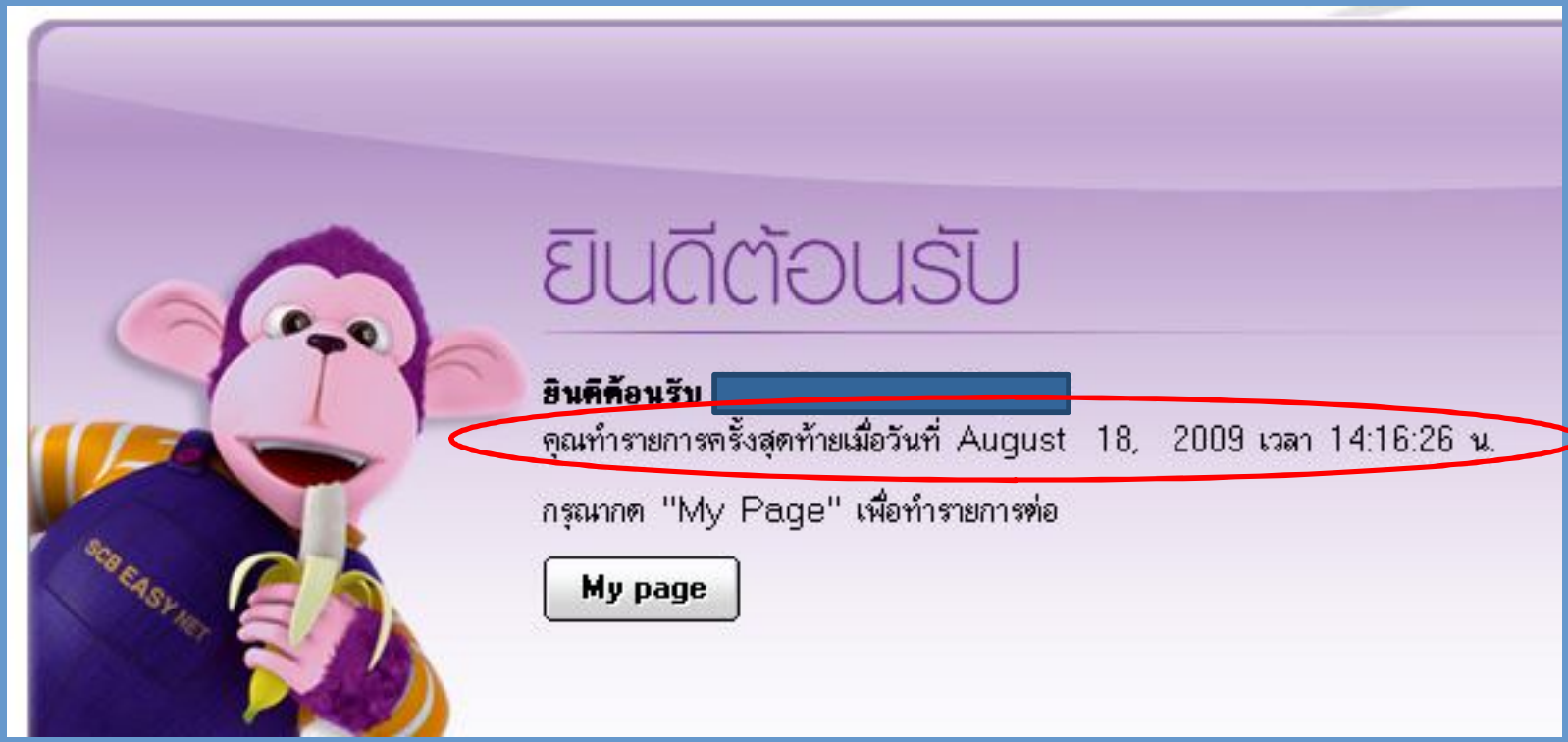


ในขั้นตอนการสมัครสมาชิก มีการส่งลิงก์ทางอีเมล์ (account / email-address validation) เพื่อให้คลิกตอบกลับมา เป็นการยืนยันตัวตนผู้สมัครว่าใช้อีเมล์นี้จริง

ตัวอย่างการรักษาความปลอดภัยบนเว็บเพิ่มเติม

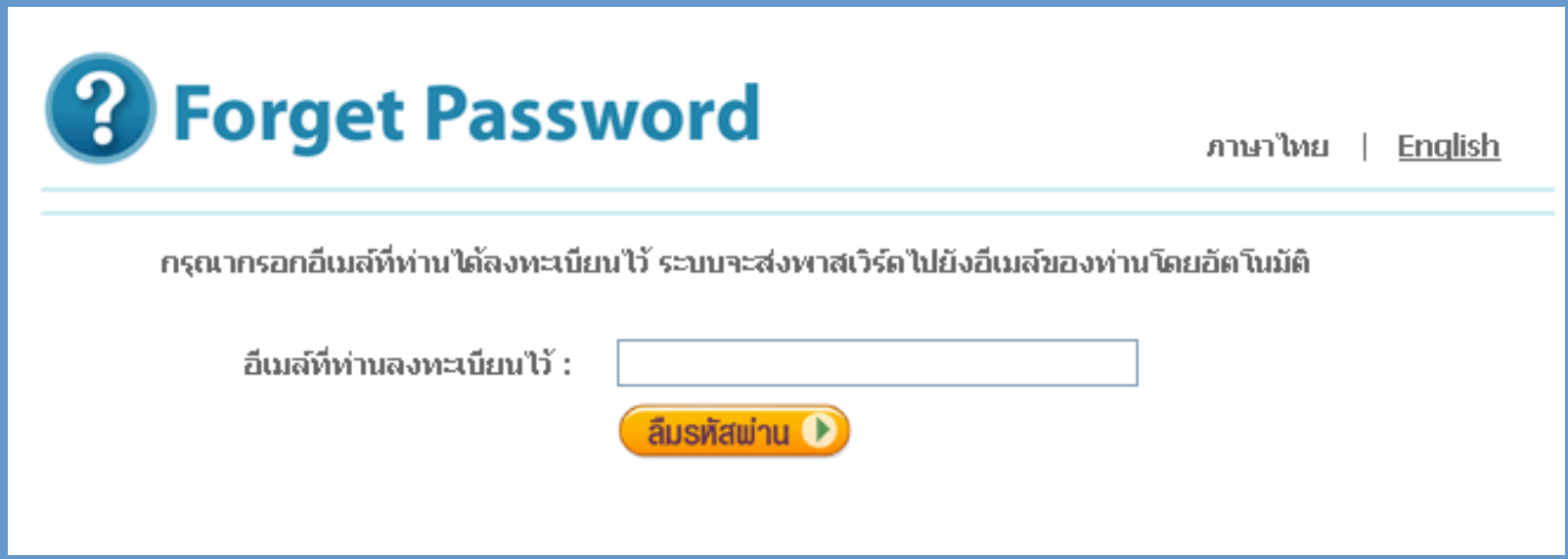
- ช่องใส่รหัสผ่านต้องแสดงเป็นสัญลักษณ์เพื่อไม่ให้ผู้อื่นมองเห็น

ตัวอย่างการรักษาความปลอดภัยบนเว็บเพิ่มเติม



- แจ้งวัน-เวลาที่ผู้ใช้เข้าระบบครั้งล่าสุด เพื่อให้รู้ตัวถ้ามีผู้อื่นแอบแฝงเข้ามาใช้งานร่วม

ตัวอย่างการรักษาความปลอดภัยบนเว็บเพิ่มเติม



- ถ้าลูกค้าลืมรหัสผ่าน จะส่งรหัสไปให้ทราบทางอีเมล์ที่ลงทะเบียนไว้เท่านั้น เพื่อป้องกันไม่ให้ผู้ที่ไม่ใช่เจ้าของล็อกอินเข้าระบบได้