ความปลอดภัยของเทคโนโลยีสารสนเทศ

ความหมายของความปลอดภัยของเทคโนโลยีสารสนเทศ

กระบวนการที่เกี่ยวข้องกับการป้องกันและตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ขั้นตอนการป้องกันจะช่วยให้ ผู้ที่ใช้งานสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่างๆ ถูกเข้าใช้งานโดยผู้ที่ไม่ได้รับสิทธิ์ ส่วนการตรวจสอบจะทำให้ทราบได้ว่ามีใครกำลังพยายามที่จะบุกรุกเข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ ผู้บุกรุกทำอะไรกับระบบบ้าง รวมทั้งการป้องกันจากภัยคุกคาม (Threat) ต่างๆ

ภัยคุกคามของเทคโนโลยีสารสนเทศ

อาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ (Computer Crimes) หมายถึง การกระทำที่ผิดต่อกฎหมายโดยการใช้คอมพิวเตอร์ หรือทำลายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่น

อาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ แบ่งเป็น 4 ลักษณะ คือ

1.การเจาะระบบรักษาความปลอดภัย ทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ

2.การเจาะเข้าไปในระบบสื่อสาร และการรักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ

3.เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัย ของระบบปฏิบัติการ(OS)

4.เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล เป็นช่องทางในการกระทำความผิด

รูปแบบการก่ออาชญากรรมคอมพิวเตอร์

แบ่งออกเป็น 9 ประเภท

1.การขโมยข้อมูลทางอินเตอร์เน็ต ซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ

2.อาชญากรนำเอาระบบการสื่อสารมาปกปิดความผิดของตนเอง

3.การละเมิดสิทธิ์ปลอมแปลงรูปแบบ เลียนแบบระบบซอฟต์แวร์โดยมิชอบ

4.ใช้คอมพิวเตอร์แพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม

รูปแบบการก่ออาชญากรรมคอมพิวเตอร์

5.ใช้คอมพิวเตอร์ฟอกเงิน

6.อันธพาลทางคอมพิวเตอร์ที่เข้าไปก่อกวน ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไป ระบบการจราจร

7.หลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม

8.แทรกแซงข้อมูลแล้วนำข้อมูลนั้นมาเป็นประโยชน์ต่อตนโดยมิชอบ

9.ใช้คอมพิวเตอร์แอบโอนเงินบัญชีผู้อื่นเข้าบัญชีตัวเอง

ภัยคุกคามที่มีต่อระบบต่างๆ (Computer Threats)

1. ภัยต่อระบบฮาร์ดแวร์ (Hardware Security Threats)

ภัยที่คุกคามต่อระบบ Hardware นี้ สามารถจำแนกได้เป็น 3 กลุ่มใหญ่ๆ ดังนี้คือ

1.1 ภัยที่มีต่อระบบการจ่ายไฟฟ้า

1.2 ภัยที่เกิดจากการทำลายทางกายภาพโดยตรง ต่อระบบคอมพิวเตอร์นั้นๆ

1.3 ภัยจากการลักขโมยโดยตรง

ภัยคุกคามที่มีต่อระบบต่างๆ (Computer Threats)

2. ภัยที่มีต่อระบบซอฟต์แวร์ (Software Security Threats) แบ่งได้เป็น 3 พวกใหญ่ๆ คือ

- การลบซอฟต์แวร์ หรือการลบเพียงบางส่วน ของซอฟต์แวร์นั้นๆ
- การขโมยซอฟต์แวร์ (Software Theft)
- การเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Software Modification)
- ขโมยข้อมูล (Information Leaks)

ภัยคุกคามที่มีต่อระบบต่างๆ (Computer Threats)

3. ภัยที่มีต่อระบบข้อมูล (Data Threats)

- การที่ข้อมูลอาจถูกเปิดเผยโดยมิได้รับอนุญาต
- การที่ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขเพื่อผลประโยชน์โดยมิได้มีการตรวจสอบแก้ไข
- การที่ข้อมูลนั้นถูกทำให้ไม่สามารถนำมาใช้งานได้

มัลแวร์

มัลแวร์ (Malware) ย่อมาจาก "Malicious Software" ซึ่งหมายถึงโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อคอมพิวเตอร์และเครือข่าย ที่บุกรุกเข้าไปติดอยู่ในระบบคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ และสร้างความเสียหายให้กับระบบคอมพิวเตอร์นั้นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่าย หรือระบบสื่อสารข้อมูล ไวรัสก็อาจแพร่ระบาดได้เช่นกัน หรือเป็นคำที่ใช้เรียกโปรแกรมที่มีจุดประสงค์ร้ายต่อ ระบบคอมพิวเตอร์ทุกชนิดแบบรวมๆ

ไวรัส (Virus)

คือ โปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ แต่ ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปเกิดจากการที่ผู้ใช้เป็นพาหะ นำไวรัสจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง

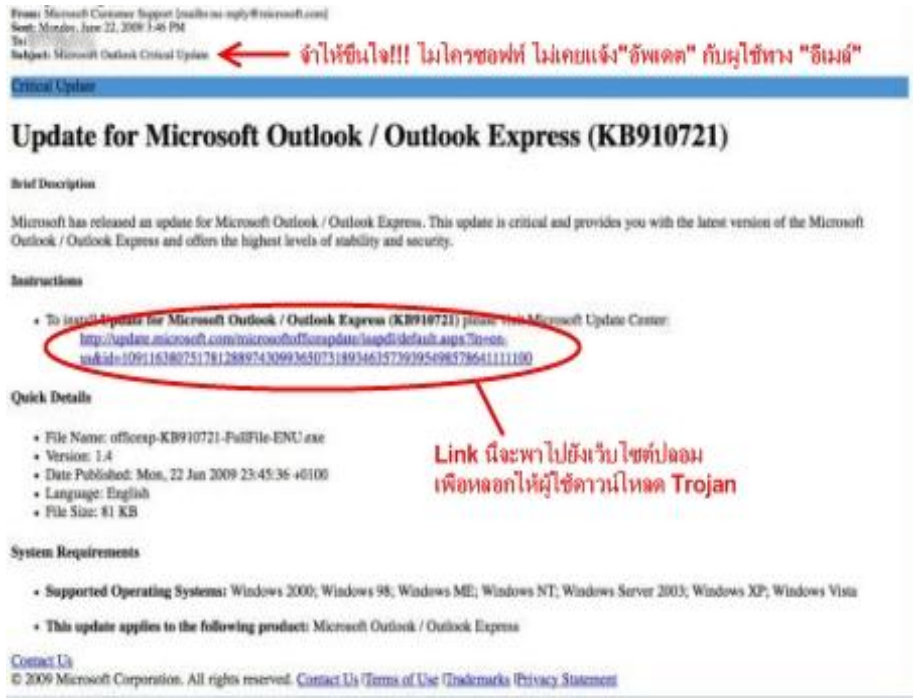
เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต

โปรแกรมที่สามารถคัดลอกตัวเองและสามารถส่งตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้อย่างอิสระ โดยอาศัยอีเมลล์, ช่องโหว่ของระบบปฏิบัติการหรือการเชื่อมต่อที่ไม่มีการป้องกัน มันจะไม่แพร่เชื้อไปติดไฟล์อื่น มักจะสร้างความเสียหายให้กับระบบเครือข่ายและระบบอินเทอร์เน็ต

โทรจันฮอร์ส(Trojan Horse)

โทรจันฮอร์ส หมายถึงโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ เช่น เกม สกรีนเวฟเวอร์ เป็นต้น ต้องอาศัยการหลอกคนใช้ให้ดาวน์โหลดเอาไปใส่เครื่องเองหรือด้วยวิธีอื่นๆ สิ่งที่มันทำคือเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาควบคุมเครื่องที่ติดเชื้อจากระยะไกล

Link หลอกให้ผู้ใช้ดาวน์โหลด Trojan



Trapdoor หรือ Backdoor

Backdoor เป็นรูรั่วในการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่ผู้ออกแบบหรือผู้ดูแลจงใจทิ้งไว้ มีความหมายเดียวกับประตูดัก (trap door) ซึ่งเป็นกลไกลับทาง software หรือ hardware ที่ใช้ในการข้ามผ่านการควบคุมความปลอดภัย backdoor จะอนุญาตให้มีการเข้าใช้ระบบโดยไม่ผ่านการตรวจสอบ

Bomb

แบ่งออกได้เป็น 2 อย่างคือ

- ***Time Bomb คือ โปรแกรมที่ระให้เวลาที่ตั้งไว้มาถึงก่อนที่จะทำการปล่อยวิธีการทำร้ายระบบออกมา***
- ***Logic Bomb คือโปรแกรมที่รอให้เหตุการณ์ที่เหมาะสมอย่างหนึ่งตามที่ถูกโปรแกรมไว้เกิดขึ้นก่อน แล้วจึงจะเริ่มทำการโจมตีระบบ***

Rabbit

โปรแกรม Virus พวกหนึ่ง ที่มีลักษณะเด่นเฉพาะตัวคือ จะสร้างตัวของมันเองขึ้นมามากๆ ที่สุดเท่าที่จะมากได้ ด้วยจุดประสงค์คือการใช้ทรัพยากรของระบบให้เกือบหมดหรือหมดไปโดยมิให้มีเหลือไว้ใช้กับงานของโปรแกรมอื่นๆ เลย

โจ๊กแอพพลิเคชัน

โจ๊กแอพพลิเคชันเป็นซอฟต์แวร์ที่ออกแบบเพื่อสร้างความสนุกสนาน แต่ก็ทำให้เสียเวลาการทำงานของระบบคอมพิวเตอร์ แอพพลิเคชันประเภทนี้มีมานานพร้อม ๆ กับการเริ่มใช้คอมพิวเตอร์ เนื่องจากแอพพลิเคชันประเภทนี้มิได้ออกแบบเพื่อการทำลาย

โฮแอ็กส์ (Hoaxes)

โดยทั่วไปโฮแอ็กส์ (Hoaxes) หมายถึง โปรแกรมที่เขียนขึ้นเพื่อหลอกให้ผู้ใช้ทำบางอย่างให้ โดยโฮแอ็กส์จะใช้เทคนิคทางด้านวิศวกรรมสังคม (Social Engineering) เพื่อหลอกให้ผู้ใช้งานคอมพิวเตอร์ทำบางอย่างให้

ฟิชชิ่ง(Phishing)

ฟิชชิ่ง คือการฉ้อโกง ดังเช่นรูปแบบฟิชชิ่งแบบหนึ่งในอีกหลายๆรูปแบบ ที่พยายามหลอกล่อให้เหยื่อจ่ายเงินหรือโอนเงิน และมีเทคนิคหลอกลวงที่สมบูรณ์แบบ โดยใช้ความเชื่อถือของผู้คนทั่วไปที่มีต่อองค์กรใหญ่ๆที่จดทะเบียนถูกต้อง ตามกฎหมาย

ฟิชชิ่ง(Phishing)

ฟิชชิ่ง(Phishing)

สแปม (Spam)

สแปม (Spam) คือ การส่งอีเมล์ยังผู้ใช้จำนวนมาก โดยมีจุดประสงค์เพื่อการโฆษณาสินค้าหรือบริการ สแปมจัดอยู่ในประเภทสิ่งที่ก่อให้เกิดความรำคาญ

สปายแวร์ (Spyware)

บางทีก็รู้จักกันในชื่อ สปายบ็อท (Spybot) หรือแทร็คกิ้งซอฟต์แวร์ (Tracking software) สปายแวร์เป็นโปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่ทำกิจกรรมบางอย่างในเครื่องคอมพิวเตอร์ โดยที่ไม่ได้รับความยินยอมจากผู้ใช้ เช่น การเก็บข้อมูลส่วนตัวของผู้ใช้ การปรับเปลี่ยนเซตติ้งของบราวเซอร์ ลดประสิทธิภาพโดยรวมของคอมพิวเตอร์ไปจนถึงการละเมิดสิทธิส่วนบุคคลของผู้ใช้

แอดแวร์ (Adware)

แอดแวร์ (Adware) เป็นโปรแกรมโฆษณาสินค้าซึ่งจะเปิดป๊อบอัพวินโดวส์ แอดแวร์ส่วนใหญ่จะรวมอยู่ในแอพพลิเคชันที่ให้ใช้ได้ฟรีและจะฝังตัวอยู่ เนื่องจากได้รับความยินยอมจากผู้ใช้ แอดแวร์จะติดตั้งก็ต่อเมื่อผู้ใช้ได้ยินยอมตามข้อตกลงเกี่ยวกับลิขสิทธิ์

อินเทอร์เน็ตคุกกี้ (Internet Cookies)

อินเทอร์เน็ตคุกกี้ (Internet Cookies) คือ เท็กซ์ไฟล์ที่เก็บไว้ที่เครื่องคอมพิวเตอร์ของผู้ใช้โดยเว็บไซต์ที่เข้าไปเยี่ยมชม คุกกี้จะเก็บข้อมูลบางอย่างที่เว็บไซต์นั้นใช้เมื่อครั้งหน้าที่ผู้ใช้เข้าไปเยี่ยมชมอีกครั้ง ซึ่งส่วนใหญ่จะเป็นข้อมูลที่ใช้บอกว่าเป็นผู้ใช้คนนี้ นอกจากนี้ในไฟล์อาจมีข้อมูลอื่น ๆ ก็ได้

ภัยคุกคามอื่นๆบนอินเทอร์เน็ต

- *Chat Room*
- *Webboard*

การรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ

แนวความคิดของการรักษาความปลอดภัยระบบคอมพิวเตอร์จะมีเป้าหมายทั่วไปอยู่ 3 ประการ

- เป้าหมายแรก คือ ความลับของข้อมูล (Data confidentiality)
- เป้าหมายที่สอง คือ ความเชื่อถือได้ของข้อมูล (Data integrity)
- เป้าหมายที่สาม การที่ระบบยังคงทำงานอยู่ได้ (System availability)

วิธีการสังเกตความปลอดภัยของเว็บไซต์

1.ชื่อเสียงของเว็บไซต์

2.เว็บไซต์จะต้องสนับสนุนระบบ SSL (Secure Socket Layer)

3.เว็บไซต์ควรจะได้รับการรับรองเรื่องความปลอดภัย

4.นโยบายส่งเสริมความมั่นใจหลังการขาย

วิธีป้องกันให้ปลอดภัยจากไวรัสคอมพิวเตอร์

1. ตัดการเชื่อมต่อเครือข่ายก่อนการติดตั้งระบบปฏิบัติการ
2. ซอฟต์แวร์ที่ใช้งานปลอดภัยหรือยัง
3. การแชร์ไฟล์ และการรับ-ส่งไฟล์ต่างๆ
4. การสำรองข้อมูล
5. ติดตามข่าวสารต่างๆ

ข้อห้าม/ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไกลห่างจากไวรัส สปายแวร์

1. ห้ามเปิดไฟล์หรือดาวน์โหลดไฟล์ที่แนบมากับเมล์ ที่เราไม่ทราบชื่อผู้ส่งหรือที่มาแน่ชัด
2. ห้ามเปิดไฟล์หรือดาวน์โหลดไฟล์ที่แนบมากับเมล์ ทั้งที่เรารู้ว่าส่งมาจากเพื่อนหรือคนรู้จัก
3. ห้ามเปิดไฟล์หรือดาวน์โหลดไฟล์ที่แนบมากับเมล์ ที่เราเห็นว่าหัวข้อหรือ subject เมล์นั้นๆ แปลกๆ หรือเป็นที่น่าสงสัย
4. ควรลบสแปมเมล์ หรือเมล์ลูกโซ่ และไม่ควรส่งต่ออีก

ข้อห้าม/ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไกลห่างจากไวรัส สปายแวร์

5. เช็คที่มาที่ไปของไฟล์ที่จะดาวน์โหลดมาจากอินเตอร์เน็ต และควรทำการแสกนไวรัสทุกครั้ง
6. หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่มาที่ไม่ใช่เว็บไซต์ เช่น Usenet group, ผ่านโปรแกรม IRC, Instant messaging ที่เราไม่รู้จัก
7. หมั่นอัพเดทโปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพราะไวรัสสปายแวร์ มีการปรับปรุง และเกิดใหม่อยู่เสมอ

ข้อห้าม/ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไกลห่างจากไวรัส สปายแวร์

8. หมั่นทำการ backup สำรองข้อมูล สำรองไฟล์ที่สำคัญบ่อยๆ ซึ่งอาจจะเขียนลง CD,DVD หรือใส่ External HD สำรองก็ได้

9. หมั่นอัพเดทวินโดวส์หรือระบบปฏิบัติการที่เราใช้ รวมไปถึงโปรแกรมเบราเซอร์ และโปรแกรมเมล์ไครเอนต์

10. ให้รอบคอบ อย่าประมาทในการทำธุรกรรมใดๆผ่านอินเตอร์เน็ต เพราะเราอาจจะโดนฟิชชิ่ง หรือโดนดักจับข้อมูลส่วนตัว

ข้อห้าม/ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไกลห่างจากไวรัส สปายแวร์

11. ห้ามเปิดข้อความ หรือคลิกลิงค์ใดๆ ที่ส่งผ่านมาทางโปรแกรมแชท MSN หรือโปรแกรมแชทอื่นๆ ที่เราไม่รู้จักที่มาหรือคนที่ส่งมาหาเรา

12. ควรเปิดการใช้ Firewall หรือกำแพงไฟ ซึ่งอาจจะเป็นแบบ Hardware Firewall หรือที่เป็น Software Firewall ยกตัวอย่างเช่น เปิดการใช้ Firewall ในวินโดวส์ทุกครั้งที่มีการติดต่อกับเครือข่ายภายนอก

ข้อห้าม/ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไกลห่างจากไวรัส สปายแวร์

13. หมั่นเช็คแอคเค้าท์ของเราที่ใช้ในการทำธุรกรรมทางอินเตอร์เน็ต เช่น การจับจ่าย ซื้อของผ่านเน็ต หรือการจ่ายค่าสาธารณูปโภคต่างๆ รวมไปถึงดูรายงาน statement การเข้า-ออก ของเงินหรือเครดิต เพราะถ้าหากเกิดปัญหาใดๆ จะได้แก้ไขได้ทันท่วงที

ข้อควรปฏิบัติทั่วๆ ไป เพื่อช่วยเพิ่มความปลอดภัยในการใช้งานคอมพิวเตอร์

1. เปิดใช้งานซอฟต์แวร์รักษาความปลอดภัยและทำการอัพเดทให้ทันสมัยอยู่เสมอ
2. ติดตั้งผลิตภัณฑ์และโซลูชั่นที่จะช่วยปกป้องการใช้งานอินเทอร์เน็ตหรือการดาวน์โหลดไฟล์ลงเครื่องคอมพิวเตอร์แบบครบวงจร
3. ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ป้องกันภัยที่ใช้ว่า ครอบคลุมการป้องกันทั้งระบบอีเมล์ เครือข่ายแบบเพียร์ทูเพียร์ และโปรแกรมแอพพลิเคชั่นการประมวลผลที่ใช้ทั้งหมด

ข้อควรปฏิบัติทั่วๆ ไป เพื่อช่วยเพิ่มความปลอดภัยในการใช้งานคอมพิวเตอร์

4. ปรับใช้เทคโนโลยีที่ทันสมัย

5. ใช้เว็บเบราว์เซอร์เวอร์ชันล่าสุดและทำการติดตั้งอัพเดทความปลอดภัยเป็นประจำ

6. ให้เลือกใช้ปลั๊ก-อินเว็บเบราว์เซอร์ที่ไม่มีการใช้งานสคริปต์

7. ตรวจสอบกับผู้ให้บริการอินเทอร์เน็ต (ISP) ที่ใช้บริการอยู่ว่าระบบเครือข่ายของผู้ให้บริการนั้นมีระบบป้องกันมัลแวร์หรือไม่

ข้อควรปฏิบัติทั่วๆ ไป เพื่อช่วยเพิ่มความปลอดภัยในการใช้งานคอมพิวเตอร์

8. ในกรณีที่ใช้ระบบปฏิบัติการวินโดว์ของไมโครซอฟต์ ให้ทำการอัพเดทเป็นประจำ

9. ติดตั้งใช้งานโปรแกรมไฟร์วอลล์ และทำการตรวจสอบและอัพเดทโปรแกรมอย่างสม่ำเสมอ

10. ตรวจสอบให้แน่ใจว่าโซลูชั่นหรือซอฟต์แวร์รักษาความปลอดภัยที่ใช้งานอยู่ได้อัพเดทฐานข้อมูลที่ทันสมัยอยู่เสมอ

ข้อควรปฏิบัติ ที่ช่วยเพิ่มความปลอดภัยในการใช้งานระบบอีเมล์

1. ตรวจสอบให้แน่ใจว่าใช้งานโปรแกรมป้องกันสแปมสำหรับแต่ละที่อยู่อีเมล์ที่ใช้งานอยู่
2. ให้ระมัดระวังอีเมลที่ได้รับจากผู้ส่งที่ท่านไม่รู้จักหรือไม่ คุ้นเคย
3. หากท่านได้รับอีเมลที่น่าสงสัย ให้ทำการรายงานหรือ แจ้งให้กับผู้ที่มีหน้าที่ดูหรือรับผิดชอบระบบอีเมลทราบ ในทันทีเพื่อทำการตรวจสอบ

ข้อควรปฏิบัติ ที่ช่วยเพิ่มความปลอดภัยในการใช้งานระบบอีเมล์

4. ก่อนทำการเปิดไฟล์ที่แนบมากับอีเมลให้ทำการสแกนด้วยโปรแกรมป้องกันไวรัสก่อน เสมอ และหากมีการส่งไฮเปอร์ลิงค์มากับอีเมลถ้าเป็นไปได้ไม่ควรทำการคลิกลิงค์ดังกล่าว แต่ให้วิธีการพิมพ์ยูอาร์แอลของลิงค์ในเว็บเบราว์-เซอร์แทน

5. ให้ระลึกไว้เสมอและอย่าหลงเชื่ออีเมลที่ร้องขอข้อมูลเกี่ยวกับรายละเอียด บัญชีธนาคาร บัตรเครดิต หรือข้อมูลส่วนตัวอื่นๆ

ข้อควรปฏิบัติ ที่ช่วยเพิ่มความปลอดภัยในการใช้งานระบบอีเมล์

6. ไม่ควรทำการส่งอีเมลที่มีเนื้อหาหรือข้อมูลเกี่ยวกับการเงินของท่านถึงใครโดยเด็ดขาด

ข้อควรปฏิบัติ ที่เพิ่มความปลอดภัยในการใช้งานอินเทอร์เน็ตและการดาวน์โหลดข้อมูล

1. ใช้บริการ Web Reputation ทำการตรวจความปลอดภัยและความน่าเชื่อถือของเว็บไซต์
2. ใช้ความระมัดระวังในการเข้าเว็บไซต์ที่ต้องการให้ท่านทำการติดตั้ง ซอฟต์แวร์ก่อนเข้าชม แนะนำว่าไม่ควรติดตั้งโปรแกรมดังกล่าว
3. ให้อ่านและทำความเข้าใจกับเงื่อนไขต่างๆ ใน "End User License Agreement"

ข้อควรปฏิบัติ ที่เพิ่มความปลอดภัยในการใช้งานอินเทอร์เน็ตและการดาวน์โหลดข้อมูล

4. หากจำเป็นต้องป้อนข้อมูลส่วนตัวให้ป้อนเฉพาะข้อมูลเท่าที่จำเป็นจริงๆ เท่านั้น และบนเว็บไซต์ที่มี การเข้ารหัสข้อมูลเท่านั้น

5. ระมัดระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ ดังนั้นควรหลีกเลี่ยงการใส่ข้อมูลสำคัญ ไม่ใช้ระบบช่วยจำ Username และ Password

ข้อควรปฏิบัติ ที่เพิ่มความปลอดภัยในการใช้งานอินเทอร์เน็ตและการดาวน์โหลดข้อมูล

6.หมั่นเปลี่ยน Password บ่อยๆ เพื่อป้องกันการแอบขโมย Password

7.หมั่นลบ Temporary Internet Files, Cookies และ History เป็นประจำ

8.ควรทำการ Logoff หรือ Logout ทุกครั้งหลังการใช้งานเรียบร้อยแล้ว

มาตรฐานความปลอดภัยของเทคโนโลยีสารสนเทศ

มาตรฐานความปลอดภัยของข้อมูล

- การรักษาความลับของข้อมูล (Confidentiality)
- การคงไว้ซึ่งความถูกต้องและครบถ้วนของข้อมูล (Integrity)
- การพร้อมให้ใช้งานเมื่อต้องการ (Availability)

แม่แบบของการบริหารความปลอดภัยข้อมูล

ปัจจุบันมีแม่แบบของการบริหารความปลอดภัยข้อมูลมากมายขึ้นอยู่กับว่าใครเป็นผู้ให้บริการ แต่แม่แบบที่ได้รับความนิยมมากที่สุด และได้กำหนดให้เป็นมาตรฐานนานาชาติ คือ BS 7799 ซึ่งเป็นมาตรฐานที่พัฒนาโดยประเทศอังกฤษ

แม่แบบของการบริหารความปลอดภัยข้อมูล

มาตรฐานนี้ประกอบด้วย 2 ส่วนคือ

- *BS 7799-1 ซึ่งต่อมาได้เปลี่ยนมาตรฐาน ISO/IEC 17799 : Information Technology Code of Practice for Information Security Management*
- *BS 7799-2 ซึ่งต่อมาได้รับการยอมรับเป็นมาตรฐาน ISO 27001 : Information Security Management : Specification with Guidance for Use*

มาตรฐาน BS 7799-1 (ISO/IEC 17799)

มาตรฐาน ISO/IEC 17799 เริ่มแรกได้ประกาศใช้เมื่อปี 2000 เป็นมาตรฐานสากลด้านการจัดการความปลอดภัยของข้อมูล ซึ่งประกอบด้วย 10 โดเมน และต่อมาได้มีการปรับปรุงอีกครั้งเมื่อปี 2005 และปรับให้มี 11 โดเมน มาตรฐาน ISO 17799 แบ่งออกเป็น 11 โดเมน

มาตรฐาน BS 7799-2 (ISO 27001)

ในส่วนที่สองของ BS 7799 หรือในอีกชื่อหนึ่งคือ ISO/IEC 27001 เป็นมาตรฐานเกี่ยวข้องกับการบริหารการรักษาความปลอดภัยข้อมูล และเป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยข้อมูล (The Information Security Management System (ISMS)) โดยใช้โมเดลการบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการสร้าง และพัฒนาระบบการรักษาความปลอดภัย

มาตรฐาน BS 7799-3

เป็นแนวทางในการบริหารความเสี่ยงของการรักษาความปลอดภัยข้อมูล และเป็นแนวทางในการทำมาตรฐาน BS 7799-2 และเหมาะสำหรับองค์กรทุกขนาด โดยเนื้อหาที่สำคัญของมาตรฐานนั้นประกอบด้วย

- *ความเสี่ยงเกี่ยวกับความปลอดภัยของข้อมูลในองค์กร*
- *การประเมินความเสี่ยง*
- *วิธีปฏิบัติเพื่อลดความเสี่ยงและการบริหารการตัดสินใจ*
- *การดำเนินกิจกรรมเกี่ยวกับการบริหารความเสี่ยง*