จริยธรรมอิเล็กทรอนิกส์
ความสำเร็จที่ยั่งยืน

11

คน...ทุกคนอาจเป็นลูกค้าของเรา

ทำ...สิ่งถนัดตอบสนองลูกค้าของเรา

กิน...ผลกำไร เพราะลูกค้าเลือกเรา

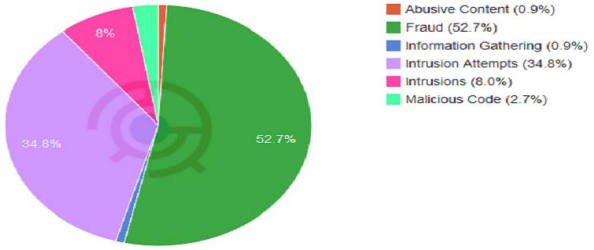
“เว็บไซต์”

ของคุณเคยเจอปัญหาเหล่านี้หรือไม่?

- เว็บ **“โหลดช้า”** ผิดปกติ หรือเข้าไม่ได้เลย
- ได้รับ **“อีเมล์ผิดปกติ”** เข้ามาเป็นจำนวนมาก
- พบ **“เว็บไซต์ปลอม”** หน้าตาเหมือนเราเปะ
- ข้อมูลลูกค้าบนเว็บไซต์ **“สูญหาย”**
- ข้อมูลลูกค้า **“ถูกขโมย”**

ผมว่าใครทำธุรกิจออนไลน์และยังไม่เคยเจอปัญหาที่ผมถามไปด้านบน อาจยังไม่เข้าใจเท่าไหร่ว่ามันเป็นประเด็นใหญ่ที่ต้องรีบหาสาเหตุ เพราะมันเป็นสัญญาที่กำลังบอกว่าเราอาจจะถูก “ภัยคุกคามทางอินเทอร์เน็ต” ขึ้นแล้ว และก็อาจจะส่งผลกระทบต่อธุรกิจของเรา ซ้ำร้ายอาจกระทบไปที่ลูกค้าของเราก็ได้ บางคนอาจมองว่าเป็นเรื่องไม่สำคัญที่ต้องเรียนรู้ เพราะมันค่อนข้างยุ่งยากซับซ้อน และอาจต้องใช้เงินลงทุนเพื่อป้องกันหรือแก้ไขปัญหาเหล่านี้ ถ้าแต่เราให้เวลากับเรื่องนี้สักนิด ผมว่ามันจะช่วยทำให้ธุรกิจของเราเติบโตอย่างปลอดภัยมากขึ้นทีเดียวครับ

ทุกท่านทราบมั้ยครับว่าในบ้านเรามีหน่วยงานที่ชื่อว่า ThaiCERT หรือชื่อเต็มๆ ของเค้าก็คือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย ทำหน้าที่ในการป้องกัน และแก้ไขปัญหาด้านภัยคุกคามทางอินเทอร์เน็ตของประเทศ ซึ่งเค้าได้รวบรวมสถิติเกี่ยวกับภัยคุมภาพทางอินเทอร์เน็ตของไทย พบว่า ภัยคุกคามเกินกว่าครึ่งมาจากเรื่อง “Fraud” หรือการหลอกลวงทางอินเทอร์เน็ต



Source: www.etda.or.th

ThaiCERT ได้ยกตัวอย่างของ Fraud ที่เกิดจากการรั่วไหลของข้อมูลลูกค้าที่เจ้าของเว็บไซต์เก็บรักษาไว้อย่างน่าสนใจทีเดียวครับ *"ผู้ประกอบการถูกขโมยรหัสผ่านของอีเมล์ ทำให้ผู้ไม่หวังดีสามารถส่งอีเมล์ ไปหลอกลวงลูกค้าให้ชำระเงินผ่านบัญชีใหม่ที่ผู้ไม่หวังดีสร้างขึ้น และลูกค้าก็หลงเชื่อเพราะเป็นคู่ค้ากันมานาน โอนเงินไปยังบัญชีดังกล่าว"*

ผลที่ตามมาจากกรณีนี้ก็คือ ลูกค้าสูญเสียเงิน และผู้ประกอบการเสียชื่อเสียง และความไว้วางใจจากลูกค้า ซึ่งเมื่อมาวิเคราะห์ถึงสาเหตที่ทำให้เกิดการรั่วไหลของรหัสผ่านอาจเกิดจากหลายสาเหต เช่น

☑ เจ้าของเว็บทำเครื่องคอมพิวเตอร์สูญหาย หรือถูกขโมยไป

☑ เจ้าของเว็บอนุญาตให้ผู้อื่นสามารถเข้าถึงข้อมูลได้

☑ เครื่องคอมพิวเตอร์ของเจ้าของเว็บติด Malware (เช่น Virus, Botnet, Spyware)

การรั่วไหลของข้อมูลกรณีนี้ ผู้ไม่หวังดีจึงสามารถนำรหัสผ่านของเว็บไซต์เพื่อ Login เข้าไป อ่านข้อมูลการซื้อขาย ผู้ไม่หวังดีอาจใช้เพื่อประโยชน์ในเชิงแข่งขันทางธุรกิจ ใช้ส่งอีเมล์ในชื่อของเราเพื่อหลอกลวงลูกค้า หรืออาจใช้เพื่อสร้างความเสื่อมเสียแก่ธุรกิจของเรา หรือลบข้อมูลลูกค้าของเราทั้งหมด หรืออาจจะสวมรอยขายสินค้าแทนเรา ในที่สุดแล้วลูกค้าก็หมดความเชื่อถือ และอาจรุนแรงถึงขั้นถูกฟ้องร้องได้เลยทีเดียว

CIA: 3 กฎเหล็กเพื่อรักษาความเป็นส่วนตัวต่อลูกค้า

เอาล่ะครับ ผมเชื่อว่าเมื่ออ่านมาถึงตรงนี้ คงเริ่มพอเห็นภาพแล้วว่าภัยคุกคามทางอินเทอร์เน็ตไม่ใช่เรื่องไกลตัวเลย เราอาจต้องเจอกับมันไม่วันใดก็วันหนึ่ง ดังนั้น มารู้จักวิธีรักษาความเป็นส่วนตัวต่อลูกค้ากันดีกว่า โดยขอให้ยึดกฎเหล็ก 3 ข้อนี้เอาไว้นะครับ

1. **C**onfidentiality - ความลับ
2. **I**ntegrity - ความสมบูรณ์
3. **A**vailability - ความพร้อมใช้

กฎข้อ 1: ต้องเก็บความลับ (Confidentiality)

กฎข้อนี้ เจ้าของเว็บไซต์ต้องมั่นใจว่า ผู้ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงข้อมูลภายในเว็บได้ ซึ่งในแง่ของการปฏิบัติก็สามารถทำได้หลายวิธี เช่น

- กำหนดนโยบายรักษาความมั่นคงปลอดภัย และ “นำไปใช้จริง”
- การจัดกลุ่มของข้อมูล เพื่อกำหนดระดับสิทธิในการเข้าถึง
- จัดหาระบบรักษาความปลอดภัยให้กับแหล่งจัดเก็บข้อมูล
- ทำการฝึกอบรมทีมงานและผู้ใช้เว็บไซต์

กฎข้อ 2: ข้อมูลต้องถูกต้อง (Integrity)

เจ้าของเว็บไซต์ต้องมั่นใจว่า มีมาตรการปกป้องเพื่อให้ข้อมูลลูกค้าไม่ถูกแก้ไข เปลี่ยนแปลง หรือถูกทำลายได้ เช่น

- การเข้าถึงระบบด้วยระบบ Login
- เพิ่มระดับความปลอดภัยด้วยระบบ Login 2 ชั้น

- นำระบบพิสูจน์บุคคลที่มีสิทธิ์เข้าถึงข้อมูลมาใช้ เช่น ลายนิ้วมือ ลายเซ็นต์ เป็นต้น
- มีการจัดเก็บและตรวจสอบข้อมูลการใช้งานของผู้ใช้แต่ละคน

<u>กฎข้อ 3:</u> ระบบต้องพร้อมใช้ตลอดเวลา (Availability)

เจ้าของเว็บไซต์ต้องเชื่อมั่นว่า ข้อมูลลูกค้าจะถูกเข้าถึงได้อย่างราบรื่นตลอดเวลาจากผู้ได้รับอนุญาตเท่านั้น ลองดูวิธีการเหล่านี้ครับ

- หมั่นตรวจตรา Software & Hardware ให้พร้อมใช้งาน
- พัฒนาเทคโนโลยีพื้นฐานของระบบไอทีให้ทันสมัยอยู่เสมอ
- จัดเตรียมแผนรับมือกับสถานการณ์ฉุกเฉินต่างๆ
- จัดเตรียมทีมงานให้พร้อม

แล้วเว็บไซต์คุณล่ะ

มีมาตรฐานรักษาความปลอดภัยต่อข้อมูลลูกค้าแล้วหรือยัง ?

☐ เก็บรักษาความลับได้ (Confidentiality)

☐ ข้อมูลสมบูรณ์ถูกต้อง (Integrity)

☐ ระบบพร้อมใช้ตลอดเวลา (Availability)

เคล็ด (ไม่) ลับ ป้องกันภัยคุกคามออนไลน์

ในหัวข้อนี้เราจะมาทำความรู้จักกับภัยคุกคามออนไลน์อีกลักษณะหนึ่งที่ไม่ได้เกิดจากการหลอกลวงที่เกิดจากคน แต่เกิดจากไวรัสคอมพิวเตอร์ที่สามารถสร้างความเสียหายให้แก่ธุรกิจของเรา อาจรุนแรงถึงขั้นโจมตีไปที่ฐานข้อมูลลูกค้าและแพร่กระจายต่อๆ ไปเหมือนไวรัสที่แพร่กระจายออกไปทุกทิศทุกทาง ซึ่งเจ้าไวรัสคอมพิวเตอร์ก็มีอยู่ด้วยกันหลายสายพันธ์นะครับ ผมจะอธิบายถึงVirus, Worm, Trojan Horses และ Phishing ครับ

1. ไวรัส (Virus)

ถ้าคอมพิวเตอร์ของเราช้าผิดปกติ อยู่ๆ ก็ Re-Start ตัวเองตลอดเวลา ขอให้สันนิษฐานเบื้องต้นไว้เลยครับว่าเราอาจติดไวรัสแล้ว ไวรัสเป็นโปรแกรมที่ถูกเขียนขึ้นมาเพื่อทำลายซอฟต์แวร์ หรือโปรแกรมต่างๆ ในเครื่องคอมพิวเตอร์ ซึ่งความจริงแล้วเจ้าไวรัสร้ายจะไม่สามารถแพร่กระจายได้ด้วยตนเอง แต่จะอาศัยโปรแกรมอื่นในการแพร่กระจายออกไป โดยผลจากการติดไวรัส เช่น

- คอมพิวเตอร์ช้ากว่าปกติ
- คอมพิวเตอร์รีสตาร์ทตัวเองตลอดเวลา หรือใช้เวลาบูตนาน
- ดับเบิลคลิกเมาส์ หรือคลิกเมาส์ขวาไม่ได้
- ไฟล์ หรือโฟล์เดอร์หายไป
- ใช้โปรแกรมปฏิบัติการบางอย่างไม่ได้
- Web Browser เปิดเองไม่ยอมหยุด
- มองไม่เห็นข้อมูลใน Drive

วิธีป้องกัน - DO

- ตั้งรหัสผ่านสำหรับ Login เข้าเครื่อง
- ล็อกหน้าจอด้วย Screen Server
- ปิดการแชร์งดใช้ข้อมูลร่วมกัน
- ติดตั้งโปรแกรมป้องกันไวรัส

วิธีป้องกัน – DON'T

- หลีกเลี่ยงการดาวน์โหลดข้อมูลที่ไม่มั่นใจถึงแหล่งที่มา
- หลีกเลี่ยงเว็บไซต์อันตราย เช่น เว็บไซต์ลามก เว็บที่ผิดกฎหมาย

2. เวิร์ม (Worm)

จัดเป็นไวรัสคอมพิวเตอร์รูปแบบหนึ่ง แต่มีความรุนแรงกว่าไวรัสมาก นิยมเรียกกันว่า "หนอนอินเทอร์เน็ต" เพราะมันสามารถแพร่กระจายได้อย่างรวดเร็วโดยการคัดลอกตัวเองและส่งตัวเองไปยังคอมพิวเตอร์อื่นๆ สามารถติดได้หลายช่องทาง เช่น การรับส่งอีเมล การแชร์ไฟล์ร่วมกัน การแชตสนทนาผ่าน Instant Messaging เป็นต้น

3. ม้าโทรจัน (Trojan Horses)

เป็นไวรัสที่เปรียบเสมือนไส้ศึกในสงคราม ที่มันสามารถหลบเลี่ยงการตรวจพบและหลอกผู้ใช้ให้คิดว่าเป็นโปรแกรมธรรมดาทั่วๆ ไป ไม่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นได้ แต่จะใช้วิธีแฝงตัวอยู่ในลักษณะของไฟล์หรือ

โปรแกรม เพื่อหลอกให้ผู้ใช้เปิดไฟล์หรือดาวน์โหลดมาใช้ จากนั้นก็จะทำงานที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์

ลองชมวิดีโอนี้

<u>วิธีป้องกัน</u>

- สำรองเครื่องให้บริการหลายตัวเพื่อทำหน้าที่แทนกัน
- ใช้ Firewall เพื่อป้องกันการถูกโจมตีจากแฮคเกอร์
- ใช้ซอฟต์แวร์สำหรับการตรวจจับและทำลายโทรจัน

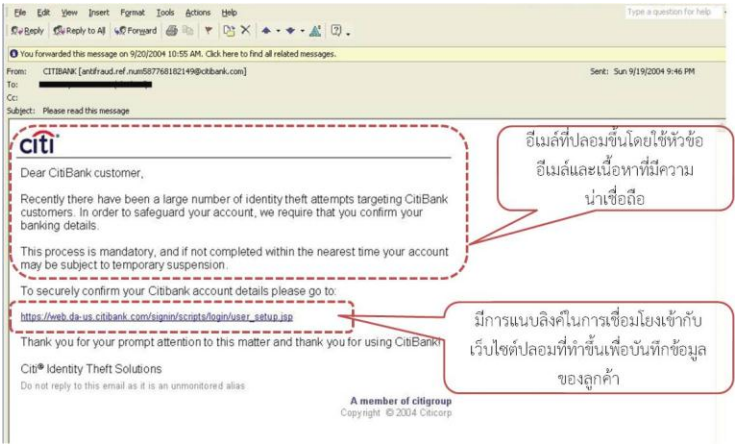
4. ฟิชชิ่ง (Phishing)

คำว่า Phishing ล้อเลียนมาจาก Fishing คือการตกปลา ลองนึกภาพตามว่าถ้าเหยื่อล่อที่ใช้ตกปลาก็คือวิธีที่ผู้ไม่หวังดีใช้หลอกลวงผู้เสียหาย ซึ่งที่พบส่วนมากจะเป็นการปลอมอีเมล และหน้าเว็บไซต์ให้มีรูปร่างหน้าตาเหมือนเว็บจริงจนทำให้ผู้เสียหายหลงเชื่อ โดยมักจะอาศัยเหตุการณ์สำคัญๆ ที่เกิดในช่วงเวลานั้น เพื่อเพิ่มโอกาสการหลอกลวงให้สำเร็จตามเป้าหมาย เช่น ในสถานการณ์ที่มีภัยธรรมชาติ อาจปลอมอีเมลเพื่อแจ้งว่าระบบของ

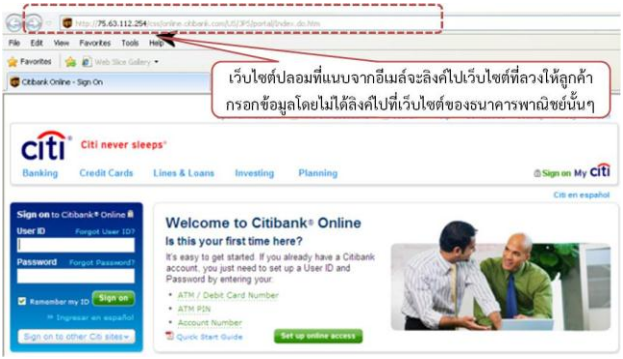
ธนาคารได้รับความเสียหาย โดยปลอมว่าเป็นอีเมลถูกส่งมาจากธนาคารที่ผู้เสียหายใช้บริการอยู่ แจ้งว่าธนาคารต้องการให้ลูกค้าเข้าไปยืนยันความถูกต้องของข้อมูลส่วนบุคคลผ่านทางลิงก์ที่แนบมาในอีเมล เมื่อผู้เสียหายคลิกที่ลิงก์ ก็พาไปยังหน้าเว็บปลอมที่ผู้ไม่หวังดีสร้างขึ้น เมื่อผู้เสียหายเข้าไปล็อกอิน ผู้ไม่หวังดีก็จะได้ทั้ง Username, Password ไปในทันที

Phishing เปรียบเสมือน "เหยื่อล่อตกปลา"

ลองชมวิดีโอนี้



ตัวอย่างของอีเมลและหน้าเว็บไซต์หลอกลวง มีอยู่มากมายเต็มไปหมดในโลกอินเทอร์เน็ต เช่นรูปนี้ เป็นรูปของสถาบันทางการเงินแห่งหนึ่ง หากสังเกตดีๆ จะเห็นว่า URL ที่แสดงขึ้นมา ไม่ใช่ URL ที่ถูกต้องของสถาบันการเงินนั้น



เว็บไซต์ปลอมที่แนบจากอีเมล์จะลิกค์ไปสู่เว็บไซต์ที่หลอกลวงให้ลูกค้ากรอกข้อมูล โดยไม่ได้ลิงค์ไปที่เว็บไซต์จริงของสถาบันการเงินนั้นๆ ดังรูป

<u>วิธีป้องกัน</u> - DO

- สังเกตระบบความปลอดภัยบนเว็บไซต์ เช่น HTTPS
- ลบอีเมลที่น่าสงสัย
- ติดตั้งโปรแกรม Anti-Virus, Anti-Spam และ Firewall

<u>วิธีป้องกัน – DON'T</u>

- ไม่เปิดลิงก์ที่แนบมาในอีเมลที่ไม่น่าเชื่อถือ
- พึงระวังการกรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่น่าเชื่อถือ

แล้วเว็บไซต์คุณล่ะ?

พบภัยคุกคามอินเทอร์เน็ตรูปแบบใดหรือไม่

☐ Virus

☐ Worm

☐ Trojan Horse

☐ Phishing

<u>หรือพบทุกข้อ?</u> "แต่อย่ากังวล ถ้ารู้ทันก็แก้ไข"

เคล็ด (ไม่) ลับ ป้องกันข้อมูลลูกค้ารั่วไหล

5 ขั้นตอนป้องกันข้อมูลลูกค้ารั่วไหล

1. รักษาความปลอดภัยให้กับเครือข่ายองค์กรด้วยการควบคุมการเข้าถึงทางกายภาพ
2. รักษาความปลอดภัยให้กับเครือข่ายองค์กรด้วยการควบคุมการเข้าถึงทางตรรกะ
3. ตรวจสอบการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
4. ป้องกันภัยคุกคามจากไวรัส
5. การป้องกันภัยคุกคามในเครือข่ายไร้สาย

Step 1 การควบคุมการเข้าถึงทางกายภาพ

ท่านกำหนดนโยบายความปลอดภัยเหล่านี้หรือยัง?

1. ทำการล็อกห้องคอมพิวเตอร์อย่างแน่นหนาเมื่อไม่ใช้งาน
2. จัดหายามรักษาความปลอดภัย
3. ติดตั้งกล้องวงจรปิดให้ครอบคลุมจุดเสี่ยง
4. ติดตั้งระบบดับเพลิง
5. จัดหา Back-Up Disk เพื่อสำรองข้อมูลอย่างสม่ำเสมอและไม่ควรเก็บไว้ในสถานที่เดียวกันกับระบบคอมพิวเตอร์นั้นๆ
6. นำระบบพิสูจน์บุคคลที่มีสิทธิ์เข้าถึงมาใช้ เช่น การพิสูจน์บุคคลด้วยลายนิ้วมือ เรตินา ลายเซ็น อุณหภูมิ และเสียง เป็นต้น

Step 2 การควบคุมการเข้าถึงทางตรรกะ

1. **การบันทึกประวัติข้อมูลส่วนตัวผู้ใช้ (User profiles) เพื่อ Log-in เข้าสู่ระบบ โดยทุกคนต้องประกอบด้วยชื่อผู้ใช้ รหัสผ่าน และสิทธิการใช้งาน "ช่องโหว่" ที่พึงระวัง**
    - ความหละหลวมในการจัดการบัญชีรายชื่อผู้ใช้ที่ลาออกจากบริษัทแล้ว
    - ไม่มีการเปลี่ยนแปลงสิทธิ์ในการเข้าใช้ระบบ
    - ขาดเครื่องมือค้นหาหรือตรวจสอบสิทธิในการเข้าใช้ระบบที่ง่ายและสะดวก

<u>5 เทคนิคป้องกันการรั่วไหลของรหัสผ่าน</u>

1. กำหนดรหัสผ่านที่มีความยาวไม่ต่ำกว่า 8 ตัวอักษร
2. ใช้อักขระพิเศษ เช่น @ ! : ; & เป็นต้น
3. รหัสไม่ควรตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้น
4. อย่าใช้รหัสผ่านเดียวกันในทุกๆ ระบบ เช่น การ Login ระบบ e-mail, ระบบสนทนาออนไลน์ (Chat) ระบบเว็บไซต์ที่เราเป็นสมาชิกอยู่ เป็นต้น
5. หมั่นเปลี่ยนรหัสผ่านทุก 3 - 6 เดือนต่อครั้งเป็นอย่างน้อย

2. การควบคุมความปลอดภัยโดยระบบปฏิบัติการ

โดยทั่วไปผู้พัฒนาแอปพลิเคชั่นและระบบปฏิบัติการจะพัฒนาโปรแกรมซ่อมเสริมระบบ ที่เรียกว่า "Patch" ซึ่งทำหน้าที่ในการซ่อมแซมระบบ แก้ไขข้อบกพร่อง และเพิ่มระบบรักษาความมั่นคงปลอดภัยให้กับระบบสม่ำเสมอ หากละเลย ไม่ดาว์นโหลด Patch มาซ่อมแซมระบบอย่าง

สม่ำเสมอ อาจทำให้ระบบปฏิบัติการมีช่องโหว่และข้อผิดพลาดสะสม จนกลายเป็นจุดอ่อนที่เสี่ยงต่อการถูกโจมตีได้จากภัยคุกคามอินเทอร์เน็ตได้

- ใช้โปรแกรมซ่อมเสริมระบบที่เรียกว่า “Patch”
- หมั่นซ่อมแซมระบบด้วย Patch

ระบบปฏิบัติการแบบเครือข่าย
จะเสี่ยงต่อการโจมตีของ “เวิร์ม” ที่อาศัยช่องโหว่
ของระบบเครือข่ายในการโจมตีได้

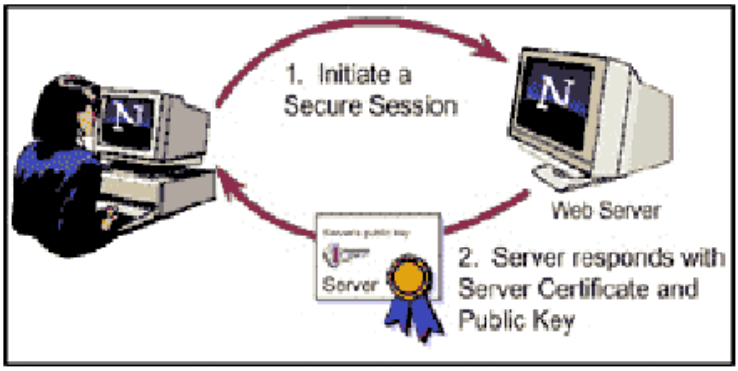
3. ติดตั้ง Firewall

เป็นระบบควบคุมการเข้าออกเครือข่าย ทำหน้าที่ปกป้องเครือข่ายภายในองค์กรจากการโจมตีจากภายนอก Firewall จะอนุญาตให้เฉพาะข้อมูลที่มีคุณลักษณะตรงกับเงื่อนไขที่กำหนดไว้ผ่านเข้าออกระบบเครือข่ายภายในเท่านั้น

Firewall ไม่สามารถป้องกันภัยคุกคามอินเทอร์เน็ตได้ทุกรูปแบบ
ไวรัสก็เป็นหนึ่งในนั้น จึงไม่สามารถรับรองได้ว่าความปลอดภัยหรือ
ความลับของข้อมูลจะมีอยู่ 100%

4. ใช้เทคโนโลยีแบบ Secure Socket Layer: SSL

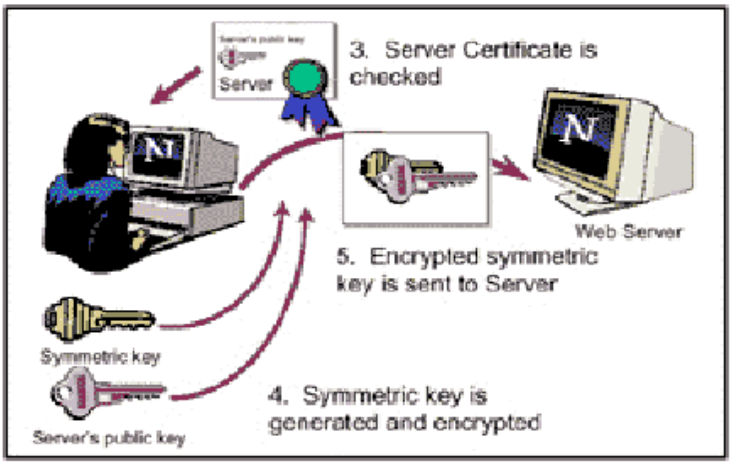
เป็นระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลบนเครือข่ายอินเทอร์เน็ต



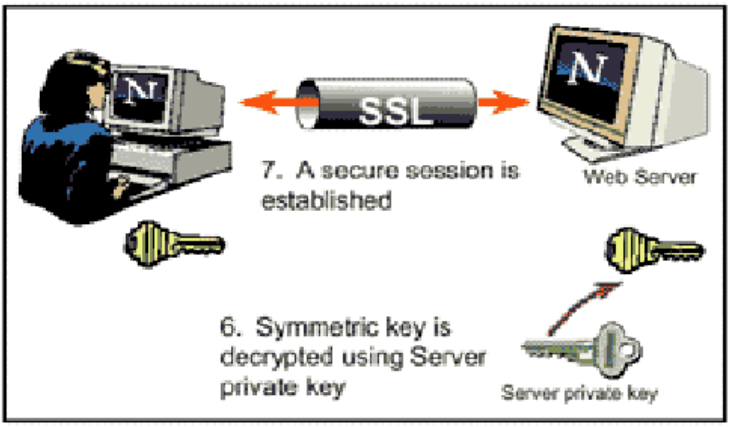
ในการทำพาณิชย์อิเล็กทรอนิกส์ หรือการทำธุรกรรมต่างๆผ่านอินเทอร์เน็ตนั้นสิ่งสำคัญที่จะขาดเสียไม่ได้เลย ได้แก่ระบบรักษาความปลอดภัยที่ดีในเว็บไซต์นั้นๆ ซึ่งในปัจจุบันมี อยู่ **2 แบบที่ใช้กันคือ SSL (Secure Sockets Layer) และ SET (Secure Electronic Transaction)** ซึ่งจะมีความซับซ้อน และมีค่าใช้จ่ายที่สูงกว่าแบบแรกจึงยังไม่เป็นที่นิยมใช้กัน

SSL นั้นจะใช้**เพื่อเข้ารหัส** (encrypt) **ข้อมูลตัวมันเองนั้น ใช้เพียงแค่การตรวจสอบหรือยืนยันได้เฉพาะฝั่งผู้ขายเท่านั้น** ว่ามีตัวตนจริงไม่สามารถยืนยันตัวผู้ซื้อได้ ซึ่ง SSL จะมีความเร็วในการทำงานมากกว่า PKI ประมาณ 10-100 เท่าและยังสามารถใช้งานกับบราวเซอร์ต่างๆ ได้

การทำงานจะเริ่มจาก ผู้ใช้งานเริ่มกระบวนการติดต่อ ไปยังเว็บเซิร์ฟเวอร์ที่มีระบบ SSL หลังจากนั้นเซิร์ฟเวอร์จะส่งใบรับรอง (Server Certificate) กลับมาพร้อมกับเข้ารหัส ด้วยกุญแจสาธารณะ (Public Key) ของเซิร์ฟเวอร์



ขั้นตอนต่อมาคอมพิวเตอร์ฝั่งผู้รับจะทำการตรวจสอบใบรับรองนั้นอีกทีเพื่อตรวจสอบตัวตนของฝั่งผู้ค้าหลังจากนั้นจะ**ทำการสร้างกุญแจสมมาตร** (Symmetric Key) **โดยการสุ่มและทำการเข้ารหัสกุญแจสมมาตรด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ที่ได้รับมา** เพื่อส่งกลับไปยังเซิร์ฟเวอร์

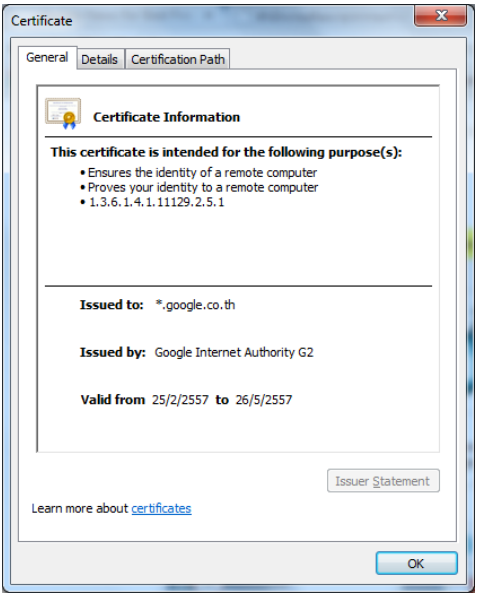


เมื่อเซิร์ฟเวอร์ได้รับแล้วก็จะทำการถอดรหัสด้วยกุญแจส่วนตัว (Private Key) ก็จะได้กุญแจสมมาตรของลูกค้ามาไว้ใช้ในการติดต่อสื่อสาร

หลังจากนั้นในการติดต่อสื่อสารกันก็ใช้การเข้ารหัสติดต่อสื่อสารกันได้อย่างปลอดภัย

ปกติการเข้าถึงเว็บไซต์ใดๆ นั้นจะมี URL ที่เป็น HTTP (Hypertext Transmission Protocol) เป็นมาตรฐาน แต่หากว่ากำลังเข้าสู่โหมด(Mode) รักษาความปลอดภัยของ SSL URL จะเปลี่ยนเป็น HTTPS (Hyper Text Transmission Protocol, Secure) **ส่วนอีกแห่งหนึ่งก็คือที่ Title Bar ด้านล่าง** ในระบบ SSL จะมีรูปแม่กุญแจสีเหลืองปรากฏอยู่ด้านซ้ายมือสำหรับ Internet Explorer ส่วน Netscape Communicator จะเป็นรูปกุญแจที่สมบูรณ์ (ไม่แตกหัก) สีเหลืองปรากฏอยู่ที่ด้านขวามือ

ตัวอย่างหน้าจอที่แสดงว่าอยู่บนเว็บไซต์ที่ใช้ระบบ SSL อยู่

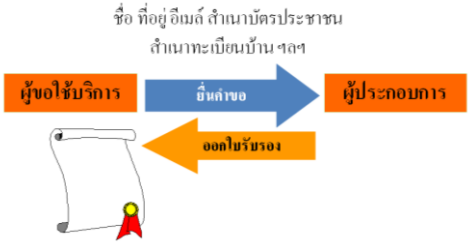


ตัวอย่างหน้าจอที่แสดงตัวตนของเว็บไซต์

วิธีนำ SSL มาใช้บนเว็บไซต์

สามารถขอใช้บริการจากผู้ให้บริการออกใบรับรอง (Certification Authority : CA*) เช่น RapidSSL, Verisign, Thawte , Comodo เป็นต้น

* CA เป็นผู้อนุมัติ SSL Certificate ให้แก่เว็บไซต์ เพื่อยืนยัน การมีตัวตนของเจ้าของเว็บไซต์และเพื่อยืนยันความสมบูรณ์ ของการเข้ารหัสข้อมูลผ่าน SSL



ขั้นตอนการขอใบรับรองจาก CA

<u>Step 3</u> ตรวจสอบการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

<u>ท่านกำหนดนโยบายความปลอดภัยเหล่านี้หรือยัง?</u>

1. นโยบายด้านสิทธิการเข้าถึงข้อมูลส่วนต่างๆ ของเว็บไซต์
2. ใครมีสิทธิที่จะเปลี่ยนแปลงแก้ไขข้อมูลในเว็บไซต์บ้าง
3. มีการจัดเก็บและตรวจสอบข้อมูลการใช้งานของผู้ใช้แต่ละคน
4. มีการกำหนดแผนป้องกันและกู้ภัยที่อาจเกิดขึ้นได้อนาคต

<u>Step 4</u> ป้องกันภัยคุกคามจากไวรัสคอมพิวเตอร์

1. ใช้โปรแกรมป้องกันไวรัส (Anti Virus)
2. อัพเดทซอฟต์แวร์ป้องกันไวรัสอย่างสม่ำเสมอ
3. ไม่ควรดาวน์โหลดโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือ
4. สแกนไฟล์แนบท้ายของอีเมลทุกฉบับ หรือแม้แต่อีเมลจากคนรู้จัก
5. อย่าตั้งค่าให้โปรแกรมอีเมลเปิดไฟล์ที่แนบมาโดยอัตโนมัติ ควรจะต้องตรวจสอบก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

Anti Virus สามารถขัดขวางและกำจัดไวรัสคอมพิวเตอร์
ซึ่งรวมไปถึงโปรแกรมที่เป็นอันตรายอื่นๆ ได้

บัญญัติ 5 ประการเกี่ยวกับ Anti Virus

1. Microsoft แจก Antivirus ให้ฟรี สามารถดาวน์โหลดได้ที่ http://windows.microsoft.com/en-us/windows/security-essentials-download
2. ระวัง Antivirus ปลอม จะกลายเป็นไวรัสเสียเอง
3. ถ้าไม่แน่ใจอย่าติดตั้ง Antivirus แปลกๆ ควรใช้ที่จำหน่ายตามร้านค้าไอทีปลอดภัยกว่า
4. หมั่น Update Antivirus อย่างสม่ำเสมอ และสแกนระบบเป็นประจำ
5. พึงระลึกเสมอว่า **“ไม่มีอะไรปลอดภัย 100% ควรใช้ความระมัดระวังอยู่เสมอแม้มี Antivirus แล้ว”**

<u>Step 5</u> การป้องกันภัยคุกคามในเครือข่ายไร้สาย

1. ติดตั้ง Firewall ให้กับ Gateway ของเครือข่ายไร้สาย
2. เลือกใช้สัญญาณดิจิทัลในการส่งข้อมูลผ่านโทรศัพท์มือถือ
3. นำเทคโนโลยีความปลอดภัยแบบ SSL มาใช้
4. ติดตั้งโปรแกรม Anti-virus และอัพเดตสม่ำเสมอ
5. อัพเดตระบบปฏิบัติการและซอฟต์แวร์ที่ใช้อย่างสม่ำเสมอ

แล้วเว็บไซต์คุณล่ะ

มีวิธีการรักษาความปลอดภัยต่อข้อมูลลูกค้าบ้างหรือไม่ ?

☐ การควบคุมการเข้าถึงทางกายภาพ

☐ การควบคุมการเข้าถึงทางตรรกะ

☐ มีตรวจสอบการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

☐ ป้องกันภัยคุกคามจากไวรัส

☐ ป้องกันภัยคุกคามในเครือข่ายไร้สาย