สารบัญ

บทนำ 6

บทที่ 1 วัตถุประสงค์และบทบาทหน้าที่ของแกนนำลูกเสือไซเบอร์ 7

1. 1 ความหมายของลูกเสือ 8

1.2 ความหมายของระบบสารสนเทศ 8

1.3 ความหมายของลูกเสือไซเบอร์ 8

1.4 บทบาทหน้าที่ของลูกเสือไซเบอร์ 8

บทที่ 2 สถิติภัยคุกคามจากการใช้งานอินเทอร์เน็ต 9

2.1 สถิติการใช้งานอินเทอร์เน็ตทั่วโลก 10

2.2 สถิติการใช้งานอินเทอร์เน็ตในประเทศไทย 10

2.3 สถิติภาพรวมการใช้เครือข่ายสังคมออนไลน์และการโจมตีทางอินเทอร์เน็ต 11

2.4 วิวัฒนาการลักษณะการโจมตีทางคอมพิวเตอร์และอินเทอร์เน็ต 12

บทที่ 3 ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต 13

3.1 มัลแวร์ (Malware) 14

3.1.1 ไวรัสคอมพิวเตอร์ (Computer Virus) 14

3.1.2 หนอนคอมพิวเตอร์ (Computer Worm) 15

3.1.3 ม้าโทรจัน (Trojan Horse) 15

3.1.4 Backdoor 15

3.1.5 สปายแวร์ (Spyware) 16

3.2 การโจมตีแบบ DoS/DDoS 16

3.3 BOTNET หรือ “Robot network” 16

3.4 ข้อมูลขยะ (Spam) 17

3.5 Phishing 17

3.6 Sniffing 17

3.7 วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต 17

บทที่ 4 วิธีป้องกันตัวเองจากภัยคุกคามทางอินเทอร์เน็ต 21

4.1 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต 22

4.2 กรณีศึกษาธุรกรรมออนไลน์ 25

บทที่ 5 ศัพท์ทางเทคนิคที่เกี่ยวข้องการหาข่าว และปฏิบัติการหาข้อมูลข่าวสาร 27

5.1 หัวใจหลักของปฏิบัติการข้อมูลข่าวสาร (Information Operations) 28

5.2 องค์ประกอบหลักของปฏิบัติการข้อมูลข่าวสาร 28

5.2.1 การปฏิบัติการจิตวิทยา (Psychological Operations: PSYOP) 28

5.2.2 การลวงทางทหาร (Military Deception: MILDEC) 28

5.2.3 การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security : OPSEC) 28

5.2.4 การสงครามอิเล็กทรอนิกส์ (Electronic Warfare : EW) 29

5.2.5 การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations: CNO) 29

5.3 คำศัพท์ที่ควรรู้สำหรับการข่าว และด้านความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ 29

5.3.1 การรักษาความลับ (Confidentiality=C) 29

5.3.2 การรักษาความถูกต้องสมบูรณ์ (Integrity=I) 29

5.3.3 การรักษาความพร้อมใช้ของสารสนเทศเมื่อต้องการเข้าถึง (Availability=A) 29

5.3.5 การไม่สามารถปฏิเสธความรับผิดชอบในการทำธุรกรรม (Non-Repudiation) 30

บทที่ 6 การค้นหารายชื่อผู้จดทะเบียนทางอินเทอร์เน็ต 31

6.1 หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับพัฒนาอินเทอร์เน็ต 32

6.1.1. สมาคมอินเทอร์เน็ต หรือ ไอซ็อก (ISOC : Internet Society) 32

6.1.2 ไอเอบี (IAB : Internet Architecture Board) 32

6.1.3. ICANN (Internet Cooperation for Assigned Names and Number) 32

6.2 IP Address คืออะไร ? 34

6.2.1 IP Version 4 (IPv4) 34

6.2.2 คลาส (Class) 34

6.2.3 ไอพีส่วนตัว (Private IP) 34

6.2.4 ไอพีสาธารณะ (Public IP) 34

6.2.5 การแปลงไอพี (NAT) 35

6.2.6 IP Address version 6 (IPv6) 35

6.3 โดเมนเนม (Domain Name) 35

6.4 การจดทะเบียนชื่อโดเมน 36

6.5 แผนที่อินเทอร์เน็ต 37

บทที่ 7 ความรู้เบื้องต้นระบบค้นหาข้อมูล 40

7.1 เทคโนโลยีของระบบค้นหาข้อมูล(Search engine).....41

7.2 ชนิดของเว็บไซต์ค้นหาข้อมูลทางอินเทอร์เน็ต 42

7.3 คำอธิบายการค้นหาบางส่วนที่เป็นประโยชน์.....43

บทที่ 8 หลักการและเทคนิคการค้นหาข้อมูลทางอินเทอร์เน็ต 44

8.1 เทคนิคการค้นหาข้อมูลจาก Google ในเชิงลึก.....45

8.1.1 ค้นหาดูเฉพาะ Title ของเว็บไซต์.....45

8.1.2 การค้นหาช่องโหว่เครื่องแม่ข่าย (Server) 45

8.1.3 การค้นหา Password โดยใช้ google 46

8.2 การค้นหารายชื่อบุคคล.....46

8.2.1 การค้นหาชื่อบุคคล สามารถทำได้ โดยค้นหาจาก 46

8.2.2 การค้นหาที่อยู่ประกอบด้วย.....46

8.3 การค้นหาประวัติข้อมูล 47

บทที่ 9 ชนิดของเครือข่ายสังคมออนไลน์ 48

9.1 ประวัติความเป็นมา.....49

9.2 โครงสร้างของเครือข่ายสังคมออนไลน์.....50

9.3 ปัญหาของเครือข่ายสังคมออนไลน์.....50

9.4 ชนิดของเครือข่ายสังคมออนไลน์ 50

9.5 สถิติของเครือข่ายสังคมออนไลน์.....51

บทที่ 10 การรักษาความลับและความมั่นคงจากเครือข่ายสังคมออนไลน์ 53

10.1 ประวัติความเป็นมาของ Twitter และ Facebook 54

10.2 การตั้งค่าความเป็นส่วนตัว Twitter 55

10.3 การตั้งค่าความเป็นส่วนตัว Facebook 57

บทที่ 11 การเรียนรู้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 61

11.1 ความเป็นมาของการพัฒนากฎหมายเทคโนโลยีสารสนเทศ และการสื่อสารในประเทศไทย 62

11.2 คำจำกัดความ ตามมาตราในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 65

11.3 ความเข้าใจเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ (Log) หลักเกณฑ์ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวกับกฎหมาย 69

บทที่ 12 จริยธรรมและคุณธรรมการใช้คอมพิวเตอร์และอินเทอร์เน็ต 73

12.1 คุณธรรม-จริยธรรมในการใช้คอมพิวเตอร์ 74

12.2 จรรยาบรรณการใช้เครือข่ายสังคมออนไลน์ 77

12.3 บัญญัติ 10 ประการ 77

บทนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศและการสื่อสารได้พัฒนาไปอย่างรวดเร็วกลายมาเป็นส่วนหนึ่งในชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ แต่เนื่องจากขณะนี้ภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการสื่อสาร โดยผ่านระบบเครือข่ายอินเทอร์เน็ต เช่นการให้ข้อมูลข่าวสารที่บิดเบือนรวมไปถึงข้อมูลที่มีลักษณะการหมิ่นสถาบันเบื้องสูง ถือเป็นเรื่องสำคัญที่ผู้ใช้งานและสังคมออนไลน์จำเป็นต้องช่วยกันสอดส่องดูแลจากสิ่งไม่พึงประสงค์ ด้วยเหตุนี้การสร้างเครือข่ายอาสาสมัครออนไลน์จึงมีความจำเป็นโดยเริ่มจากการปลูกฝังจิตสำนึกในการร่วมมือกันส่งเสริม ปกป้องให้สังคมไทยเกิดความตระหนักในการรับรู้และใช้งานข้อมูลข่าวสารบนโลกออนไลน์อย่างเหมาะสมและสร้างสรรค์

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในฐานะหน่วยงานหลักที่ต้องดำเนินการให้สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะได้ดำเนินการจัดเพิ่มจำนวนบุคลากร เพื่อช่วยตรวจสอบความปลอดภัยบนเครือข่ายอินเทอร์เน็ต รวมทั้งได้มีการติดตั้งอุปกรณ์รักษาความปลอดภัยทางด้านเทคนิคที่มีประสิทธิภาพอย่างดีแล้วก็ตาม แต่ภัยหรืออาชญากรรมออนไลน์ยังเกิดขึ้นตลอดเวลา เนื่องจากสังคมไทยยังขาดความรู้ ความตระหนักในการป้องกันตนเองจากภัยบนเครือข่ายอินเทอร์เน็ต และเป็นเหตุผลที่ภาครัฐมีนโยบายที่จะช่วยสร้างสังคมให้มีความเข้มแข็ง มีภูมิคุ้มกันภัยอันตรายที่มากับระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพราะผู้ใช้งานระบบถือเป็นจุดอ่อนที่เปราะบางที่สุดของการรักษาความมั่นคงปลอดภัย การให้ความรู้สร้างความเข้าใจเรื่องรูปแบบของภัยคุกคามออนไลน์ เพื่อช่วยกันสอดส่องดูแลสังคมให้ปลอดภัยจากสิ่งไม่พึงประสงค์ รวมทั้งปลูกฝังจิตสำนึกในการต่อต้านเนื้อหาและกิจกรรมที่อันตราย ตลอดจนการยกย่องส่งเสริมวัฒนธรรมออนไลน์ที่ดี จึงเป็นสิ่งที่ควรดำเนินการเพื่อช่วยสร้างภูมิคุ้มกันภัยที่ถาวรยั่งยืนให้กับสังคมไทย

การจัดทำโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต หรือ Cyber Scout นี้ เพื่อให้เป็นแบบอย่างแก่เครือข่ายทางสังคมในการส่งเสริมการใช้งานอินเทอร์เน็ตอย่างเหมาะสม โดยร่วมกันช่วยสอดส่องดูแลภัยอันตรายและเฝ้าระวังข้อมูลข่าวสารที่เป็นภัยต่อสถาบัน รวมถึงความมั่นคงของประเทศ ตลอดจนเพื่อให้เกิดช่องทางสำหรับติดต่อประสานงานเครือข่ายอาสาสมัครอย่างเป็นระบบ รวมทั้งเป็นเครือข่ายทางสังคมออนไลน์ ในภาคประชาชนที่จะเป็นพลังหนุนสำคัญในการสร้างสรรค์สังคมในอนาคต ทั้งนี้ สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ มีความยินดีที่จะเข้ามาช่วยในการจัดทำโครงการสร้างลูกเสือบนเครือข่ายอินเทอร์เน็ต หรือ Cyber Scout เพื่อให้บรรลุตามเป้าหมายที่สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้วางไว้

บทที่ 1

วัตถุประสงค์และบทบาทหน้าที่ของแกนนำลูกเสือไซเบอร์

ขอบเขต

ในบทนี้กล่าวถึงบทบาทหน้าที่ของแกนนำลูกเสือไซเบอร์เพื่อที่จะได้นำความรู้และความสามารถที่ได้อบรมในหลักสูตรสามารถนำความรู้และความสามารถนั้นถ่ายทอดให้กับกลุ่มอาสาสมัครได้อย่างถูกต้อง

จุดประสงค์

เพื่อสร้างความตะหนักในการใช้ข้อมูลสารสนเทศให้เกิดความมั่นคงปลอดภัย ซึ่งเป็นแนวร่วมที่สร้างความมั่นคง สามัคคีกับจิตสำนึกที่ดีต่อสถาบันหลักของชาติ รวมทั้งเป็นการถ่ายทอดองค์ความรู้ที่ได้สร้างความเข้มแข็งให้กับชุมชนและสังคมเพื่ออนาคตอย่างยั่งยืน

เนื้อหาในบทนี้

1. ความหมายของลูกเสือ
2. ความหมายของระบบสารสนเทศ
3. ความหมายของลูกเสือไซเบอร์
4. บทบาทและหน้าที่ของลูกเสือไซเบอร์

1. วัตถุประสงค์และบทบาทหน้าที่ของลูกเสือไซเบอร์

1. 1 ความหมายของลูกเสือ

ลูกเสือ คือ เยาวชนชายและหญิงอายุระหว่าง 8 - 25 ปี ที่รับการฝึกอบรมตามหลักสูตรวิชาลูกเสือ โดยยึดมั่นในหลักการ (Principle) วิธีการ (Method) และวัตถุประสงค์ (Purpose) ของการลูกเสือ (Scouting) อย่างเคร่งครัดตามพระราชบัญญัติลูกเสือ (ฉบับที่ 3) พ.ศ. 2528 และข้อบังคับคณะลูกเสือแห่งชาติ ว่าด้วยการปกครองหลักสูตรและวิชาพิเศษลูกเสือ พ.ศ. 2509 ได้กำหนดประเภท เหล่าลูกเสือ 4 ประเภท คือ สำรอง สามัญ สามัญรุ่นใหญ่ วิสามัญ และอาจจัดให้มีลูกเสือเหล่าสมุทร และลูกเสือเหล่าอากาศได้ สำหรับลูกเสือที่เป็นหญิง อาจใช้ชื่อเรียกว่า เนตรนารี หรือชื่ออื่นซึ่งได้รับความเห็นชอบจากคณะกรรมการบริหารลูกเสือแห่งชาติให้หมายถึง ลูกเสือที่เป็นหญิงด้วย

1.2 ความหมายของระบบสารสนเทศ

ระบบสารสนเทศ (Information System) หมายถึง ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ ส่วนไซเบอร์ คือ โลกของสารสนเทศที่ไร้ขอบเขต คำว่าโลกไซเบอร์ หรือ "ไซเบอร์เวิลด์" ถูกนำเสนอครั้งแรกในหนังสือเรื่อง "ไซเบอร์เวิลด์" โดยศาสตราจารย์ โทชิยาสึ ลอเรนส์ คูนิอิ โดยให้โลกไซเบอร์สามารถถูกสร้างขึ้นโดยเจตนา หรือเกิดขึ้นเองก็ได้ และโลกของสารสนเทศเหล่านี้สามารถเป็นได้ทั้งแบบเสมือน โลกจริง หรือโลกที่ผสมกันระหว่างความจริงและสารสนเทศเสมือน โดยโลกไซเบอร์ยังสร้างและประยุกต์ใช้กับ ธุรกรรมอิเล็กทรอนิกส์ การพาณิชย์อิเล็กทรอนิกส์ การเรียนรู้อิเล็กทรอนิกส์ และวัฒนธรรมประเพณีหรือสังคมเผ่าพันธ์ทางอิเล็กทรอนิกส์ ผ่านเครือข่ายอินเทอร์เน็ต

1.3 ความหมายของลูกเสือไซเบอร์

ลูกเสือไซเบอร์ คือ เหล่าลูกเสือหรือผู้บำเพ็ญตนเพื่องานสาธารณะ โดยปฏิบัติหน้าที่ในการดูแล และเฝ้าระวังภัยคุกคามผ่านเครือข่ายอินเทอร์เน็ตหรือโลกไซเบอร์ เพื่อมิให้เกิดการกระทำที่ละเมิด และความเสียหายแก่บุคคลอื่น โดยอยู่ภายใต้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

1.4 บทบาทหน้าที่ของลูกเสือไซเบอร์

เมื่อทราบความหมายและนิยามลูกเสือไซเบอร์ และสิ่งที่ควรทำความเข้าใจคือบทบาทหน้าทีของลูกเสือไซเบอร์นั้นควรประกอบไปด้วยหน้าที่ดังต่อไปนี้

- สร้างความตระหนักในการใช้ข้อมูลสารสนเทศให้เกิดความมั่นคงปลอดภัย
- แนวร่วมสร้างความมั่นคง สามัคคี และจิตสำนึกที่ดีต่อสถาบันหลักของชาติ ได้แก่ ชาติ ศาสนา พระมหากษัตริย์
- สามารถถ่ายทอดองค์ความรู้ที่ได้ สร้างความเข้มแข็งให้กับชุมชน และสังคม เพื่ออนาคตอย่างยั่งยืน

สามารถใช้ข้อมูลอินเทอร์เน็ตในทางที่เหมาะสม มีจริยธรรม คุณธรรม ศีลธรรมอันดี ในการใช้ข้อมูลให้เกิดประโยชน์ต่อสังคมและประเทศชาติได้

บทที่ 2

สถิติภัยคุกคามจากการใช้งานอินเทอร์เน็ต

ขอบเขต

ในบทนี้กล่าวถึงสถิติภัยคุกคามทางเครือข่ายอินเทอร์เน็ตเพื่อที่จะทำให้ได้รับรู้และเกิดความตระหนักถึงทิศทางภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ตได้

วัตถุประสงค์

เพื่อเป็นการสร้างความตระหนักถึงภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต โดยการนำข้อมูลเชิงสถิติที่เกิดขึ้นจริงในโลกปัจจุบันมาเรียนรู้ถึงแนวโน้มภัยคุกคามที่เกิดขึ้นจากการใช้ข้อมูลสารสนเทศจากสถิติ ดังต่อไปนี้

- อธิบายสถิติการใช้งานอินเทอร์เน็ตทั่วโลก
- อธิบายสถิติการใช้งานอินเทอร์เน็ตในประเทศไทย
- อธิบายสถิติการใช้งานเครือข่ายสังคมออนไลน์
- อธิบายสถิติภัยคุกคามและการโจมตีทางอินเทอร์เน็ต
- อธิบายวิวัฒนาการลักษณะการโจมตีคอมพิวเตอร์และอินเทอร์เน็ต

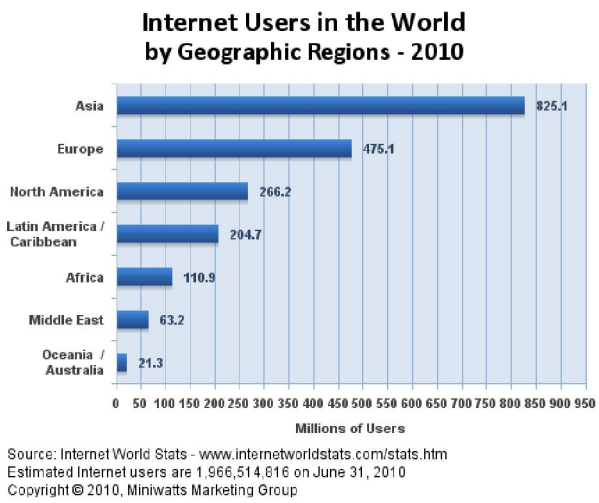
เนื้อหา

1. สถิติการใช้งานอินเทอร์เน็ตทั่วโลก
2. สถิติการใช้งานอินเทอร์เน็ตในประเทศไทย
3. สถิติการใช้งานเครือข่ายสังคมออนไลน์และการโจมตีทางอินเทอร์เน็ต
4. วิวัฒนาการลักษณะการโจมตีคอมพิวเตอร์และอินเทอร์เน็ต

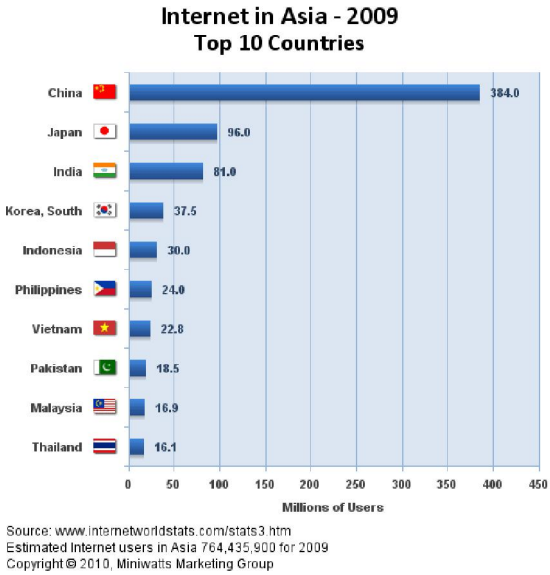
2. สถิติภัยคุกคามจากการใช้งานอินเทอร์เน็ต

2.1 สถิติการใช้งานอินเทอร์เน็ตทั่วโลก

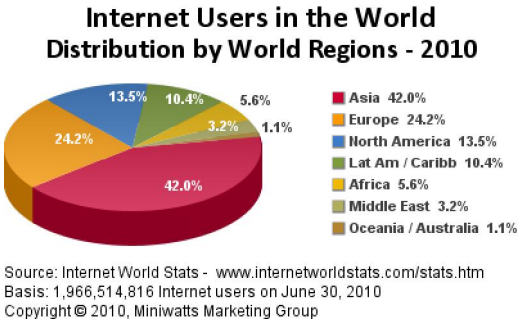
สถิติการใช้งานอินเทอร์เน็ตทั่วโลกเมื่อ มิถุนายน 2553 มีการใช้งานทั่วโลกถึง 1,967 ล้านคน โดยเอเชียมาเป็นอันดับหนึ่งด้วยจำนวน 825 ล้านคน ภาพรวมผู้ใช้งานอินเทอร์เน็ตจะเห็นได้ว่าในภูมิภาคเอเชีย มีการใช้งานอินเทอร์เน็ตสูงที่สุดถึง 42% หรือเกือบครึ่งของผู้ใช้งานอินเทอร์เน็ตทั่วโลก ข้อมูลปี ค.ศ. 2009 เอเชียมีผู้ใช้ 764,435,900 คน ประเทศไทยอยู่อันดับที่ 10 ของเอเชีย ที่มีผู้ใช้งานอินเทอร์เน็ตมากที่สุด คิดเป็นจำนวนผู้ใช้งานอินเทอร์เน็ต 16.1 ล้านคน



ภาพที่ 2.1 สถิติการใช้งานอินเทอร์เน็ตสำรวจเมื่อเดือนมิถุนายน 2553



ภาพที่ 2.2 สถิติจัดอันดับประเทศในเอเชียเป็นเปอร์เซ็นต์



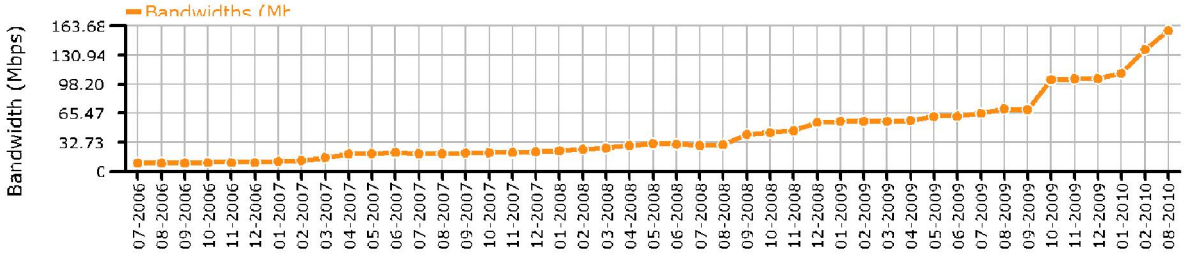
ภาพที่ 2.3 การใช้งานอินเทอร์เน็ตเมื่อเทียบเป็นเปอร์เซ็นต์ทั่วโลก

2.2 สถิติการใช้งานอินเทอร์เน็ตในประเทศไทย

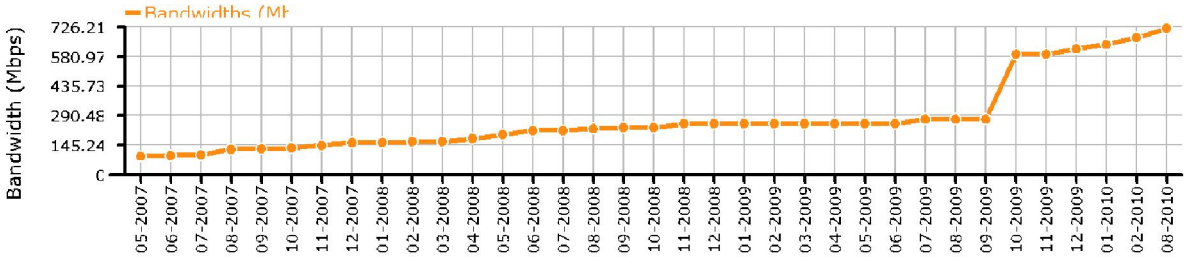
ปริมาณการใช้ข้อมูลอินเทอร์เน็ตแบนด์วิธปี 2010

1. แบนด์วิธภายในประเทศ (Domestic Bandwidth) เรียกว่า National Internet Exchage:NIX คือ ผลรวมของแบนด์วิธทั้งหมดของผู้ให้บริการอินเทอร์เน็ตที่เชื่อมต่อแลกเปลี่ยนข้อมูลที่เกตเวย์ภายในประเทศ

2. แบนด์วิธไปต่างประเทศ (International Bandwidth) เรียกว่า International Internet Gateway:IIG คือ ผลรวมของแบนด์วิธของผู้ให้บริการอินเทอร์เน็ตทั้งหมดที่เชื่อมต่อแลกเปลี่ยนข้อมูลที่ เกตเวย์ไปต่างประเทศ และจากผู้ให้บริการอินเทอร์เน็ตที่เชื่อมต่อไปต่างประเทศโดยตรง



IIG



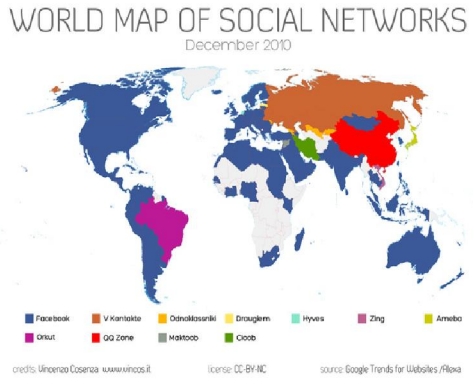
NIX

ภาพที่ 2.4 ภาพแสดงจำนวน Bandwidth ของประเทศไทย โดยแบ่งตามเส้นทางภายใน และภายนอกประเทศ พฤติกรรมการใช้งาน คนไทยส่วนใหญ่ใช้งานช่วงเวลาบ่ายสอง และใช้งานน้อยสุดช่วงเวลาตีห้า ตามลำดับ

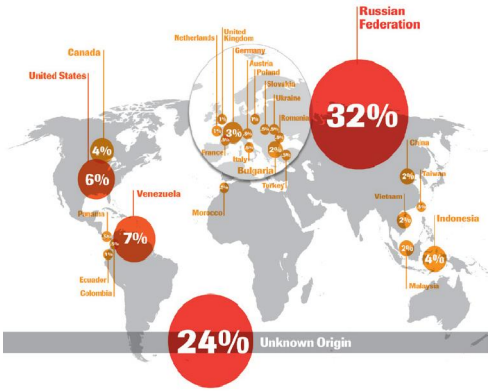
อ้างอิงข้อมูลจาก งานวิจัยข้อมูลอินเทอร์เน็ต : Internet Information Research (IIR)
หน่วยปฏิบัติการวิจัยเทคโนโลยีเครือข่าย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ

2.3 สถิติภาพรวมการใช้เครือข่ายสังคมออนไลน์และการโจมตีทางอินเทอร์เน็ต

สถิติภัยคุกคามทางอินเทอร์เน็ต พบว่าจำนวนถึง 32% มาจากประเทศรัสเซีย และอีก 24% ไม่สามารถระบุประเทศได้ การโจมตีที่ไม่สามารถแยกแยะได้ว่ามาจากประเทศไหน นั้นอาจเกิดจากการปลอมแปลงค่า IP Address หรือเรียกว่าการ spoof IP เกิดขึ้นจนไม่สามารถบ่งบอกได้ว่ามาจากประเทศหรือทวีปใดในโลกนี้ได้



ภาพที่ 2.5 สถิติการใช้เครือข่ายสังคมออนไลน์



ภาพที่ 2.6 อัตราการโจมตีทางอินเทอร์เน็ตแบ่งตามประเทศ

2.4 วิวัฒนาการลักษณะการโจมตีทางคอมพิวเตอร์และอินเทอร์เน็ต

จาก ปี ค.ศ. 1980 จนถึง ค.ศ. 2010

30 ปีก่อนลักษณะการโจมตีทางคอมพิวเตอร์เป็นการเข้าถึงข้อมูลทางกายภาพเสียส่วนใหญ่

20 ปีผ่านมา เริ่มมีการโจมตีผ่านระบบเครือข่ายคอมพิวเตอร์ (Network)

10 ปีผ่านมา เริ่มมีการโจมตีผ่านระบบ Application จากการติดต่อสื่อสาร เช่น E-mail , Chat และเครือข่ายไร้สาย (Wireless)

ในปัจจุบัน เป็นการโจมตีแบบผสมผสาน โดยอาศัยสังคมออนไลน์ และผ่านการติดต่อสื่อสารเพื่อเข้าถึงผู้ใช้งานมากขึ้นผ่านอุปกรณ์มือถือหรือสมาร์ทโฟน (smart phone)

บทที่ 3
ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต

ขอบเขต

ในบทนี้กล่าวถึงชนิดภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ตในยุคปัจจุบัน ความเข้าใจชนิดของภัยคุกคามในแต่ละชนิด และทราบถึงศัพท์ทางเทคนิคที่ใช้กันอย่างถูกต้อง

วัตถุประสงค์

1. อธิบายความหมายของชนิดภัยคุกคามทางอินเทอร์เน็ต
2. ผู้เรียนต้องสร้างความเข้าใจประเภทภัยคุกคามมัลแวร์ (Malware)
3. ผู้เรียนต้องสร้างความเข้าใจชนิดการโจมตีแบบ DDoS/DoS
4. ผู้เรียนต้องสร้างความเข้าใจชนิดการโจมตีจาก Botnet
5. ผู้เรียนต้องสร้างความเข้าใจชนิดการโจมตีจากข้อมูลขยะ (Spam)
6. ผู้เรียนต้องสร้างความเข้าใจการหลอกลวงข้อมูล (Phishing)
7. ผู้เรียนต้องสร้างความเข้าใจการดักข้อมูล (Sniffer)

เนื้อหา

1. ชนิดภัยคุกคามและความหมายของมัลแวร์ (Malware)
2. ชนิดการโจมตีแบบ DDoS/DoS
3. ชนิดการโจมตีจาก Botnet
4. ชนิดการโจมตีจากข้อมูลขยะ (Spam)
5. การหลอกลวงข้อมูล (Phishing)
6. การดักข้อมูล (Sniffer)
7. วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต

3. ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต

ชนิดของภัยคุกคามที่เกิดขึ้นบนอินเทอร์เน็ต เพื่อเรียนรู้ชนิดและประเภทของภัยคุกคามที่เกิดขึ้นจากการใช้ข้อมูลสารสนเทศ เข้าใจถึงคำศัพท์และรูปแบบของการโจมตีในแต่ละชนิดที่เกิดขึ้นจริงในปัจจุบัน

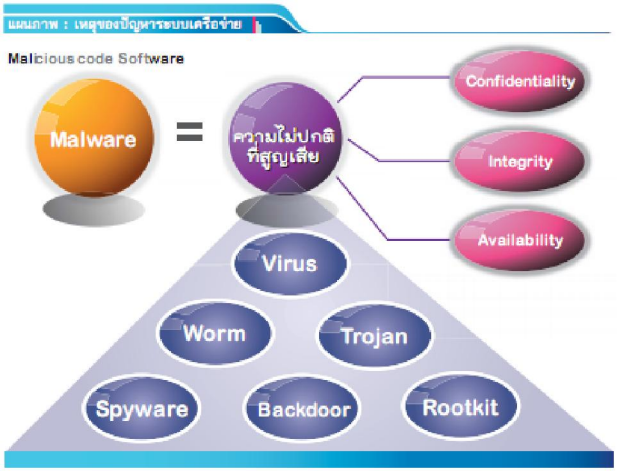
เมื่อพูดถึงภัยในโลกอินเทอร์เน็ต ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ชื่อที่หลายคนนึกถึงเป็นอันดับต้นๆ คือ “ไวรัสคอมพิวเตอร์” ซึ่งเข้ามามีบทบาทตั้งแต่ยุคแรกเริ่มของคอมพิวเตอร์ จนถึงปัจจุบัน เป็นที่คุ้นเคยของคนทุกเพศทุกวัย ไม่ว่าจะเป็นผู้ที่เชี่ยวชาญ หรือเป็นแค่มือใหม่ ก็อาจจะได้รับภัยจากไวรัสหลากสายพันธุ์ไปบ้าง ไม่มากก็น้อย

ไวรัสคอมพิวเตอร์เป็นเพียงเสี้ยวหนึ่งของภัยคุกคามทางคอมพิวเตอร์ จัดอยู่ในกลุ่ม มัลแวร์ (Malware หรือ Malicious Code Software) ซึ่งแตกออกไปได้อีกหลากหลายรูปแบบ โดยรายละเอียดของภัยคุกคามต่าง ๆ ที่เกิดขึ้นมีดังนี้

3.1 มัลแวร์ (Malware)

คือ ความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality), I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด จนเกิดเป็นไวรัส เวิร์ม โทรจัน สปายแวร์ Backdoor และ Rootkit ดังภาพ ที่ 3-1

- การสูญเสีย C (Confidentiality) คือ สูญเสียความลับทางข้อมูล
- การสูญเสีย I (Integrity) คือ สูญเสียความไม่เปลี่ยนแปลงของข้อมูล นั่นคือ ข้อมูลถูกเปลี่ยนแปลงแก้ไข โดยเฉพาะส่วนสำคัญที่เกี่ยวโยงกับระบบภายในระบบปฏิบัติการ
- การสูญเสีย A (Availability) คือ สูญเสียเสถียรภาพของระบบปฏิบัติการ



ภาพที่ 3.1 เหตุของปัญหาระบบเครือข่าย

มัลแวร์แบ่งออกได้เป็นหลายประเภท แต่ละชนิดล้วนก่อให้เกิดอันตรายต่อข้อมูล คอมพิวเตอร์และเครือข่าย บ่อยครั้งที่ส่วนใหญ่นำคำเหล่านี้มาใช้แทนกันโดยไม่ทราบความแตกต่างที่แท้จริง จึงขออธิบายรายละเอียดพอสังเขป ดังนี้

3.1.1 ไวรัสคอมพิวเตอร์ (Computer Virus)

คือ รหัสหรือโปรแกรมที่สามารถทำสำเนาตัวเองและแพร่กระจายสู่เครื่องอื่นได้ โดยเจ้าของเครื่องนั้นๆ ไม่รู้ตัว (หากไม่ติดตั้งโปรแกรมป้องกันไวรัส หรือโปรแกรมดังกล่าวไม่รู้จักไวรัสชนิดนั้นๆ) ถือเป็นสิ่งไม่พึงประสงค์ซึ่งฝังตัวเองในโปรแกรมหรือไฟล์ แล้วแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ผ่านสื่อรูปแบบต่างๆ เช่น CD, DVD, Multimedia

Card, USB Drive หรือผ่านทางเครือข่าย เช่น อินเทอร์เน็ต ระบบ LAN หรืออีเมล์ เป็นต้น ซึ่งไวรัสส่วนใหญ่มักฝังอยู่ในโปรแกรมชนิด execute (.exe) ซึ่งหมายถึงไวรัสอาจอาศัยอยู่ในเครื่องคอมพิวเตอร์ แต่ไม่แสดงความผิดปกติให้พบ หากผู้ใช้ไม่เรียกใช้โปรแกรมดังกล่าว สิ่งสำคัญคือไวรัสไม่อาจแพร่กระจายได้หากขาดคนกระทำ เช่น แบ่งปันไฟล์ที่ติดไวรัส หรือส่งอีเมล์โดยแนบไฟล์ที่ติดไวรัส เป็นต้น ซึ่งไวรัสคอมพิวเตอร์เหมือนกับไวรัสในมนุษย์ที่มีความรุนแรงหลายระดับ ตั้งแต่สร้างความรำคาญให้ผู้ใช้งาน จนถึงขั้นทำลายฮาร์ดแวร์ ซอฟต์แวร์ หรือไฟล์ข้อมูลทำให้ผู้ใช้งานหรือเป็นเจ้าของคอมพิวเตอร์จำเป็นต้องเรียกหาโปรแกรมป้องกันไวรัสมาติดตั้งจนกลายเป็นโปรแกรมสำคัญสำหรับคอมพิวเตอร์ทุกเครื่อง

3.1.2 หนอนคอมพิวเตอร์ (Computer Worm)

คือ เรียกสั้นๆ ว่า เวิร์ม เป็นหน่วยย่อยลงมาจากไวรัส ซึ่งสามารถทำสำเนาตัวเองและแพร่กระจายผ่านเครือข่ายหรืออินเทอร์เน็ต สู่คอมพิวเตอร์หรือเครือข่ายอื่นได้ เวิร์มต่างจากไวรัสตรงที่ไม่ต้องอาศัยผู้ใช้งาน แต่จะอาศัยไฟล์หรือคุณสมบัติในการส่งต่อข้อมูลในคอมพิวเตอร์ เพื่อกระจายตัวเอง โดยสแกนเครือข่ายเพื่อหาระบบที่มีช่องโหว่ โจมตีช่องโหว่และบุกรุกเข้าระบบเหล่านั้นโดยอัตโนมัติ เวิร์มบางชนิดสามารถติดตั้ง Backdoor ที่เครื่องติดเวิร์ม และสร้างสำเนาตัวเองได้ โดยผู้สร้างเวิร์มชนิดนั้น ซึ่งสามารถสั่งการได้จากระยะไกล ที่เรียกว่า Botnet โดยอาจมีเป้าหมายเพื่อโจมตีสร้างความเสียหายให้กับคอมพิวเตอร์และเครือข่าย หรือเพียงแค่ต้องการโฆษณาสินค้าหรือบริการก็ได้ ซึ่งรายละเอียดจะได้กล่าวถึงต่อไป แม้เวิร์มจะเป็นหน่วยย่อยของไวรัส แต่ก็มีความรุนแรงเหนือกว่าไวรัสมาก สิ่งที่อันตรายอย่างยิ่งของเวิร์มคือ มันสามารถจำลองตัวเองในคอมพิวเตอร์เครื่องหนึ่ง แล้วแพร่กระจายสำเนาของตัวเองออกไปได้จำนวนมาก ตัวอย่างเช่น สามารถดักจับ username และ password และใช้ข้อมูลนี้เพื่อบุกรุกบัญชีผู้ใช้นั้น ทำสำเนาตัวเองแล้วส่งต่อไปยังทุกรายชื่อที่มีอยู่ในลิสต์อีเมล์ จากนั้นทำสำเนาต่ออีก แล้วส่งไปยังบัญชีรายชื่อของผู้รับอีเมล์นั้นทุกคน ท้ายที่สุดส่งผลให้การรับส่งข้อมูลผ่านเครือข่าย (Network Bandwidth) ทำได้ช้าลง เป็นเหตุให้ Web Server, Network Server และเครื่องคอมพิวเตอร์หยุดทำงาน

3.1.3 ม้าโทรจัน (Trojan Horse)

คือ โปรแกรมชนิดหนึ่งที่ดูเหมือนมีประโยชน์ แต่แท้ที่จริงก่อให้เกิดความเสียหายเมื่อรันโปรแกรม หรือติดตั้งลงบนคอมพิวเตอร์ ผู้ที่ได้รับไฟล์โทรจันมักถูกหลอกให้เปิดไฟล์ดังกล่าว โดยหลงคิดว่าเป็นซอฟต์แวร์ถูกกฎหมาย หรือไฟล์จากแหล่งที่ถูกต้องตามกฎหมาย เมื่อไฟล์ถูกเปิดอาจเกิดผลลัพธ์หลากหลายรูปแบบ ตั้งแต่สร้างความรำคาญ เช่น เปลี่ยนหน้า Desktop หรือสร้างไอคอนที่ไม่จำเป็นบนหน้า Desktop จนถึงขั้นสร้างความเสียหายรุนแรง ด้วยการลบไฟล์และทำลายข้อมูลในคอมพิวเตอร์ โทรจันบางชนิดอาจฝัง Backdoor ไว้ในเครื่องคอมพิวเตอร์ เป็นเหตุให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องคอมพิวเตอร์นั้น ล้วงข้อมูลส่วนตัว และข้อมูลที่เป็นความลับ สร้างความเสียหายได้ สิ่งหนึ่งที่โทรจันแตกต่างจากไวรัสและเวิร์มคือ โทรจันไม่สามารถสร้างสำเนาโดยแพร่กระจายสู่ไฟล์อื่น และไม่สามารถจำลองตัวเองได้.

3.1.4 Backdoor

แปลเป็นไทยก็คือ “ประตูหลัง” ที่เปิดทิ้งไว้ให้บุคคลอื่นเดินเข้านอกออกในบ้านได้โดยง่าย Backdoor ในมุมมองด้านความปลอดภัยสารสนเทศ ก็คือช่องทางลัดที่เกิดจากช่องโหว่ของระบบ ทำให้ผู้ไม่มีสิทธิเข้าถึงระบบหรือเครื่องคอมพิวเตอร์สามารถเข้าถึงระบบเพื่อใช้ทรัพยากรในเครื่องนั้นเพื่อกระทำการใดๆ ได้ โดยทั่วไป Backdoor อาจเกิดจากความตั้งใจของผู้ดูแลระบบ เพื่อสร้างช่องทางลัดเข้าสู่ระบบเองก็ได้ แต่เมื่อไปผสมผสานกับภัยคุกคามอื่น เช่น โทรจัน ทำให้ระบบเกิดช่องโหว่ที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงเพื่อสร้างความเสียหายได้

3.1.5 สปายแวร์ (Spyware)

คือ มัลแวร์ชนิดหนึ่งที่ติดตั้งบนเครื่องคอมพิวเตอร์แล้วทำให้ล่วงรู้ข้อมูลของผู้ใช้งานได้โดยเจ้าของเครื่องไม่รู้ตัว สามารถเฝ้าดูการใช้งานและรวบรวมข้อมูลส่วนตัวของผู้ใช้ได้ เช่น นิสัยการท่องเน็ต และเว็บไซต์ที่เข้าชม ทั้งยังสามารถเปลี่ยนค่าที่ตั้งไว้ของคอมพิวเตอร์ ส่งผลให้ความเร็วในการเชื่อมต่ออินเทอร์เน็ตช้าลง หรือหน้าโฮมเพจเปลี่ยนแปลง เป็นต้น สปายแวร์ที่มีชื่อคุ้นเคยกันดีคือโปรแกรม Keylogger ซึ่งตกเป็นข่าวหน้าหนึ่งของหนังสือพิมพ์ เมื่อผู้ใช้ดาวน์โหลดไฟล์จากอินเทอร์เน็ตที่แฝงโปรแกรม Keylogger ทำให้โปรแกรมเข้ามาฝังตัวในคอมพิวเตอร์ส่วนตัว เมื่อผู้ใช้ได้ใช้เครื่องคอมพิวเตอร์เพื่อทำธุรกรรมการเงินในเว็บ E-Banking ข้อมูล username และ password ของบัญชีผู้ใช้จึงถูกส่งตรงถึงมิจฉาชีพ ซึ่งสวมรอยเป็นเจ้าของบัญชี ลักลอบโอนเงินออกมาโดยเจ้าของตัวจริงไม่รู้ตัว เป็นต้น สิ่งที่น่าสนใจสำหรับข่าวอาชญากรรมชิ้นนี้ก็คือผู้ต้องหาเป็นเพียงผู้เล่นเกมธรรมดามิใช่ผู้เชี่ยวชาญทางคอมพิวเตอร์ และให้การรับสารภาพว่าไปดาวน์โหลดโปรแกรม Keylogger นี้จากอินเทอร์เน็ต แล้วลองใช้งานจริง นั่นหมายความว่าการจะหามัลแวร์เพื่อไปโจมตีผู้อื่น หรือหาผลประโยชน์ใส่ตัว ไม่ใช่เรื่องยาก และภัยคุกคามอยู่ใกล้ตัวเราเพียงแค่การสัมผัสคีย์บอร์ดเท่านั้น

3.2 การโจมตีแบบ DoS/DDoS

คือ การพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ด้วยเทคโนโลยีที่ก้าวล้ำในปัจจุบันซึ่งมีภัยคุกคามมากมาย และแพร่กระจายอย่างรวดเร็ว ทำให้ปัจจุบันการโจมตีส่วนใหญ่ในโลกออนไลน์ มักเป็นการโจมตีแบบ DDoS

3.3 BOTNET หรือ “Robot network”

คือ เครือข่ายหุ่นรบที่ถือเป็นสะพานเชื่อมภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการตัวนำทางเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เองโดยลำพัง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น ซึ่งแสดงภัยคุกคามดังกล่าวมี “คน” ซักใยอยู่เบื้องหลัง เมื่อเครื่องของผู้รู้เท่าไม่ถึงการณ์ ติดมัลแวร์ จะกลายสภาพเป็นผู้แพร่กระจาย Botnet ซึ่งอาจบัญชาการจากระยะไกลโดยผู้ควบคุม เช่น แฮกเกอร์ หรือกระทำการอิสระโดยอัตโนมัติตามที่ตั้งโปรแกรมไว้ แหล่งควบคุม Botnet ส่วนใหญ่อยู่ใน IRC (Internet Relay Chat) ห้องสนทนายุคแรกเริ่ม ด้วยเหตุผลหลัก 2 ประการ คือ

1) Protocol ในการติดต่อ IRC เป็นแบบ UDP ซึ่งมีความเร็ว และ ไม่ต้องการความถูกต้องในการสื่อสารมากนัก ทำให้เครื่องที่ติด Botnet แทบไม่รู้ตัวว่าได้เชื่อมต่อ Server IRC ที่อยู่ห่างไกลออกไป

2) IRC เป็นแหล่งที่แฮกเกอร์ส่วนใหญ่ในอดีตใช้แลกเปลี่ยนเทคนิค รวมทั้งเรื่องราวต่างๆ เป็นแหล่งที่ยากต่อการควบคุมและค้นหาตัวตนที่แท้จริง

Botnet จะอาศัยเครื่องคอมพิวเตอร์ที่อ่อนแอ มีช่องโหว่ไม่มีการป้องกัน ดังนั้นหากเครื่องไม่ได้รับการเอาใจใส่ในการป้องกันจากเจ้าของ วันหนึ่งคอมพิวเตอร์ก็อาจติด Botnet ได้โดยเจ้าของเครื่องไม่รู้ตัว วิธีป้องกัน Botnet ที่ดีที่สุดจึงเป็นการป้องกันเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบอยู่ให้ดีที่สุด ด้วย 10 วิธีง่ายๆ ที่จะได้กล่าวถึงต่อไปในบทที่ 4

3.4 ข้อมูลขยะ (Spam)

คือ ภัยคุกคามกันส่วนใหญ่เกิดจากอีเมล์หรือเรียกว่า อีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล์ เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

หลายคนอาจสงสัยว่า spammer รู้อีเมล์แอดเดรสได้อย่างไร คำตอบคือ ได้จากเว็บไซต์ ห้องสนทนา ลิสต์รายชื่อลูกค้า รวมทั้งจากไวรัสชนิดต่างๆ ที่เป็นแหล่งรวบรวมอีเมล์แอดเดรสชั้นดี และ ส่งถูกขายต่อกันเป็นทอดๆ

วิธีป้องกันเบื้องต้นไม่ให้อีเมล์ของคุณที่เผยแพร่อยู่ในที่สาธารณะ เช่น เว็บไซต์องค์กร หรือกระดานสนทนาออนไลน์ ถูก Botnet ค้นเหาเจอ แล้วกระจายแอดเดรสของคุณเข้าไปในลิสต์ส่งอีเมล์ของ spammer นั้น ทำได้โดยเปลี่ยนวิธีการสะกด โดยเปลี่ยนจากเครื่องหมาย “@” เป็นคำว่า “at” แทน

3.5 Phishing

เป็นคำพ้องเสียงกับ “fishing” หรือการตกปลาเพื่อให้เหยื่อมาติดเบ็ด คือ กลลวงชนิดหนึ่งในโลกไซเบอร์ด้วยการส่งข้อความผ่านอีเมล์หรือเมสเซนเจอร์ หลอกให้เหยื่อหลงเชื่อว่าเป็นสถาบันการเงินหรือองค์กรน่าเชื่อถือ เชิญชวนด้วยกลวิธีต่างๆ เช่น คุณได้รับรางวัล แล้วทำลิงค์ล่อให้เหยื่อคลิก เพื่อหวังจะได้ข้อมูลสำคัญ เช่น username / password, เลขที่บัญชีธนาคาร, เลขที่บัตรเครดิต เป็นต้น แต่ลิงค์ดังกล่าว จะนำไปสู่หน้าเว็บเลียนแบบ หากเหยื่อเผลอกรอกข้อมูลส่วนตัวลงไป มิจฉาชีพสามารถนำไปหาประโยชน์ในทางมิชอบได้ หากได้รับอีเมล์ในลักษณะนี้ ไม่ควรคลิกลิงค์ ถ้าได้รับอีเมล์แปลกปลอมที่ไม่น่าไว้ใจ ให้ทำการลบทิ้งทันที

3.6 Sniffing

การดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง บนเครือข่ายในองค์กร (LAN) เป็นวิธีการหนึ่งที่นักโจมตีระบบ นิยมใช้ดักข้อมูลเพื่อแกะรหัสผ่านบนเครือข่ายไร้สาย (Wireless LAN) และ ดักข้อมูล User / Password ของผู้อื่นที่ไม่ได้ผ่านการเข้ารหัส เช่น การดัก User / Password จากเว็บไซต์ (HTTP) หรือ E-mail ที่ขาดการ Login ที่เข้ารหัสผ่าน ซึ่งการดักข้อมูลถือว่าผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในมาตรา 8 โดยพิจารณาถึงเจตนาเป็นหลัก

3.7 วิธีสังเกตภัยคุกคามจากอินเทอร์เน็ต

ส่วนประกอบที่ 1 คือ คน การกระทำของคนที่เกิดขึ้นจากคนเป็นการรับรู้ในสิ่งต่างๆ มีทั้งภายใน และภายนอก ตัวคน

1. ภายในเองก็ประกอบด้วย ตา หู จมูก ลิ้น กาย และใจ หากอธิบายในทางวิทยาศาสตร์ ในร่างกายของคนก็มีการติดต่อสื่อสารภายใน ในระดับเซลล์ ประจุไฟฟ้า อนุภาคที่มีขนาดเล็ก รวมเป็นเนื้อเยื่อ รวมเป็นระบบประสาทที่เชื่อมโยงสื่อสารภายในตัวคน มีการถ่ายทอดข้อมูลจากบรรพบุรุษผ่านระบบดีเอ็นเอ (DNA) ที่เป็นพิมพ์เขียวจากอดีตที่ตกทอดมาถึงเรา แม้กระทั่งสารเคมีต่างๆ ที่อยู่ภายในร่างกายของเราที่ทำงานตลอดเวลาจนกว่าเรา จะหมดลมหายใจ

2. ภายนอก เป็น อารมณ์ ที่ทำได้จาก ตาเห็นรูป , หูได้ยินเสียง , จมูกได้กลิ่น , ลิ้นได้รส , กายได้สัมผัส และใจที่มีความคิดปรุงแต่งตามสภาวะชั่วขณะ ที่เกิดขึ้น ตั้งอยู่ และดับไป ทุกสิ่งทุกอย่างเป็นไปตามกระแสของเหตุปัจจัย หรือในพุทธศาสนาเรียกว่า "ปฏิจจสมุปบาท" ซึ่งทั้งหมดนี้จะทำให้คน คนนั้นทำกิจกรรมและมีพฤติกรรมการแสดงออกที่แตกต่างกันตามช่วงเวลา เกิด อยู่ ตั้งอยู่ และดับไป ไม่คงที่มีการเปลี่ยนแปลงอยู่ตลอด

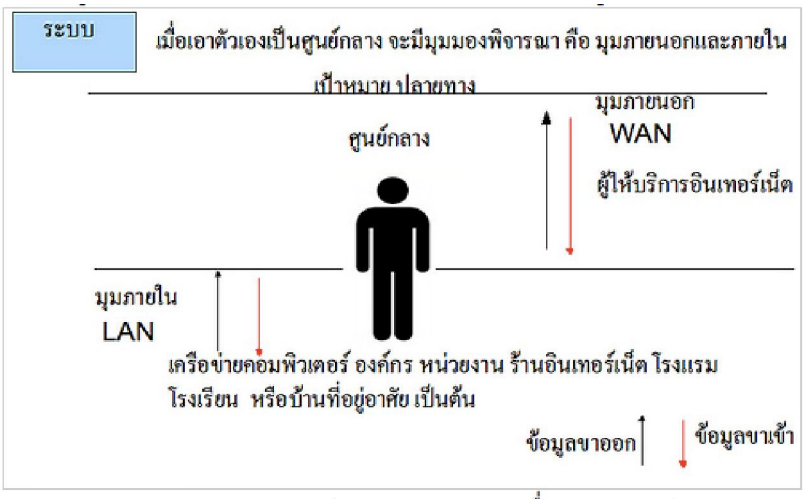
ส่วนประกอบที่ 2 คือ เครื่อง หมายถึงเครื่องมือสื่อสาร ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ มือถือ หรืออื่นๆที่สามารถติดต่อสื่อสารได้ ทั้งฝั่งรับข้อมูล และ ฝั่งส่งข้อมูล ในที่นี้เปรียบเทียบเป็นเหมือนยานพาหนะ เครื่องเป็นพาหนะที่เกิดจากคนเป็นผู้ใช้งาน มุมมองในการพิจารณาก็มีทั้งภายในและภายนอก โดยใช้คนเป็นศูนย์กลางในการพิจารณา

1. ภายใน คือ คนใช้เครื่องโดยตรง
2. ภายนอก คือ ถูกผู้อื่นใช้เครื่อง ทั้งที่เป็นเจตนา และไม่เจตนา บนความรู้เท่าไม่ถึงการณ์

ส่วนประกอบที่ 3 คือ ระบบ หมายถึงโครงข่ายข้อมูล (Network) ที่เป็นช่องทางในการสื่อสาร ไม่ว่าเป็นการสื่อสารผ่านอินเทอร์เน็ต มือถือ หรืออื่นๆ ในที่นี้ขอเปรียบเทียบเป็นเหมือนช่องถนนในการเดินทางของพาหนะ ระบบนั้นก็มีมุมมองในการพิจารณา มีทั้งภายใน และ ภายนอก เช่นกัน โดยใช้คน และ เครื่อง เป็นศูนย์กลางในการพิจารณา โดยใช้คน และเครื่องเป็นศูนย์กลาง

1. ภายใน คือ ช่องทางการติดต่อสื่อสารภายในเครือข่ายองค์กร (LAN Technology)
2. ภายนอก คือ ช่องทางการติดต่อสื่อสารภายนอกเครือข่ายองค์กร (WAN Technology)

โดยทั้งคู่สามารถพิจารณาไปถึงการไหลเวียนของข้อมูลที่เกิดขึ้นจากหลัก OSI 7 layer



รูปที่ 3.2 เปรียบเทียบการรับ-ส่งข้อมูลเมื่อใช้คนเป็นศูนย์กลาง

เมื่อเอาตัวคนเป็นศูนย์กลางหากเราใช้หลักพิจารณาภายในและภายนอก โดยใช้คนเป็นศูนย์กลางในการพิจารณาแล้ว จะเห็นว่าในระดับผู้ให้บริการ (ISP) นั้นจะกลายเป็นมุมภายนอกเสมอ ซึ่งในความเป็นจริงแล้วไม่ใช่ เนื่องจากผู้ให้บริการ (ISP) ก็จะมีระบบภายใน (LAN) เช่นกัน ดังนั้นการพิจารณาในเรื่องนี้นอกจากใช้คนเป็นศูนย์กลางในการพิจารณาแล้วยัง ต้องอาศัยข้อมูลเป็นศูนย์กลางในการพิจารณาด้วย โดยข้อมูลจะแบ่งประเภทดังนี้

การพิจารณาโดยใช้ข้อมูลเป็นศูนย์กลาง ซึ่งในที่นี้จะหมายถึงข้อมูลนั้นเกิดจาก คน และเครื่อง ในประเทศไทย

1. ข้อมูลที่รับและส่งภายในประเทศ จะต้องผ่านช่องทางการติดต่อสื่อสาร ที่ผมเปรียบเทียบได้กับถนน ถนนที่เกิดจากผู้ให้บริการ (ISP) สร้างขนาดถนนที่แตกต่างกัน ขนาดของ Bandwidth ในการรับและส่งข้อมูลซึ่งผู้ให้บริการบางรายอาจเปรียบได้กับถนน 4 แลน บางรายอาจเปรียบได้กับ ถนน 2 เลน เป็นต้น การติดต่อสื่อสารภายในประเทศ ก็เหมือนกับถนนที่เชื่อมกันระหว่างผู้ให้บริการในประเทศ ยกตัวอย่างเช่น เปิดเว็บไซต์ www.mict.go.th ซึ่งตัวเว็บไซต์นั้นตั้งอยู่ภายในประเทศไทย การติดต่อสื่อสารก็จะเกิดเฉพาะภายในประเทศไทย
2. ข้อมูลที่รับส่งภายนอกประเทศ จะต้องผ่านช่องทางการติดต่อสื่อสาร หรือ ถนนที่เกิดจากผู้ให้บริการ (ISP) ที่มีการสร้างขนาดถนนที่แตกต่างกัน เช่นเดียวกันกับการรับส่งข้อมูลภายในประเทศ ที่แตกต่างกันคือข้อมูลฝั่งปลายทางที่ติดต่อไปนั้นอยู่ต่างประเทศ ยกตัวอย่างเช่น เปิดเว็บไซต์ www.blogger.com ซึ่งเมื่อทำการ whois ดูพบว่าตั้งอยู่ต่างประเทศ ที่ไม่ใช่ประเทศไทย การติดต่อสื่อสารก็เริ่มจากเครื่องที่อยู่ที่บ้าน ไปยังผู้ให้บริการที่ให้ บริการอินเทอร์เน็ต ผู้ให้บริการก็เปิดช่องทางต่างประเทศให้ข้อมูลที่เรียกเว็บไซต์ www.blogger.com ไปถึงที่หมายปลายทาง เพียงช่วงพริบตา

ส่วนประกอบที่ 4 คือ ผลลัพธ์ ผลลัพธ์มีทั้งเรื่องปกติ และเรื่องไม่ปกติ ซึ่งสามารถแยกแยะได้ดังนี้

- เรื่องที่ปกติ เกิดจากการใช้งานคอมพิวเตอร์ ในการรับและส่งข้อมูลได้อย่างปกติที่เคยใช้ รับรู้ได้ด้วยตัวเอง
- เรื่องที่ผิดปกติ เกิดจากการใช้งานคอมพิวเตอร์ ในการรับและส่งข้อมูลได้นั้นมีความผิดปกติ เกิดได้ดังนี้
    1. เกิดจากการรั่วไหลของข้อมูลที่เป็นความลับ (C : Confidentiality)
    2. เกิดจากการแสดงข้อมูลที่ไม่ถูกต้องจากความเป็นจริง (I : Integrity)
    3. เกิดจากความไม่คงที่ของข้อมูลทำให้ความเสถียรภาพข้อมูลนั้นสูญเสียไป (A : Availability)

ทั้งหมดนี้ คือการเสียทั้ง C, I และ A หรือการสูญเสียอย่างใดอย่างหนึ่ง ทำให้เกิดความผิดปกติจากการใช้งานคอมพิวเตอร์ และการรับ-ส่งข้อมูลเกิดขึ้น ซึ่งเรียกว่า ความผิดปกติที่เกิดขึ้นจากผลลัพธ์ทางเทคนิคว่า "เหยื่อ" หมายถึงคนและเครื่องมือในการติดต่อสื่อสารนั้น ซึ่งการตกเป็นเหยื่อทางเทคนิคบนความรู้เท่าไม่ถึงการณ์

เหยื่อในทางเทคนิค ได้แก่ การติดมัลแวร์ (Virus/worm, Trojan, Backdoor, rootkit และอื่นๆ), การตกเป็นเครื่องมือให้นักโจมตีระบบใช้ทรัพยากรเครื่องของเราในการส่งข้อมูลขยะ (Spam) หรือการโจมตีระบบให้เกิดความเสียหาย (DDoS/DoS)

ผลลัพธ์ไม่ใช่ทางเทคนิคผลลัพธ์ที่เป็นเรื่องปกติ ก็หมายถึงข้อมูลที่เรารับรู้ที่ได้ปรากฏขึ้นนั้นสามารถยอมรับได้ด้วยกฎหมาย และศีลธรรมบนประเทศที่เราได้ทำการสื่อสารข้อมูลขึ้น เนื่องจากแต่ละประเทศนั้นมีความแตกต่างด้าน กฎหมาย ดังนั้นหากเอาตัวเรา และเครื่องคอมพิวเตอร์ของเราเป็นศูนย์กลางต้องพิจารณาว่าเราใช้เครื่องคอมพิวเตอร์ รับ-ส่งข้อมูลที่ประเทศใด ถ้าเป็นประเทศไทยก็ต้องดูกฎหมายในประเทศไทยเป็นหลัก ส่วนศีลธรรมนั้นมีทั่วไป เป็นเรื่องที่ทั่วโลก มีความเห็นสอดคล้องกัน

เรื่องผิดปกติ ก็หมายถึงข้อมูลที่เรารับรู้ที่ได้ปรากฏขึ้นนั้น เกิดจากความคิดเห็นที่แตกต่างกันในแต่ละบุคคล ซึ่งเรื่องไม่ปกตินั้นควรดูกฎหมายและศีลธรรมของประเทศนั้นๆ ในการพิจารณาต่อไป

จะขอเรียกความผิดปกติที่เกิดจากผลลัพธ์ที่ไม่ใช่เทคนิคนี้ ว่า "เหยื่อ" ความหมายคือ คนและเครื่องมือในการติดต่อสื่อสารนั้นตกเป็นเหยื่อ บนความไม่รู้เท่าทันขยายความได้ว่า เนื่องจากข้อมูลที่เรา เรา ท่าน ท่าน ที่ได้รับข้อมูลมานั้น หากเราไม่มีสติและความรู้เท่าทันภัย เราอาจกลายเป็นเหยื่อโดยที่เราไม่รู้ตัวได้เช่นกัน

เหยื่อที่เกิดขึ้นโดยไม่ใช่ทางเทคนิค ได้แก่ การรับรู้ข้อมูลที่ทำให้เกิดความเข้าใจผิด ซึ่งความเข้าใจผิดอาจจะก่อให้เกิดความเชื่อ การยึดมั่นถือมั่นในสิ่งที่เข้าใจผิดไป และคิดว่าเป็นจริง หรือเรียกว่า สัญญาวิปลาส เห็นกงจักรเป็นดอกบัว เป็นต้น

การแสดงความเป็นห่วงโดยไม่มองให้รอบด้าน ในการสื่อสารสมัยใหม่อาศัยคนเป็นเหยื่อมากขึ้น ขอยกตัวอย่าง เช่น การแสดงความคิดเห็นในเว็บบอร์ด หรือเครือข่ายสังคมออนไลน์ (Social network) พบข้อมูลอันไม่เหมาะสม ตัวเราเองกลับเผยแพร่ให้ขยายวงการรับรู้มากขึ้นด้วยความเป็นห่วงในการเห็นข้อมูลนี้ไม่เหมาะสม เผยแพร่จาก 1 คน เป็น 2 จาก 2 เป็น 4 มากขึ้นเรื่อยๆ ทำให้จากเดิมมีคนรู้ไม่กี่คน ทำให้รู้มากขึ้น แบบนี้แสดงว่าผู้เผยแพร่นั้นกำลังตกเป็นเครื่องมือ หรือเป็นเหยื่ออยู่ เป็นต้น การตกเป็นเหยื่อในกรณีนี้ แก้ไขโดยหยุดทำการส่งข้อความ หรือข้อมูลต่อให้กับผู้อื่นที่เราควบคุมการเผยแพร่ข้อมูลไม่ได้ หากพบเรื่องไม่เหมาะสมต่อสถาบันหลักของประเทศ ก็ควรส่งให้กับหน่วยงานที่รับผิดชอบ หรือถ้าเป็นทางข้อมูลอินเทอร์เน็ตก็ส่งให้หน่วยงานในกระทวงเทคโนโลยีสารสนเทศและการสื่อสาร สายด่วน 1212 เป็นต้น

บทที่ 4

วิธีป้องกันตัวเองจากภัยคุกคามทางอินเทอร์เน็ต

ขอบเขต

เมื่อได้เรียนรู้จากบทก่อนหน้านี้แล้ว จะทำให้เราทราบถึงภัยคุกคามต่าง ๆ ที่อาจจะเกิดขึ้นจากการใช้งานอินเทอร์เน็ต ในบทนี้จะกล่าวถึงวิธีการป้องกันตัวเองจากภัยคุกคามทางอินเทอร์เน็ต เพื่อป้องกันตนเองจากการใช้ข้อมูลสารสนเทศต่อไป

วัตถุประสงค์

การเรียนรู้ถึงชนิดของภัยคุกคามต่าง ๆ ที่เกิดขึ้นจากการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตแล้ว ในหัวข้อเรื่องนี้จะบอกวิธีการป้องกันตนเองให้พ้นจากภัยคุกคามต่าง ๆ ได้ดีมากขึ้นจากเทคนิคการป้องกันภัย 10 ข้อ และกรณีศึกษาการป้องกันตนเองจากการทำธุรกรรมอิเล็กทรอนิกส์

เนื้อหา

1. เทคนิคการป้องกันภัยคุกคามทางอินเทอร์เน็ต 10 วิธี
2. กรณีศึกษาภัยคุกคามจากการทำธุรกรรมออนไลน์

4.1 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต

สำหรับการใช้งานส่วนบุคคล มีดังนี้

4.1.1 การตั้งสติก่อนเปิดเครื่อง ก่อนเปิดเครื่องคอมพิวเตอร์ให้รู้ตัวเสมอว่าเราอยู่ที่ไหน – ที่บ้าน ที่ทำงาน หรือที่สาธารณะและระมัดระวังการใช้งานคอมพิวเตอร์ตั้งแต่เริ่มเปิดเครื่อง ดังนี้

- ก่อน Login เข้าใช้งานคอมพิวเตอร์ ต้องมั่นใจว่าไม่มีใครแอบดู Password
- เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อคหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า Login ป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ได้อย่างง่าย อาจก่อการประสงค์ร้ายต่างๆ
- อย่าประมาทในการใช้งานอินเทอร์เน็ต จงตระหนักไว้ว่าข้อมูลความลับและความเป็นส่วนตัวอาจถูกเปิดเผยได้เสมอในโลกออนไลน์ แม้จะระมัดระวังมากเพียงใดก็ตามข้อมูลเหล่านั้นก็อาจถูกเปิดเผยได้

4.1.2 การกำหนด Password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้นและการใช้งานอินเทอร์เน็ตทั่วไป เช่นการ Login ระบบ e-mail, ระบบสนทนาออนไลน์ (chat) ระบบเว็บไซต์ที่เป็นสมาชิกอยู่ ทางที่ดีควรใช้ password ที่ต่างกันบ้างพอให้จำได้

4.1.3 การสังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์ ถูกเรียกใช้ขึ้นมาพร้อมๆ กับการเปิดเครื่องหรือไม่ ถ้าสังเกตไม่ทันให้สังเกตระยะเวลาบูตเครื่อง หากนานผิดปกติ อาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือภัยคุกคามรูปแบบต่างๆ ได้

4.1.4 การหมั่นตรวจสอบและอัพเดต OS หรือซอฟต์แวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่องคอมพิวเตอร์ เช่น โปรแกรมป้องกันไวรัส, โปรแกรมไฟร์วอลล์และ ควรใช้ระบบปฏิบัติการและ ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ควรอัพเดทอินเทอร์เน็ตบราวเซอร์ให้ทันสมัยอยู่เสมอ เนื่องจาก Application Software สมัยใหม่ มักพึ่งพาอินเทอร์เน็ตบราวเซอร์ ก่อให้เกิดช่องโหว่ใหม่ ๆ ให้ภัยคุกคามเจาะผ่านบราวเซอร์ และสร้างปัญหาให้เกิดได้

4.1.5 ไม่ลงซอฟต์แวร์มากเกินความจำเป็น ซอฟต์แวร์ที่จำเป็นต้องลงในเครื่องคอมพิวเตอร์ ได้แก่

- อินเทอร์เน็ตบราวเซอร์ เพื่อใช้เปิดเว็บไซต์ต่างๆ
- E-mail เพื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร
- โปรแกรมสำหรับงานด้านเอกสาร, โปรแกรมตกแต่งภาพ เสียง วิดีโอ
- โปรแกรมป้องกันไวรัสคอมพิวเตอร์ และ/หรือ โปรแกรมไฟร์วอลล์

หากจำเป็นต้องใช้โปรแกรมอื่น ๆ ควรพิจารณาใช้โปรแกรมที่ผ่าน Web Application เช่น Chat, VoIP เป็นต้น หรือบันทึกโปรแกรมลงบน Thumb Drive เพื่อประมวลผลจากภายนอกเครื่องคอมพิวเตอร์

ซอฟต์แวร์ที่ไม่ควรมีบนเครื่องคอมพิวเตอร์ที่ใช้งาน ได้แก่

1. ซอฟต์แวร์ที่ใช้ในการ Crack โปรแกรม
2. ซอฟต์แวร์สำเร็จรูปที่ใช้ในการโจมตีระบบ, เจาะระบบ (Hacking Tools)
3. โปรแกรมที่เกี่ยวกับการสแกนข้อมูล การดักรับข้อมูล (Sniffer) และอื่นๆ ที่อยู่ในรูปซอฟต์แวร์สำเร็จรูป ที่ไม่เป็นที่รู้จัก แม้ค้นหาข้อมูลก็ไม่พบรายละเอียด ซึ่งหากเป็นเช่นนี้ควรระมัดระวังหากจำเป็นต้องใช้ชุดซอฟต์แวร์ดังกล่าว
4. ซอฟต์แวร์ที่ใช้หลบหลีกการป้องกัน เช่น โปรแกรมที่ซ่อน IP address เพื่อป้องกันไม่ให้ผู้อื่นเห็น IP ที่แท้จริงนั้น มักใช้เส้นทางระบบเครือข่ายของอาสาสมัครต่าง ๆ ซึ่งในที่นี้อาจเป็นเครื่องของผู้ไม่ประสงค์ดีที่ต้องการดักข้อมูลของผู้ใช้งานทั่วไปก็ได้

4.1.6 ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เว็บไซต์ประเภทนี้ ได้แก่

- เว็บไซต์ลามก อนาจาร
- เว็บไซต์การพนัน
- เว็บไซต์ที่มีหัวเรื่อง "Free" แม้กระทั่ง Free Wi-Fi ที่คิดว่าได้เล่นอินเทอร์เน็ตฟรี แต่อาจเป็นแผนของ Hacker ให้มาใช้ระบบ Wi-Fi ก็เป็นได้ ให้คิดเสมอว่า "ไม่มีของฟรีในโลก" หากมีการให้ฟรีก็อาจมีของต่างตอบแทน เช่น โฆษณาแฝง เป็นต้น
- เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรม ซึ่งมีการแนบ file พร้อมทำงานในเครื่องคอมพิวเตอร์ ได้แก่ ไฟล์นามสกุล .exe .dll .vbs เป็นต้น
- เว็บไซต์ที่แจก Serial Number เพื่อใช้ crack โปรแกรม
- เว็บไซต์ที่ให้ดาวน์โหลด เครื่องมือในการเจาะระบบ (Hacking Tools)
- เว็บไซต์ที่เกี่ยวข้องกับยาเสพติด
- เว็บไซต์ที่มี Link ไม่ตรงกับชื่อ โดย Redirect ไปอีกหน้าเพจหนึ่งที่ชื่อไม่ตรงกับ domain ที่ต้องการใช้งาน
- เว็บไซต์ที่มีหน้าต่าง pop-up ขึ้นหลายเพจ
- เว็บไซต์ที่มีชื่อ domain ยาวและมีเครื่องหมายมากเกินปกติ ไม่ใช่ชื่อที่เหมาะแก่การตั้ง เช่น www.abc-xyz-xxx.com มีเครื่องหมาย “–” มากเกินไป
- เว็บไซต์ที่ทำตัวเองเป็น Proxy อนุญาตให้เราใช้งานแบบไม่ระบุชื่อ (anonymous) เนื่องจากผู้ใช้ Free proxy มักประมาทและคำนึงแต่ผลประโยชน์ จนลืมคิดไปว่าการได้ IP Address นั้นปลอม จากการใช้ Anonymous Proxy อาจจะถูกสร้างขึ้นเพื่อดักข้อมูลของผู้ใช้ดังกล่าวก็ได้

ทั้งหมดที่กล่าวมานั้นเป็นข้อสังเกตเว็บไซต์เสี่ยงภัย หากหลีกเลี่ยงการเข้าเว็บที่มีลักษณะดังกล่าวไม่ได้ ก็ควรตั้งสติให้รอบคอบ และระมัดระวังในการใช้งานเว็บไซต์ดังกล่าวในข้างต้น

4.1.7 สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ เว็บไซต์ E-Commerce ที่ปลอดภัยควรมีลักษณะดังนี้

- มีการทำ HTTPS เนื่องจาก HTTPS จะมีการเข้ารหัสข้อมูล เพื่อป้องกันการดัก User name และ Password ในเวลาที่ทำการ Login เข้าใช้บริการ e-commerce
- มีใบรับรองทางอิเล็กทรอนิกส์ (Certificate Authority : CA) เพื่อช่วยในการยืนยันตัวบุคคลและรักษาความปลอดภัยในการรับส่งข้อมูลผ่านระบบอินเทอร์เน็ตที่ใช้บนเครื่องให้บริการนั้น
- มีมาตรฐาน (Compliance) รองรับ เช่นการผ่านมาตรฐาน PCI/DSS สำหรับเว็บไซต์ E-Commerce เป็นต้น

4.1.8 ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network ชื่อที่ใช้ควรเป็นชื่อเล่นหรือฉายาที่กลุ่มเพื่อนรู้จัก และไม่ควรเปิดเผยข้อมูลดังต่อไปนี้

- เลขที่บัตรประชาชน
- เบอร์โทรศัพท์ส่วนตัว
- หมายเลขบัตรเครดิต
- หมายเลขหนังสือเดินทาง
- ข้อมูลทางการแพทย์
- ประวัติการทำงาน

หากจำเป็นต้องกรอกข้อมูลดังกล่าว ให้สังเกตว่าเว็บไซต์นั้นน่าเชื่อถือหรือไม่ พิจารณาจากเนื้อหาในเว็บไซต์ที่ควรบ่งบอกรายละเอียดที่มาในการให้บริการ และควรเป็นเว็บไซต์ที่รู้จักกันแพร่หลาย เพื่อหลีกเลี่ยงปัญหาการถูกดักข้อมูลส่วนตัวจากการสร้างเว็บไซต์หลอกลวง (Phishing) และป้องกันข้อมูลปรากฏในระบบค้นหา (Search Engine) ที่ไม่ประสงค์จะให้สาธารณชนได้รับรู้

4.1.9 ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือ ให้คำนึงถึงใจเขาใจเรา – หากเราไม่ชอบสิ่งใด ก็ไม่ควรทำสิ่งนั้นกับผู้อื่น ในเวลาแสดงความคิดเห็นบนกระดานแสดงความคิดเห็น (Web board), การรับส่ง e-mail, หรือการกระทำใดๆ กับข้อมูลบนอินเทอร์เน็ต

4.1.10 ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนปักใจเชื่อในสิ่งที่ได้รับรู้

10 วิธีข้างต้นถือเป็นคาถาสำหรับผู้ใช้อินเทอร์เน็ต เพื่อเพิ่มความระมัดระวังในการใช้งานอินเทอร์เน็ตให้มากขึ้น เพราะภัยคุกคามจากการใช้อินเทอร์เน็ตมักเกิดจากพฤติกรรมการใช้งานของผู้ใช้งาน การมีชุดซอฟต์แวร์ป้องกันในเครื่องมิใช่คำตอบสุดท้าย ความปลอดภัยจะเกิดขึ้นได้ล้วนแล้วแต่พึ่งพาสติและความรู้เท่าทันของผู้ใช้งาน

ความมั่นคงปลอดภัยของข้อมูลจะเกิดขึ้นได้ ต้องเริ่มต้นจากตัวเองเสียก่อน หากผู้ใช้งานปลอดภัย ระบบเครือข่ายภายในองค์กรนั้นก็จะปลอดภัย เครือข่ายองค์กรอื่นๆที่มาร่วมใช้งานระบบก็ปลอดภัย เกิดเป็นห่วงโซ่แห่งความปลอดภัย จากระดับเล็กสู่ระดับใหญ่ ไปถึงระดับชาติ ช่วยให้ประเทศของเราปลอดภัยจากการใช้ระบบสารสนเทศได้

นอกจากนี้ ในปัจจุบันมีการทำธุรกรรมออนไลน์กันอย่างแพร่หลาย และเกิดเหตุฉ้อโกงให้เห็นเป็นข่าวอยู่บ่อยครั้ง จึงขอหยิบยกบทความ “ธุรกรรมออนไลน์ ภัยร้ายแฝงเงามืด” เพื่อให้ตระหนักถึงปัญหาและหาทางป้องกันไม่ให้ภัยออนไลน์เข้าถึงตัวได้โดยง่าย

4.2 กรณีศึกษาธุรกรรมออนไลน์

เมื่อหลายเดือนก่อนได้เกิดคดีที่เกี่ยวข้องกับการทำธุรกรรมทางอินเทอร์เน็ต โดยผู้เสียหายได้ใช้บริการ Internet Banking และตกเป็นเหยื่อโดยไม่รู้ตัว ซึ่งเมื่อตรวจสอบพบว่ามีผู้ดักข้อมูลโดยใช้โปรแกรม Key Logger ซึ่งคอยเก็บข้อมูลจากแป้นคีย์บอร์ดขณะใช้งาน และส่งผ่านระบบอินเทอร์เน็ตให้กับแฮกเกอร์ ซึ่งนำข้อมูลที่ได้มานั้นมาสวมรอยเป็นผู้ใช้งาน เข้าทำธุรกรรมทางการเงิน ซึ่งสร้างความเสียหายมูลค่าไม่น้อย เหตุการณ์นี้สามารถป้องกันได้ โดยผู้ใช้งานและผู้ให้บริการระบบธุรกรรมออนไลน์ควรตระหนักและรู้เท่าทันภัยคุกคาม ตลอดจนเสริมสร้างเทคโนโลยีให้ปลอดภัยมากยิ่งขึ้น

ในปัจจุบันแฮกเกอร์ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคาร หรือผู้ให้บริการธุรกรรมออนไลน์ เพื่อเข้าถึงชั้นความลับของลูกค้าเพียงอย่างเดียว แต่เปลี่ยนเป้าหมายเป็นผู้ใช้งาน (User) อินเทอร์เน็ต ซึ่งเข้าถึงได้ง่ายกว่าแทน โดยอาศัยความรู้เท่าไม่ถึงการณ์ เนื่องจากมีการใช้งานอินเทอร์เน็ตอย่างทั่วถึงมากยิ่งขึ้น บางครั้งผู้ใช้งานอาจพยายามดาวน์โหลดโปรแกรมหรือข้อมูลบางอย่างที่แฮกเกอร์ได้เผยแพร่ไว้ตามเว็บสาธารณะยอดนิยม โดยโปรแกรมดังกล่าวมักมีชื่อที่ดึงดูดให้ดาวน์โหลด เช่น clip ฉาว, โปรแกรมเร่งความเร็ว, โปรแกรม crack serial number, โปรแกรมเกมส์ เป็นต้น เมื่อผู้ใช้งานหลงดาวน์โหลดโปรแกรมดังกล่าวมาติดตั้งในเครื่อง อาจมีมัลแวร์แฝงมากับไฟล์ ทำให้ผู้ใช้ตกเป็นเหยื่อมิจฉาชีพที่จ้องดักข้อมูลได้

ในแง่ผู้ใช้งานทั่วไป : ต้องป้องกันภัยคุกคามที่เกิดขึ้นโดยตระหนักรู้ และควบคุมพฤติกรรมตนเองในการใช้งานอินเทอร์เน็ต บนเครื่องคอมพิวเตอร์ส่วนตัวไม่ดาวน์โหลดโปรแกรมที่ไม่มั่นใจในความปลอดภัย, หมั่นดูแลเครื่องคอมพิวเตอร์ให้มีการอัพเดททั้งซอฟต์แวร์ป้องกัน และ Patch, ตั้งรหัสผ่านที่ยากต่อการคาดเดา หากต้องทำธุรกรรมทางอินเทอร์เน็ต เช่น ซื้อสินค้า หรือทำธุรกรรมทางการเงิน ให้ทำบนเครื่องตนเองที่คิดว่าปลอดภัย, เลือกช่องทางการใช้งานให้ถูกต้อง เช่น เมื่อมีการ Login ผ่านเว็บไซต์ให้ดูว่าเป็นการใช้ผ่าน HTTPS หรือไม่ หากไม่ใช่ก็ไม่ควรใช้ โดยเฉพาะหากอยู่ในวง LAN ไม่ว่าจะเป็นร้านอินเทอร์เน็ตคาเฟ่ หรือบริษัท เพราะอาจมีการดัก User / Password ผ่านระบบเครือข่ายได้ และควรเลือกใช้บริการธุรกรรมอินเทอร์เน็ตจากผู้ให้บริการที่น่าเชื่อถือเท่านั้น

ในแง่ผู้ให้บริการ : ผู้ให้บริการต้องให้ความสำคัญกับเทคโนโลยีในการระบุตัวตนผู้ใช้งาน, ดูแลความปลอดภัยของข้อมูลและวิธีการใช้งานเมื่อลูกค้าต้องทำธุรกรรมผ่านระบบอินเทอร์เน็ต ตลอดจนให้ความรู้แก่ลูกค้าให้รู้เท่าทันถึงภัยคุกคามในปัจจุบัน

ในที่นี้ ขอเน้นเรื่องการใช้เทคโนโลยีการพิสูจน์ตัวตนของลูกค้าที่ทำธุรกรรมออนไลน์ ซึ่งที่ใช้กันอยู่มี 3 รูปแบบคือ

* สิ่งที่คุณมี (Something you have) เช่น กุญแจไขประตู, บัตรอิเล็กทรอนิกส์ หรือระบบ Token เป็นต้น
* สิ่งที่คุณรู้ (Something you know) คือ รหัสผ่านหรือชุดตัวเลขเฉพาะ

* สิ่งที่คุณเป็น (Something you are) เป็นการพิสูจน์ตัวตนแบบชีวมาตร เช่น ลายนิ้วมือ ระบบรู้จำเสียง ระบบสแกนม่านตา เป็นต้น

นอกจากระบบพิสูจน์ตัวตนแล้ว ผู้ให้บริการควรมีนโยบายด้านความมั่นคงปลอดภัยข้อมูล ตลอดจนวิธีการปฏิบัติและการควบคุมที่เหมาะสม และควรประเมินความสามารถของเทคนิคการพิสูจน์ตัวตนที่ใช้อยู่ว่าสามารถรับมือกับภัยคุกคามและความเสี่ยงใหม่ๆ ที่เกิดขึ้นได้หรือไม่ การประเมินความเสี่ยงอย่างสม่ำเสมอ จะช่วยลดความเสี่ยงภายในระบบได้

สำหรับผู้ให้บริการธุรกรรมออนไลน์ผ่าน Web Application ที่ยังไม่ได้จัดทำระบบ Two Factor Authentication ก็ควรมีการเก็บค่าการล็อกอินหน้าเว็บ ให้สามารถสืบได้ว่ามีใครเข้ามาใช้บริการเว็บไซต์บ้าง (คำว่า “ใคร” ในที่นี้ ประกอบด้วย IP ที่เรียกใช้บริการ, ชื่อ ISP, ชุดคำสั่งในการใช้บริการ ได้แก่ ชนิดบราวเซอร์ ระบบปฏิบัติการ รวมถึง Session ID ของค่า Cookie ซึ่งเครื่องแม่ข่ายที่ให้บริการสร้างขึ้น เป็นต้น) ทั้งหมดนี้เพื่อสร้างความปลอดภัยให้กับลูกค้า ในลักษณะเดียวกับกล้องวงจรปิดที่ติดตั้งตามตู้ ATM ซึ่งจะช่วยให้ผู้ให้บริการสามารถเก็บบันทึก Log File ได้สอดคล้องตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อีกด้วย

กล่าวโดยสรุปคือ ผู้ให้บริการด้านพาณิชย์อิเล็กทรอนิกส์ เช่น สถาบันการเงิน, ผู้ประกอบธุรกิจ E-Commerce ควรนำเทคโนโลยีการพิสูจน์ตัวตนแบบ Two-Factor Authentication มาใช้เป็นอย่างน้อย ตลอดจนให้ความรู้แก่ลูกค้าในการทำธุรกรรมผ่านระบบอินเทอร์เน็ต เพื่อไม่ให้ตกเป็นเหยื่อของพวกมิจฉาชีพที่นับวันจะมีวิธีการที่ซับซ้อนและแยบยลขึ้น

บทที่ 5

ศัพท์ทางเทคนิคที่เกี่ยวข้องการหาข่าว และปฏิบัติการหาข้อมูลข่าวสาร

ขอบเขต

ในบทนี้กล่าวถึงเทคนิคในการหาข่าวและเข้าใจถึงความหมาย และวิธีการปฏิบัติการข้อมูลสารสนเทศเบื้องต้น หรือที่เรียกว่า IOs (Information Operations) ซึ่งเป็นจิตวิทยาในการสร้างกระแสข้อมูลเพื่อใช้ในสงครามการข่าวสาร

วัตถุประสงค์

เพื่อให้มีความรู้ความเข้าใจคำศัพท์เทคนิคในการหาข่าว เข้าใจถึงความหมาย และวิธีการปฏิบัติการข้อมูลสารสนเทศเบื้องต้น หรือที่เรียกว่า IOs (Information Operations) ซึ่งเป็นจิตวิทยาในการสร้างกระแสข้อมูล เพื่อใช้ในสงครามการข่าวสาร หรือเรียกว่า Cyber warfare ให้สร้างสรรค์และเป็นประโยชน์ต่อสังคมตามภารกิจของลูกเสือไซเบอร์

เนื้อหาในบทนี้

1. หัวใจหลักของปฏิบัติการข้อมูลข่าวสาร (Information Operations)
2. องค์ประกอบหลักของปฏิบัติการข้อมูลข่าวสาร
3. คำศัพท์ที่ควรรู้สำหรับการข่าว และด้านความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ

5. การปฏิบัติการข้อมูลข่าวสาร

5.1 หัวใจหลักของปฏิบัติการข้อมูลข่าวสาร (Information Operations)

การปฏิบัติการข้อมูลข่าวสารเป็นการบูรณาการสารสนเทศในทุกๆ ด้าน เพื่อปกป้อง, สนับสนุน และเพื่อการเพิ่มอำนาจ ในการปฏิบัติการด้านมวลชน (Public affairs) ที่เป็นการปฏิบัติการในการส่งข่าวสารสู่สื่อสารมวลชน การปฏิบัติการจิตวิทยาที่เป็นการปฏิบัติการ ฝ่ายผู้ใช้พยายามสร้างอิทธิพลผลในแง่ความคิด ความเชื่อ และการตกลงใจต่อฝ่ายตรงข้าม ให้เป็นไปตามที่ฝ่ายผู้ใช้ต้องการ

ในปัจจุบันหลายหน่วยงานได้นำแนวความคิดในการปฏิบัติการข่าวสารมาใช้ในการปฏิบัติการ เพื่อสร้างผลกระทบหรือสร้างอิทธิพลต่อกระบวนการตกลงใจข่าวสาร และระบบสารสนเทศของฝ่ายตรงข้าม ขณะเดียวกันก็ดำเนินการป้องกันข่าวสาร และระบบสารสนเทศของฝ่ายผู้ใช้ ปรัชญาของการทำสงครามของกองทัพในหลายประเทศ คือออกแบบเครื่องมือหรือวิธีการในการทำลายความประสานสอดคล้องของการปฏิบัติของฝ่ายตรงข้าม ด้วยการหลอกลวงและสร้างความสับสนจนกระทั่งการปฏิบัติของฝ่ายตรงข้ามลดความรวดเร็ว รุนแรง และการจู่โจมลง

5.2 องค์ประกอบหลักของปฏิบัติการข้อมูลข่าวสาร

5.2.1 การปฏิบัติการจิตวิทยา (Psychological Operations: PSYOP)

คือ การปฏิบัติเพื่อนำข่าวสารและสิ่งชี้แนะที่ได้เลือกไว้ให้แก่ผู้รับเพื่อต้องการให้เกิดผลทางอารมณ์ การจูงใจ ความมีเหตุผลและประการสุดท้ายที่สำคัญที่สุดคือ มีผลต่อพฤติกรรมของรัฐบาลต่อประเทศ องค์การ กลุ่มชนและบุคคล

การปฏิบัติการจิตวิทยาสามารถแยกออกเป็น 3 ระดับได้ดังนี้

ก. ระดับยุทธศาสตร์ การปฏิบัติการจิตวิทยา อาจจะดำเนินการในรูปแบบทางการเมืองหรือทางการทูต การประกาศหรือแถลงการณ์

ข. ระดับยุทธการ การปฏิบัติการจิตวิทยา สามารถกระทำด้วยการแจกใบปลิว การกระจายเสียง หรือ สื่อการแพร่ข่าวอื่นๆ ซึ่งในบางสถานการณ์ต้องคำนึงถึงการใช้สื่อใหม่ เช่น สื่อดิจิตอลต่างๆในระบบเครือข่ายสังคมเป็นต้น

ค. ระดับยุทธวิธี การปฏิบัติการจิตวิทยา จะใช้การกระจายเสียงเพื่อเพิ่มความกลัว และเกิดความกระด้างกระเดื่องในกลุ่มเป้าหมาย

5.2.2 การลวงทางทหาร (Military Deception: MILDEC)

คือ การปฏิบัติการที่มีเป้าหมายไม่เพียงแต่ทำให้ผู้ที่ทำการตัดสินใจของฝ่ายตรงข้ามคิดผิดเท่านั้น ยังมีวัตถุประสงค์กระทำเพื่อให้ผู้ที่ทำการตัดสินใจของฝ่ายตรงข้ามมีความคิดที่ไม่ถูกต้อง เกี่ยวกับขีดความสามารถหรือความตั้งใจของฝ่ายเรา การปฏิบัติการลวงขึ้นอยู่กับการปฏิบัติด้านการข่าว ในการกำหนดเป้าหมายการลวงที่เหมาะสม เพื่อช่วยในการสร้างเรื่องที่น่าเชื่อถือมากขึ้น

5.2.3 การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security : OPSEC)

คือ กระบวนการในการวางแผนและปฏิบัติเพื่อให้ได้มาและดำรงรักษาความลับที่สำคัญเกี่ยวกับขีดความสามารถการปฏิบัติ และเจตนารมณ์ที่แท้จริงของผู้บงการ

5.2.4 การสงครามอิเล็กทรอนิกส์ (Electronic Warfare : EW)

คือ การปฏิบัติการทางทหารที่เกี่ยวกับการใช้คลื่นแม่เหล็กไฟฟ้าและส่งพลังงานโดยตรงเพื่อควบคุมแถบคลื่นแม่เหล็กไฟฟ้า การควบคุมนี้ไม่จำกัดเฉพาะคลื่นวิทยุหรือเรดาร์เท่านั้นยังรวมถึงคลื่นที่มองเห็น และอินฟาเรดพลังงานของคลื่นต่างๆ ที่อาจนำมาใช้ทำงานเกี่ยวกับอาวุธสงครามอิเล็กทรอนิกส์ เช่น การจำกัดคลื่นความถี่วิทยุต่างๆ เพื่อไม่ให้สามารถส่งข่าวสาร หรือข้อมูลถึงกันได้

5.2.5 การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations: CNO)

คือ การประสานการใช้องค์ประกอบทั้ง 5 ได้แก่ OPSEC, PSYOP, MILITARY DECEPTION, EW, PHYSICAL DESTRUCTION ทำให้เกิดศักยภาพในการทำลายฝ่ายตรงข้าม ซึ่งถือว่าเป็นผลการทวีกำลัง (Synergistic Effects) โดยการปฏิบัติหลักทั้ง 5 ประการนี้ร่วมกับการปฏิบัติสนับสนุน และการปฏิบัติที่เกี่ยวข้องแล้ว จะเป็นเครื่องมือหลักในการสร้างอิทธิพลต่อบุคคลหรือกลุ่มบุคคลเป้าหมาย (Target Audiences: Tas) ในฝ่ายตรงข้ามอันจะทำให้กำลังรบมีเสรีในการปฏิบัติในสภาวะแวดล้อมของข่าวสาร

5.3 คำศัพท์ที่ควรรู้สำหรับการข่าว และด้านความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ

5.3.1 การรักษาความลับ (Confidentiality=C)

หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูล หรือถ้ามองอีกมุมหนึ่งก็จะหมายถึง การปกป้องข้อมูลไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้นั่นเอง ข้อมูลบางอย่างที่มีความสำคัญ ซึ่งจำเป็นต้องเก็บไว้เป็นความลับเพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้

5.3.2 การรักษาความถูกต้องสมบูรณ์ (Integrity=I)

หมายถึง ความเชื่อถือได้ของข้อมูล และการทำให้สารสนเทศที่อ่อนไหว และมีคุณค่า ไม่ถูกเปิดเผยโดยคนที่ไม่ได้รับอนุญาตแหล่งที่มา ซึ่งการรักษาความถูกต้องของข้อมูลนั้นคือ การป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงจากสภาพเดิม หรือการป้องกันไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตสามารถเปลี่ยนแปลงข้อมูลได้

5.3.3 การรักษาความพร้อมใช้ของสารสนเทศเมื่อต้องการเข้าถึง (Availability=A)

หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการความพร้อมใช้งาน เป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) เนื่องจากการที่ระบบไม่พร้อมใช้งานก็จะไม่ต่างกับการที่ไม่มีระบบเลย ส่วนหนึ่งของความพร้อมใช้งานที่เกี่ยวกับการรักษาความปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยการทำให้ระบบไม่สามารถทำงานได้

5.3.4 การพิสูจน์ตัวตน (Authentication)

หมายถึง การพิสูจน์ทราบตัวตนนั้นเกิดขึ้นเมื่อระบบควบคุมพิสูจน์ว่าผู้ใช้เป็นบุคคลนั้นจริงหรือไม่ เช่น ถ้าผู้ใช้ระบบยูสเซอร์เนมแล้วก็ต้องสามารถระบุรหัสผ่านที่คู่กับยูสเซอร์นั้นได้ หรืออีกตัวอย่างหนึ่งคือ การใช้ใบรับรองอิเล็คทรอนิกส์ในการสร้างการเชื่อมต่อแบบ SSL (Secure Socket Layer) เพื่อพิสูจน์ว่าเซิร์ฟเวอร์ที่เชื่อมต่ออยู่นั้นเป็นเครื่องที่ต้องการเชื่อมต่อจริงๆ

5.3.5 การไม่สามารถปฏิเสธความรับผิดชอบในการทำธุรกรรม (Non-Repudiation)

หมายถึง วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้ว และผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่า ไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

บทที่ 6
การค้นหารายชื่อผู้จดทะเบียนทางอินเทอร์เน็ต

ขอบเขต

ในบทนี้จะกล่าวถึงเทคนิคค้นหารายชื่อผู้จดทะเบียนทางอินเทอร์เน็ต นั้นจำเป็นต้องเข้าใจถึงหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับอินเทอร์เน็ต และการเรียนรู้แผนที่อินเทอร์เน็ตรวมทั้งค่า IP Address และ Domain Name ที่ควรศึกษา

วัตถุประสงค์

เพื่อให้มีความรู้ในการค้นหารายชื่อผู้จดทะเบียนทางอินเทอร์เน็ต ดังนี้

1. การเรียนรู้เกี่ยวกับหน่วยงานที่เป็นผู้กำหนดค่า Domain / IP Address
2. การเรียนรู้แผนที่อินเทอร์เน็ตประเทศไทย รู้จักค่า ASN
3. การค้นหาเว็บไซต์ต้องสงสัย ที่กระทบต่อสถาบันหลักของประเทศไทยสามารถสืบค้น รายชื่อผู้จดทะเบียน ที่อยู่อีเมล์ ผู้ดูแลเว็บไซต์ (Web master) ได้
4. การค้นหาที่ตั้งของค่า IP Address รายชื่อผู้ให้บริการอินเทอร์เน็ต ISP ได้อย่างถูกต้อง

เนื้อหา

อินเทอร์เน็ตเกิดขึ้นในปี ค.ศ. 1969 (พ.ศ. 2512) จากการเกิดเครือข่าย ARPANET (Advanced Research Projects Agency NETwork) ซึ่งเป็นเครือข่ายสำนักงานโครงการวิจัยชั้นสูงของกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยมีวัตถุประสงค์หลักของการสร้างเครือข่าย เพื่อให้คอมพิวเตอร์สามารถเชื่อมต่อ และมีปฏิสัมพันธ์กันได้ เครือข่าย ARPANET ถือเป็นเครือข่ายเริ่มแรก ซึ่งต่อมาได้ถูกพัฒนาให้เป็นเครือข่ายอินเทอร์เน็ตในปัจจุบัน

6.1 หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับพัฒนาอินเทอร์เน็ต

6.1.1. สมาคมอินเทอร์เน็ต หรือ ไอซ็อก (ISOC : Internet Society)

องค์กรระหว่างประเทศที่ก่อตั้งขึ้นเมื่อ พ.ศ. 2535 ไอซ็อกเป็นองค์กรที่ไม่มุ่งเน้นผลกำไรและมีนโยบายสนับสนุนการใช้อินเทอร์เน็ตให้แพร่หลาย รวมทั้งสนับสนุนการจัดทำมาตรฐานอินเทอร์เน็ตโดยอาศัย IAB, IETF และ IRTF นอกจากนี้ไอซ็อกยังทำหน้าที่สนับสนุนการวิจัยและให้ทุนในกิจกรรมที่เกี่ยวข้องกับอินเทอร์เน็ต

6.1.2 ไอเอบี (IAB : Internet Architecture Board)

เป็นหน่วยงานที่ก่อตั้งขึ้นเมื่อ พ.ศ. 2526 แต่เดิมนั้นใช้ชื่อว่า Internet Activities Board เมื่อไอซ็อกถือกำเนิดขึ้นก็ได้โอน IAB เข้ามาเป็นหน่วยงานในสังกัด หน้าที่ของ IAB คือผลักดันและดูแลพัฒนาการด้านเทคนิคของอินเทอร์เน็ตให้กับไอซ็อก IAB ดูแลองค์กรสองแห่งซึ่งดำเนินงานด้านเทคนิคโดยตรงได้แก่ IETF และ IRTF นอกจากนี้ไอเอบียังทำหน้าที่จัดการงานบรรณาธิการและตีพิมพ์เอกสาร RFC และการกำหนดหมายเลขเพื่อใช้ในอินเทอร์เน็ต โดย IAB มอบภาระงานทั้งสองนี้ให้กับ บรรณาธิการ อาร์เอฟซี (RFC Editor) และ ไอนา (IANA : Internet Assigned Number Authority) ตามลำดับ ส่วน ICANN จะกล่าวในเนื้อหาต่อไปเนื่องจากเป็นหน่วยงานที่สำคัญต่อการจัดสรรค่าโดเมน และค่าไอพีที่ใช้ในอินเทอร์เน็ตปัจจุบัน

6.1.3. ICANN (Internet Cooperation for Assigned Names and Number)

ออกเสียงว่า "ไอแคน" เป็นองค์กรที่มีหน้าที่บริหารทรัพยากรโดเมนและจัดสรรค่าไอพี ที่ดำเนินงานแบบไม่หวัง ผลกำไร (non-profit organization) มีโครงสร้างการดำเนินงานที่อาศัยความร่วมมือจากนานาชาติ และบริหารจัดการโดย คณะกรรรมการที่ได้รับเลือกมาจากนานาชาติ

การทำงานของ ICANN

การสร้างและบริหารนโยบายต่างๆ เพื่อให้เกิด เสถียรภาพและความมั่นคงของระบบโดเมนแก่ประชาคมอินเทอร์เน็ตโลก ซึ่งมีผู้มีส่วนได้ส่วนเสีย (ICANN's stakeholder model) ดังนี้

- ผู้มีผลประโยชน์ทางธุรกิจ (Business Interests)
- ภาคพลเมืองในสังคม (Civil Society)
- ภาครัฐที่เกี่ยวข้อง (Government & Government Agencies)
- ผู้ให้บริการเลขหมายอินเทอร์เน็ต (Internet Service Provider)
- ผู้ลงทะเบียนโดเมนเนม (Registrants)
- ผู้รับลงทะเบียนโดเมนเนม (Registrars)
- ประสานความร่วมมือและการทำงานร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียต่างๆ
- สร้างและดำเนินการกระบวนการฉันทามติเพื่อเป็นตัวแทนการตัดสินใจให้ประชาคมอินเทอร์เน็ตโลก เช่น Public comment
- จัดให้มีกระบวนการร้องขอ,อนุมัติและดำเนินการรวมทั้งกำกับดูแลเพื่อเปิดใช้งานโดเมนระดับบนสุด ทั้งgTLD และ ccTLD ในระบบโดเมนโลก
- กำกับดูแลการดำเนินงานของ Registry, Registrar และ Sponsorship Organization ให้เป็นไปตามสัญญาต่างๆ
- กำกับดูแลนโยบายเพื่อกรณีพิพาทในโดเมนเนม

- เป็นผู้บริหารนโยบายการดำเนินงานให้แก่ IANA ซึ่งเป็นหน่วยปฏิบัติงานด้านการดูแล root server รวมทั้งการดูแลการจัดสรรหมายเลข IP

- พัฒนาและดูแลหน่วยงานภายใน ICANN ที่ประกอบไปด้วยตัวแทนจากภาคส่วนต่างๆ

- เผยแพร่การดำเนินงานต่างๆของ ICANN แก่ประชาคมอินเตอร์เน็ต

หน้าที่ส่วนหนึ่งของ ICANN ยังมอบอำนาจให้ศูนย์สารสนเทศเครือข่ายอินเทอร์เน็ตที่แบ่งออกไปตามภูมิภาคทำหน้าที่ดูแลการจัดสรรแอดเดรสและบริหารโดเมน ได้แก่

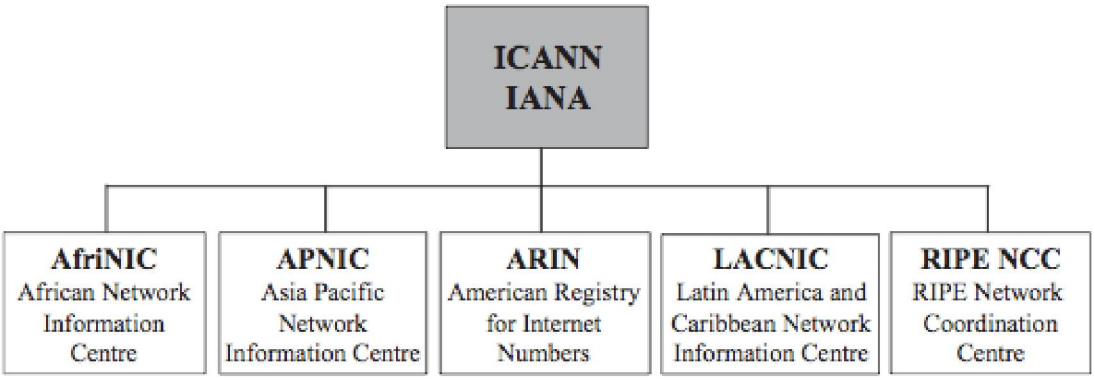
- ARIN (American Registry for Internet Numbers) ทำหน้าที่ให้บริการสำหรับกลุ่มประเทศในทวีปอเมริกาและแคนาดา

- RIPE (Reseaux IP Europeens Network Coordination Centre) ทำหน้าที่ให้บริการสำหรับกลุ่มประเทศในทวีปยุโรป

- APNIC (Asia Pacific Network Information Centre) ทำหน้าที่ดูแลแถบเอเชีย-แปซิฟิก ซึ่งผู้ให้บริการอินเทอร์เน็ตในประเทศไทย หรือ ISP (Internet Services Provider) นั้นไม่ว่าจะเป็น CATTelecom , TOT , True หรือ 3BB ก็จะต้องถูกจัดสรรค่า IP Address และ Domain จาก APNIC เป็นอันดับแรกก่อน

- AfriNIC (African Network Information Centre) ทำหน้าที่ให้บริการสำหรับกลุ่มประเทศทวีปแอฟริกา

- LACNIC (Latin America and Caribbean Network Information Centre) จะทำหน้าที่ให้บริการสำหรับกลุ่มลาตินอเมริกา และแถบทะเลแคริบเบียน



ภาพที่ 6.1 โครงสร้างหน่วยงานที่เกี่ยวข้องกับการจัดสรรค่า IP Address และ Domain name

6.2 IP Address คืออะไร ?

เลขที่อยู่ไอพี (อังกฤษ: IP address) หรือชื่ออื่น เช่น ที่อยู่ไอพี, หมายเลขไอพี, เลขไอพี, ไอพีแอดเดรส คือหมายเลขที่ใช้ในระบบเครือข่ายที่ใช้โพรโทคอลอินเทอร์เน็ต (IP) คล้ายกับหมายเลขโทรศัพท์ ที่เครื่องคอมพิวเตอร์ เครื่องเราท์เตอร์ เครื่องแฟกซ์ จะมีหมายเลขเฉพาะตัวโดยใช้เลขฐานสอง จำนวน 32 บิต โดยการเขียนจะแบ่งเป็นชุด 4 ชุด โดยแต่ละชุดจะใช้เลขฐานสองจำนวน 8 บิต ซึ่งโดยทั่วไปแล้ว ผู้คนส่วนใหญ่จะคุ้นเคยกับระบบเลขฐานสิบ จึงมักแสดงผลโดยการใช้เลขฐานสิบจำนวน 4 ชุด ซึ่งแสดงถึงหมายเลขเฉพาะของเครื่องนั้น สำหรับการส่งข้อมูลภายในเครือข่ายแลน (LAN) แวน (WAN) หรืออินเทอร์เน็ต โดยหมายเลขไอพีมีไว้เพื่อให้ผู้ส่งรู้ว่าเครื่องของผู้รับคือใคร และผู้รับสามารถรู้ได้ว่าผู้ส่งคือใคร

6.2.1 IP Version 4 (IPv4)

ระบบตัวเลขไอพีที่ใช้ในปัจจุบันเป็นระบบ ไอพีเวอร์ชันที่ 4 (IPv4) ซึ่งจะเป็นระบบ 32 บิตหรือสามารถระบุเลขไอพีได้ตั้ง 0.0.0.0 ถึง 255.255.255.255 (ตัวเลขบางตัวเป็นไอพีสงวนไว้สำหรับหน้าที่เฉพาะเช่น 127.0.0.0 จะเป็นการระบุถึงตัวอุปกรณ์เองไม่ว่าอุปกรณ์นั้นจะมีไอพีสื่อสารจริงๆ เป็นเท่าไร) อย่างไรก็ตามจากระบบตัวเลขที่จำกัดนี้สามารถเพิ่มขยายด้วยเทคนิคของไอพีส่วนตัว (private IP) กับการแปลงไอพี (Network Address Translation หรือ NAT)

6.2.2 คลาส (Class)

ไอพีเวอร์ชัน 4 ทั้งหมดถูกแบ่งออกเป็น Class ชนิดต่างๆเพื่อจุดประสงค์ในการใช้งานที่ต่างๆกันดังต่อไปนี้

1. คลาส A เริ่มตั้งแต่ 1.0.0.1 ถึง 127.255.255.254
2. คลาส B เริ่มตั้งแต่ 128.0.0.1 ถึง 191.255.255.254
3. คลาส C เริ่มตั้งแต่ 192.0.1.1 ถึง 223.255.254.254
4. คลาส D เริ่มตั้งแต่ 224.0.0.0 ถึง 239.255.255.255 ใช้สำหรับงาน multicast
5. คลาส E เริ่มตั้งแต่ 240.0.0.0 ถึง 255.255.255.254 ถูกสำรองไว้ ยังไม่มีการใช้งาน

สำหรับไอพีในช่วง 127.0.0.0 ถึง 127.255.255.255 ใช้สำหรับการทดสอบระบบ

6.2.3 ไอพีส่วนตัว (Private IP)

ไอพีส่วนตัวมีไว้สำหรับใช้งานภายในองค์กรเท่านั้น ไม่ว่าองค์กรนั้นจะมีขนาดใหญ่หรือเล็กเพียงใดก็ตาม ได้แก่

1. ไอพีส่วนตัว คลาส A เริ่มตั้งแต่ 10.0.0.0 ถึง 10.255.255.255 สับเน็ตมาสต์ที่ใช้ได้ เริ่มตั้งแต่ 255.0.0.0 ขึ้นไป
2. ไอพีส่วนตัว คลาส B เริ่มตั้งแต่ 172.16.0.0 ถึง 172.31.255.255 สับเน็ตมาสต์ที่ใช้ได้ เริ่มตั้งแต่ 255.240.0.0 ขึ้นไป
3. ไอพีส่วนตัว คลาส C เริ่มตั้งแต่ 192.168.0.0 ถึง 192.168.255.255 สับเน็ตมาสต์ที่ใช้ได้ เริ่มตั้งแต่ 255.255.0.0 ขึ้นไป

ไอพีส่วนตัวข้างต้นถูกกำหนดให้ไม่สามารถนำไปใช้งานในเครือข่ายสาธารณะ (Internet)

6.2.4 ไอพีสาธารณะ (Public IP)

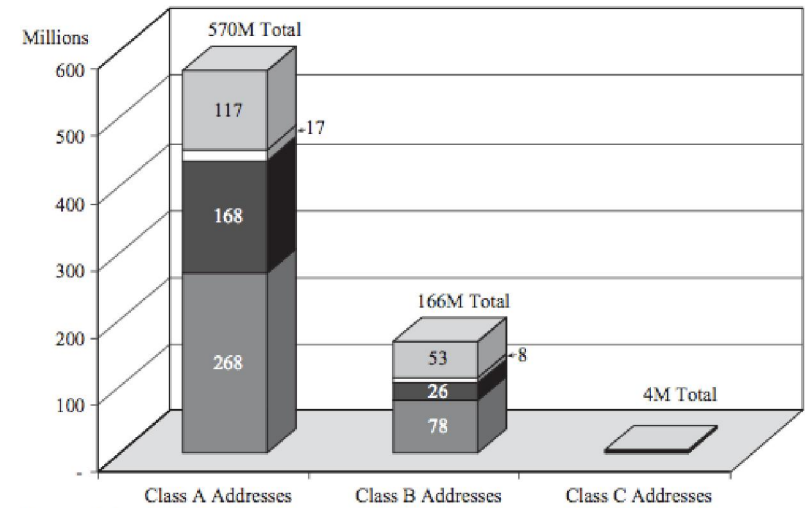
ไอพีสาธารณะมีไว้สำหรับให้แต่ละองค์กร แต่ละบุคคลต่างก็สามารถเชื่อมต่อเข้าหากัน รับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

6.2.5 การแปลงไอพี (NAT)

เนื่องจากเมื่อแต่ละองค์กร แต่ละบุคคลต่างก็ใช้งานไอพีส่วนตัวกับเครื่องคอมพิวเตอร์ของตนเอง ซึ่งส่งผลให้ไม่สามารถติดต่อกับเครือข่ายสาธารณะ (Internet) ได้ จึงทำให้องค์กรเหล่านี้จำเป็นต้องอาศัยการแปลงไอพี เพื่อช่วยให้เครื่องคอมพิวเตอร์ของตนเองสามารถเชื่อมต่อกับเครือข่ายสาธารณะ ได้ นอกจากนี้ไอพีสาธารณะเองก็มีอยู่อย่างจำกัด ทำให้เมื่อแต่ละองค์กร แต่ละบุคคลต้องการที่จะเชื่อมต่อเข้ากับเครือข่ายสาธารณะจะทำให้เกิดปัญหาไอพีสาธารณะไม่เพียงพอต่อการใช้งาน ดังนั้นเพื่อให้เกิดการใช้งานไอพีสาธารณะอย่างมีประสิทธิภาพจึงจำเป็นต้องมีการแปลงไอพีส่วนตัวของแต่ละองค์กรให้สามารถแบ่งปันกันใช้งาน ไอพีสาธารณะที่มีอยู่อย่างจำกัด (Overloaded NAT) ในแง่ของความปลอดภัย การแปลงไอพีสามารถช่วยเพิ่มความปลอดภัยให้กับระบบเครือข่ายได้ เนื่องจากเครื่องคอมพิวเตอร์จากเครือข่ายสาธารณะทั้งหลาย จะไม่สามารถรู้จักไอพีที่แท้จริงของคอมพิวเตอร์ในองค์กร ทำให้ความเสี่ยงที่คอมพิวเตอร์ภายในองค์กรจะถูกโจมตีในแง่ต่างๆลดลงไปด้วย

6.2.6 IP Address version 6 (IPv6)

ไอพีเวอร์ชันที่ 6 (IPv6) ถูกพัฒนาขึ้นมาด้วยจุดประสงค์หลักในการแก้ปัญหาการขาดแคลนจำนวนหมายเลขไอพี ซึ่งกำหนดโดยมาตรฐานไอพีเวอร์ชันที่ 4 ซึ่งในมาตรฐานของเวอร์ชัน 6 นี้จะใช้ระบบ 128 บิตในการระบุหมายเลขไอพี



	Class A Addresses	Class B Addresses	Class C Addresses
Commercial	117,440,512	53,346,304	2,417,408
Government	16,777,216	8,454,144	184,832
Defense	167,772,160	25,755,648	219,648
Research	268,435,456	78,446,592	1,328,896

รูปที่ 6.2 สถิติการใช้ IP Address เมื่อแบ่งตามประเภทหน่วยงาน

6.3 โดเมนเนม (Domain Name)

ชื่อโดเมน หรือ โดเมนเนม (domain name) หมายถึง ชื่อที่ใช้ระบุลงในคอมพิวเตอร์ (เช่น เป็นส่วนหนึ่งของที่อยู่เว็บไซต์ หรืออีเมลแอดเดรส) เพื่อไปค้นหาในระบบ โดเมนเนมซีสเทม เพื่อระบุถึง ไอพีแอดเดรส ของชื่อนั้นๆ เป็นชื่อที่ผู้จดทะเบียนระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน บางครั้งเราอาจจะใช้ "ที่อยู่เว็บไซต์" แทนก็ได้

โดเมนเนม หรือ ชื่อโดเมน เป็นชื่อที่ตั้งขึ้นเพื่อให้ง่ายต่อการจดจำ เนื่องจากไอพีแอดเดรสนั้นจดจำได้ยากกว่า และเมื่อการเปลี่ยนแปลงไอพีแอดเดรส ผู้ใช้ไม่จำเป็นต้องรับรู้หรือจดจำไอพีแอดเดรสใหม่ ยังสามารถใช้โดเมนเนมเดิมได้ต่อไป

หนึ่งไอพีแอดเดรส สามารถใช้โดเมนเนมได้มากกว่า 1 โดเมนเนม และหลายๆ โดเมนเนมอาจจะใช้ไอพีแอดเดรสเดียวกันได้

Domain Name Server (DNS) คือสิ่งที่นำมาอ้างถึงหมายเลขเครื่อง หรือ หมายเลข IP Address เพื่อให้ง่ายต่อการจดจำ DNS จะทำหน้าที่คล้ายกับสมุดโทรศัพท์ คือ เมื่อต้องการจะโทรศัพท์หาใคร ก็จะต้องเปิดสมุดโทรศัพท์เพื่อค้นหาเบอร์โทรศัพท์ของผู้ที่ต้องการจะติดต่อ คอมพิวเตอร์ก็เช่นกัน เมื่อต้องการจะสื่อสารกับคอมพิวเตอร์เครื่องอื่น เครื่องนั้นก็จะทำการสอบถามหมายเลข IP ของเครื่องที่ต้องการจะสื่อสาร กับ DNS server ซึ่งจะทำการค้นหาหมายเลขดังกล่าว ในฐานข้อมูลแล้วแจ้งให้ Host ดังกล่าวทราบ ระบบ DNS แบ่งออกได้เป็น 3 ส่วน คือ

Name Resolvers โดยเครื่อง Client ที่ต้องการสอบถามหมายเลขไอพีเรียกว่า Resolver ซึ่งซอฟต์แวร์ที่ทำหน้าที่เป็น Resolvers นั้นจะถูกสร้างมากับแอพพลิเคชันหรือเป็น Library ที่มีอยู่ใน Client

Domain Name Space เป็นฐานข้อมูลของ DNS ซึ่งมีโครงสร้างเป็น Tree หรือเป็นลำดับชั้น แต่ละโหนดคือโดเมนโดยสามารถมีโดเมนย่อย (Sub Domain) ซึ่งจะใช้จุดในการแบ่งแยก

Name Servers เป็นคอมพิวเตอร์ที่รันโปรแกรมจัดการฐานข้อมูลบางส่วนของ DNS โดย Name Server จะตอบการร้องขอทันที โดยการหาข้อมูลตัวเอง หรือส่งต่อการร้องขอไปยัง Name Server อื่น ซึ่งถ้า Name Server มีข้อมูลของส่วนโดเมนแสดงว่า Server นั้นเป็นเจ้าของโดเมนเรียกว่า Authoritative แต่ถ้าไม่มีเรียกว่า Non-Authoritative

6.4 การจดทะเบียนชื่อโดเมน

แบ่งออกเป็น 2 ประเภท คือ

1. การจดทะเบียนโดเมนต่างประเทศ

   ก. .com ใช้ทำเว็บไซต์ของบริษัท ห้างร้านโดยทั่วไป รวมทั้งเว็บไซต์ส่วนตัว และมีบางครั้งนำไปใช้ทำเว็บไซต์ (web site) ประเภทอื่นๆ ด้วย

   ข. .net ใช้ทำเว็บไซต์เกี่ยวกับระบบเน็ตเวิร์ค (network) ของคอมพิวเตอร์ หรือเว็บไซต์บริการอินเทอร์เน็ต แต่บางครั้งก็นำไปใช้ด้านอื่นด้วย

   ค. .org ใช้ทำเว็บไซต์ของส่วนราชการ บางครั้งก็มีการจดทะเบียนนำไปใช้กับเว็บไซต์ประเภทอื่นด้วย

2. การจดทะเบียนโดเมนภายในประเทศ

   ก. .co.th ใช้ทำเว็บไซต์ของบริษัท ห้างร้านโดยทั่วไป

   ข. .or.th ใช้ทำเว็บไซต์ของส่วนราชการ และชื่อโดเมนต้องเป็นชื่อขององค์กร หรือตัวย่อของชื่อองค์กรนั้นๆ ต้องใช้สำเนาเอกสารทางราชการเป็นหลักฐานการจดทะเบียน

   ค. .ac.th ใช้ทำเว็บไซต์ของสถานศึกษาต่างๆ ชื่อของโดเมนที่จดทะเบียนต้องเป็นชื่อของสถานศึกษานั้นๆ หรือชื่อย่อของชื่อสถานศึกษา ใช้สำเนาเอกสารการขออนุญาตก่อตั้งสถานศึกษาเป็นหลักฐาน

   ง. .go.th ใช้ทำเว็บไซต์ของส่วนราชการของประเทศไทย โดยปกติจะเป็นองค์กรขนาดใหญ่

   จ. .in.th ใช้ทำเว็บไซต์ของบุคคลธรรมดาโดยทั่วไป ชื่อโดเมนจะใช้ชื่ออะไรก็ได้ แต่ต้องอยู่ภายใต้นโยบายชื่อโดเมน ของ THNIC การจดโดเมนนี้ ใช้สำเนาบัตรประชาชน หรือสำเนาใบขับขี่เป็นหลักฐานการจดทะเบียน

หลักที่ใช้ในการตั้งชื่อโดเมน

1. ความยาวของชื่อ Domain ตั้งได้ไม่เกิน 63 ตัวอักษร
2. สามารถใช้ตัวอักษรภาษาอังกฤษผสมกับตัวเลข หรือเครื่องหมายขีด (-) ได้
3. ตัวอักษรภาษาอังกฤษ ใช้ตัวเล็กหรือตัวใหญ่ก็ได้
4. ห้ามใช้เครื่องหมายขีด (-) นำหน้าชื่อ domain
5. ห้ามเว้นวรรคในชื่อโดเมน

6.5 แผนที่อินเทอร์เน็ต

ค่า ASN หรือชื่อเต็มว่า Autonomous System Number จะเป็นค่าประจำ Router ในระดับ Gateway มีความสำคัญในการกระจายค่าที่เป็น Public IP Address โดยกำหนดช่วง IP Address (Prefix) การเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่าง Router ตัวอื่นๆ ในระบบเครือข่ายอินเทอร์เน็ต

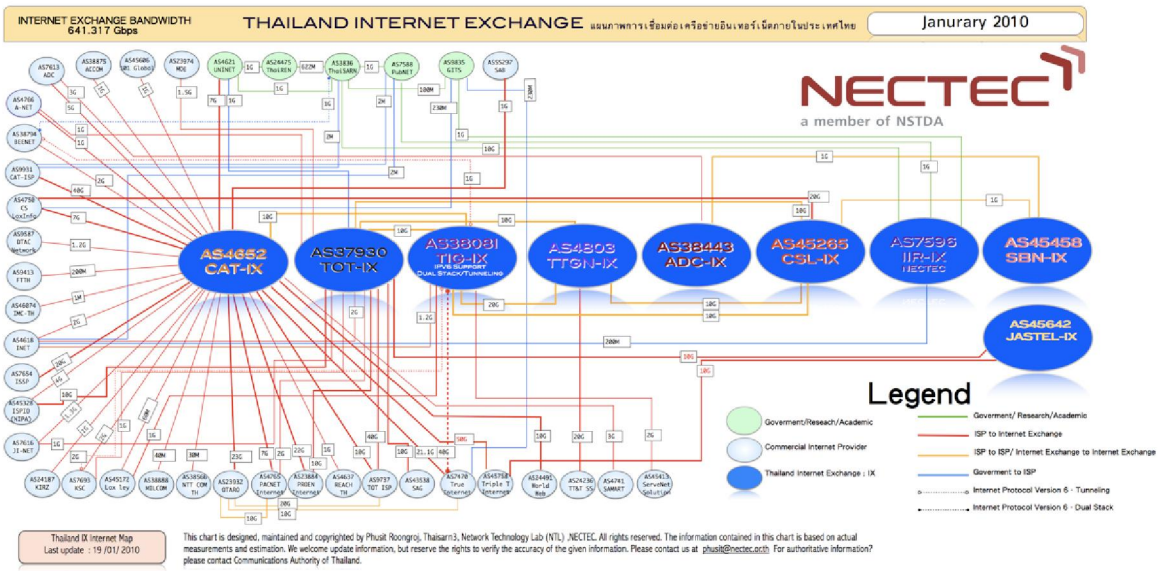
ยกตัวอย่าง ASN ที่สำคัญในประเทศไทยคือ AS4651 ของ CAT Telecom เป็น Gateway ขาต่างประเทศตัวใหญ่ของประเทศไทย ที่มีจำนวน Link ระหว่าง Router ในแต่ละ ISP ในประเทศไทยมากที่สุดส่วนขาในประเทศคือ AS9931 ที่กระจายค่า IP Address ให้กับหน่วยงานสำคัญๆ ในประเทศไทยเป็นต้น

ภาพที่ 6.3 หน่วยงานที่ดูแลค่า AS Number

แผนที่อินเทอร์เน็ตสำหรับใช้ในการรับ-ส่งข้อมูลภายในประเทศ จะเห็นว่าช่องวงกลมสีน้ำเงินวงใหญ่จะเป็นค่า ASN Router สำหรับ Gateway ของผู้ให้บริการอินเทอร์เน็ต (ISP) รายใหญ่ที่มีจำนวนค่า Public IP Address จำนวนมาก ทำการเชื่อมต่อทางอินเทอร์เน็ตในปริมาณแบนวิธ (Bandwidth) ที่แตกต่างกันขึ้นอยู่การจัดสรรค่า IP Address ที่ได้ลงทะเบียนผ่าน APNIC ประจำภูมิภาคเอเชียที่จัดสรรค่า IP Address ให้แต่ละผู้ให้บริการ (ISP) ในประเทศไทย

ยกตัวอย่าง การติดต่อเว็บไซต์ในประเทศไทย เช่น เว็บ xxxx.com จะพบว่า xxxx.com ตั้งอยู่ที่ KSC ซึ่งถือว่าเป็นผู้ให้บริการอินเทอร์เน็ตรายหนึ่งในประเทศไทย

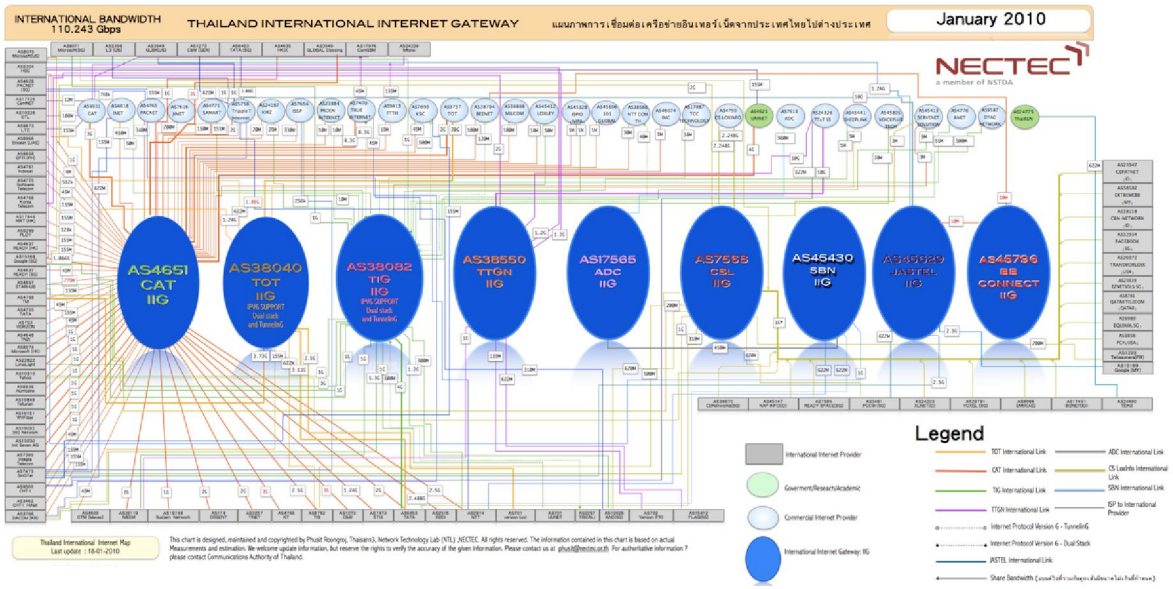
ดังนั้น หากจะเปิดเว็บไซต์ xxxx.com และการใช้อินเทอร์เน็ตของ TOT ในติดต่อสื่อสารของเราจะเกิดขึ้นภายใต้แผนที่อินเทอร์เน็ตนี้นั้นหมายถึง TOT AS37930 จะต้องเชื่อมกับ AS7693 ของ KSC ซึ่งหากเราต้องการรู้ตำแหน่งและผ่านช่องทางผู้ให้บริการทางอินเทอร์เน็ตใดบ้างก็ต้องทำการ trace route ดูเพื่อคำนวณจำนวน hop ที่เกิดขึ้น เป็นต้น



ภาพที่ 6.4 แผนที่อินเทอร์เน็ตภายในประเทศ (NIX)

การรับส่งข้อมูล ผ่าน ASN Router ในระดับ Gateway แผนที่นี้จะแสดงเส้นทางการติดต่อสื่อสารจากประเทศไทยไปยังผู้ให้บริการในต่างประเทศ จะสังเกตเห็นว่า AS4651 CAT Telecom นั้นมีเส้นเชื่อมการติดต่อสื่อสารจำนวนมาก นั้นแสดงว่าในหลายๆ ผู้ให้บริการอินเทอร์เน็ตในประเทศไทย เวลาติดต่อสื่อสารข้อมูลที่ต้องผ่านต่างประเทศส่วนใหญ่จำเป็นต้องออกเส้นทางนี้

ยกตัวอย่าง หากเราต้องการเปิดเว็บไซต์ google.com ที่ตั้งอยู่ประเทศอเมริกา โอกาสที่เราใช้อินเทอร์เน็ตที่บ้านหรือที่โรงเรียนเส้นทางการติดต่อเว็บ google.com มีโอกาสผ่าน AS4651 ของ CAT Telecom ได้ เป็นต้น



ภาพที่ 6.5 แผนที่อินเทอร์เน็ตภายนอกประเทศ (IIG)

เมื่อเข้าใจถึงที่มาค่า IP Address / Domain name ค่า ASN และหลักการไหลเวียนข้อมูลที่เกิดขึ้นจากการติดต่อสื่อสารผ่านอินเทอร์เน็ตแล้ว เพื่อให้ตรงตามวัตถุประสงค์ในการสืบหาข้อมูล และให้เกิดประโยชน์แก่ภารกิจของลูกเสือไซเบอร์จำเป็นต้องเรียนรู้เครื่องมือในการหาข่าวที่มาของ IP Address / Domain / ASN โดยผ่านเครื่องมือที่เรียกว่า Whois ซึ่งการ Whois สามารถทำได้ผ่านทางอินเทอร์เน็ตเว็บไซต์ โดยผ่านตัวอย่างการใช้งานดังนี้

1. เว็บไซต์ชื่อ Who.is
2. เว็บไซต์ Netcraft / robtex
3. เว็บไซต์ checkdomain.com
4. เว็บไซต์ sran.org

บทที่ 7
ความรู้เบื้องต้นระบบค้นหาข้อมูล

ขอบเขต

ในบทนี้กล่าวถึงเรื่องของเครื่องมือการค้นหา และเทคโนโลยีที่ใช้ รวมไปถึงชนิดต่าง ๆ ของเครื่องมือ และวิธีการในการใช้เครื่องมือในการค้นหาเพื่อดึงความสามารถในการค้นหามาใช้ได้อย่างเต็มที่

วัตถุประสงค์

- การเรียนรู้เทคโนโลยีที่ใช้ในการทำระบบค้นหาข้อมูล (Search Engine)
- การเรียนรู้ชนิดระบบค้นหาข้อมูลทางอินเทอร์เน็ต
- การนำความรู้ที่ได้จากการค้นหาข้อมูลไปใช้ได้อย่างมีประสิทธิภาพมากขึ้น

เนื้อหา

1. เทคโนโลยีของระบบค้นหาข้อมูล(Search engine)
2. ชนิดของเว็บไซต์ค้นหาข้อมูลทางอินเทอร์เน็ต
3. อธิบายการค้นหาบางส่วนที่เป็นประโยชน์

ระบบค้นหาข้อมูล (search engine) คือโปรแกรมที่ช่วยในการสืบค้นหาข้อมูล โดยเฉพาะข้อมูลบนอินเทอร์เน็ต โดยครอบคลุมทั้งข้อความ รูปภาพ ภาพเคลื่อนไหว เพลง ซอฟต์แวร์ แผนที่ ข้อมูลบุคคล กลุ่มข่าว และอื่น ๆ ซึ่งแตกต่างกันไป แล้วแต่โปรแกรมหรือผู้ให้บริการแต่ละราย ระบบค้นหาข้อมูลส่วนใหญ่จะค้นหาข้อมูลจากคำสำคัญ (คีย์เวิร์ด) ที่ผู้ใช้ป้อนเข้าไป จากนั้นก็จะแสดงรายการผลลัพธ์ที่คิดว่าผู้ใช้น่าจะต้องการขึ้นมาในปัจจุบัน ระบบค้นหาข้อมูลบางตัว เช่น กูเกิล (Google) จะบันทึกประวัติการค้นหาและการเลือกผลลัพธ์ของผู้ใช้ไว้ด้วย และจะนำประวัติที่บันทึกไว้นั้นมาช่วยกรองผลลัพธ์ในการค้นหาครั้งต่อไป

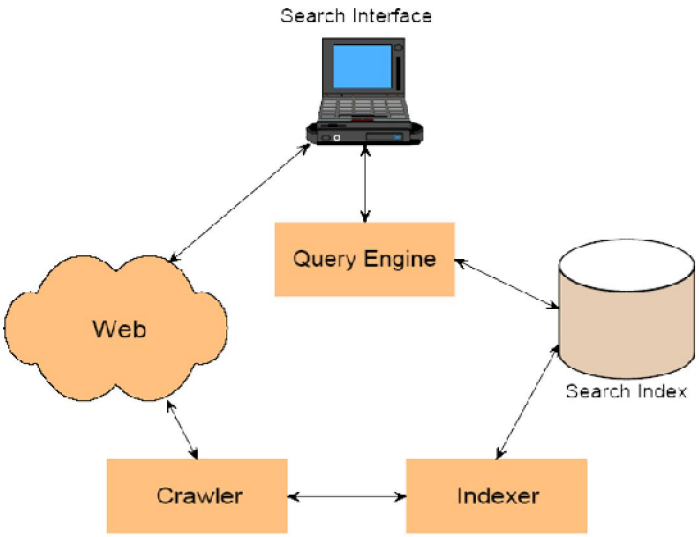
7.1 เทคโนโลยีของระบบค้นหาข้อมูล(Search engine)

ประกอบด้วย 3 ส่วนดังนี้

1. Keyword Index การค้นหาข้อมูล โดยการค้นจากข้อความในเว็บเพจที่ได้ผ่านการสำรวจมาแล้ว จะอ่านข้อความ ข้อมูล อย่างน้อยๆ ประมาณ 200-300 ตัวอักษรแรกของเว็บเพจนั้นๆ โดยการอ่านนี้จะหมายรวมไปถึงอ่านข้อความที่อยู่ในโครงสร้างภาษา HTML ซึ่งอยู่ในรูปแบบของข้อความที่อยู่ในคำสั่ง alt ซึ่งเป็นคำสั่งภายใน TAG คำสั่งของรูปภาพ แต่จะไม่นำคำสั่งของ TAG อื่นๆ ในภาษา HTML และคำสั่งในภาษา JAVA มาใช้ในการค้นหา วิธีการค้นหาของ Search Engine ประเภทนี้จะให้ความสำคัญกับการเรียงลำดับข้อมูลก่อน-หลัง และความถี่ในการนำเสนอข้อมูลนั้น การค้นหาข้อมูล โดยวิธีการนี้จะมีความรวดเร็วมาก แต่มีความละเอียดในการจัดแยกหมวดหมู่ของข้อมูลค่อนข้างน้อย เนื่องจากไม่ได้คำนึงถึงรายละเอียดของเนื้อหาเท่าที่ควร

2. Subject Directories การจำแนกหมวดหมู่ข้อมูล Search Engine ประเภทนี้ จะจัดแบ่งโดยการวิเคราะห์เนื้อหา รายละเอียดของแต่ละเว็บเพจ ว่ามีเนื้อหาเกี่ยวกับอะไร โดยการจัดแบ่งนี้จะใช้แรงงานคนในการพิจารณาเว็บเพจ ซึ่งทำให้การจัดหมวดหมู่ขึ้นอยู่กับวิจารณญาณของคนจัดหมวดหมู่แต่ละคนว่าจะจัดเก็บข้อมูลนั้นๆ อยู่ในเครือข่ายข้อมูลอะไร ดังนั้นฐานข้อมูลของ Search Engine ประเภทนี้จะถูกจัดแบ่งตามเนื้อหาก่อน แล้วจึงนำมาเป็นฐานข้อมูลในการค้นหาต่อไป การค้นหาค่อนข้างตรงกับความต้องการของผู้ใช้ และมีความแม่นยำในการค้นหาสูง เป็นต้นว่า หากเราต้องการหาข้อมูลเกี่ยวกับเว็บไซต์ หรือเว็บเพจที่นำเสนอข้อมูลเกี่ยวกับคอมพิวเตอร์ Search Engine ก็จะประมวลผลรายชื่อเว็บไซต์มาที่ผู้ใช้

3. Metasearch Engines จุดเด่นของการค้นหาด้วยวิธีการนี้ คือ สามารถเชื่อมโยงไปยัง Search Engine ประเภทอื่นๆ และยังมีความหลากหลายของข้อมูล แต่การค้นหาด้วยวิธีนี้มีจุดด้อย คือ วิธีการนี้จะไม่ให้ความสำคัญกับขนาดของตัวอักษร และมักจไม่รองรับประเภท Natural Language (ภาษาพูด) ดังนั้นหากผู้ใช้จะใช้ Search Engine แบบนี้ควรตระหนักถึงข้อบกพร่องเหล่านี้ด้วย



ภาพที่ 7.1 กระบวนการค้นหาข้อมูล

7.2 ชนิดของเว็บไซต์ค้นหาข้อมูลทางอินเทอร์เน็ต

1. กูเกิล (Google)
2. ยาฮู(Yahoo!)
3. เอ็มเอสเอ็น (MSN หรือ Bing)
4. เอโอแอล (AOL)
5. อาส์ก (Ask)
6. ไป่ตู้ (Baidu) ระบบค้นหาข้อมูล อันดับ 1 ของประเทศจีน
7. Cuil
8. ยานเดกซ์ (Yandex) ระบบค้นหาข้อมูล อันดับ 1 ของรัสเซีย

ภาพที่ 7.2 ผู้ให้บริการระบบค้นหาข้อมูล

7.3 คำอธิบายการค้นหาบางส่วนที่เป็นประโยชน์

1. การค้นหาข้อมูลในเว็บไซต์เป้าหมาย

วิธีค้นหาเฉพาะจงเว็บไซต์เป้าหมายโดยกำหนด site: ชื่อ URL เช่น ถ้าผู้ใช้ต้องการหาเว็บเกี่ยวกับการสอบ admission ของมหาวิทยาลัยธรรมศาสตร์ ให้พิมพ์ admission site:www.tu.ac.th

2. การค้นหา Link ต่างๆในเว็บไซต์เป้าหมาย

เมื่อเราต้องการค้นหาว่าในเว็บไซต์ที่เราสนใจนั้นมีความเกี่ยวข้องสัมพันธ์กับเว็บอื่นๆ หรือไม่ก็สามารถทำได้โดยการค้นหาดังนี้ ให้พิมพ์ link: ชื่อ URL เช่น link:www.tu.ac.th

3. การค้นหาชนิดของนามสกุลของไฟล์

เราใช้คำค้นหาได้ดังนี้ filetype:ชื่อ นามสกุลไฟล์ เช่น หากต้องการค้นหา filetype ชนิดของ Microsoft Powerpoint 2008 ให้พิมพ์ filetype:pptx

4. การค้นหาอดีตที่เคยปรากฏของเว็บไซต์หรือข้อมูลบนเว็บไซต์เป้าหมาย

ใน Google สามารถเก็บ Cached ของเว็บที่จะเข้าชมไว้ได้ (โดยคลิ้กที่ Cached หรือ ถูกเก็บไว้ ใน Google ภาษาไทย) ประโยชน์ของ google cache คือช่วยให้เราสามารถเข้าเว็บไซต์ ที่อาจโดนลบไปแล้ว โดยข้อมูลที่ได้จะเป็นข้อมูลก่อนถูกลบ

ยกตัวอย่างเช่น การค้นหา Cached เว็บไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือ mict.go.th ก็ให้พิมพ์ http://webcache.googleusercontent.com/search?q=cache:0MIb7p7kOOIJ:www.mict.go.th

5. การค้นหา E-mail ของหน่วยงานหรือเว็บไซต์เป้าหมาย

ค้นหาประเภทนี้จะทำให้เราได้รายชื่อของ E-mail หน่วยงานนั้นๆ ซึ่งอาจเป็นชื่อพนักงานคนหนึ่ง หรือชื่อกลุ่ม E-mail ของหน่วยงานหรือชื่อผู้ติดต่อเว็บไซต์นั้นๆ โดยใช้การค้นหาว่า @ ตามด้วยชื่อเว็บไซต์หน่วยงาน ยกตัวอย่างเช่น @mict.go.th เป็นต้น

6. การค้นหาอื่นๆ ที่เป็นประโยชน์

การใช้เครื่องหมายคำพูดใส่ระหว่างคำ (Keyword) ที่เราต้องการค้นหาเฉพาะก็จะทำให้การค้นหานั้นเจาะจงมากขึ้น เช่น ค้นหาคำว่า "Cyber Scout” ก็จะค้นหาเฉพาะคำที่เขียนแบบนี้โดยเฉพาะ Google จะใช้ and (และ) อยู่ในประโยคเสมอ เช่น ค้นหา harvest moon back to nature Google จะค้นหาแบบ harvest AND moon AND back

การใช้ OR (หรือ) คือการให้ Google หาข้อมูลมากขึ้นจาก คำ A และ คำ B (คือนำผลที่ได้ มารวมกัน) วิธีใช้ พิมพ์ OR ด้วยตัวใหญ่ระหว่างคำที่ต้องการ เช่น vacation london OR paris คือหาทั้งใน London และ Paris

บทที่ 8

หลักการและเทคนิคการค้นหาข้อมูลทางอินเทอร์เน็ต

ขอบเขต

ในบทนี้จะกล่าวถึงหลักการและเทคนิคการค้นหาข้อมูลทางอินเทอร์เน็ต ซึ่งผู้เรียนจะได้ทราบถึงเทคนิคการค้นหาเชิงประยุกต์ผ่านระบบ Search engine รวมถึงการค้นหาข้อมูลรายชื่อบุคคลและเว็บไซต์ที่ต้องการในเชิงประยุกต์ได้

จุดประสงค์

1. เพื่อเรียนรู้เทคนิคการใช้ Google ในการค้นหาข้อมูลเชิงลึก
2. เพื่อเรียนรู้เทคนิคการค้นหารายชื่อบุคคล
3. เพื่อเรียนรู้เทคนิคการค้นหาประวัติของข้อมูล

เนื้อหา

1) เทคนิคการค้นหาข้อมูลจาก Google ในเชิงลึก
2) เทคนิคการค้นหาข้อมูลรายชื่อบุคคล
3) เทคนิคการค้นหาประวัติของข้อมูล

8.1 เทคนิคการค้นหาข้อมูลจาก Google ในเชิงลึก

8.1.1 ค้นหาดูเฉพาะ Title ของเว็บไซต์

เทคนิคการค้นหาดูเฉพาะ Title จะใช้คำว่า intitle: ตามด้วยชื่อข้อความที่ต้องการดู title วิธีนี้จะนิยมใช้กับการค้นหาข้อมูลเชิงลึกโดยเรียกว่า google hack

การใช้ google ค้นหาข้อมูลเชิงลึก หรือทีเรียกว่า google Hack สามารถเข้าถึงข้อมูลที่ถูกซ่อนไว้หากผู้ดูแลระบบเว็บไซต์หรือเทคโนโลยีดังกล่าวขาดความระมัดระวัง เช่น การใช้เทคโนโลยีกล้องวงจรปิด ที่ติดไว้โดยสามารถดูผ่านช่องทางอินเทอร์เน็ตได้ กล้องวงจรปิดเหล่านั้นอาจถูกผู้อื่นเข้ามาดูได้โดยผ่านการค้นหาแบบ google hack

การแอบดูกล้องวงจรปิด Online ผ่าน google hack เรียกเทคนิคนี้ว่า "Various Online Devices" ยกตัวอย่างการใช้คำค้นหา ยี่ห้อกล้อง Webcam ที่ชื่อว่า EvoCam ใช้คำค้นหาว่า intitle:"EvoCam" inurl:"webcam.html"

อีกตัวอย่าง กล้องวงจรปิดยี่ห้อ AXIS ก็สามารถแอบดูได้ผ่านช่องทางการค้นหา google โดยใช้วิธีการพิมพ์ว่า intitle:"Live View / - AXIS" | inurl:view/view.shtml OR inurl:view/indexFrame.shtml | intitle:"MJPG Live Demo" | "intext:Select preset position"

8.1.2 การค้นหาช่องโหว่เครื่องแม่ข่าย (Server)

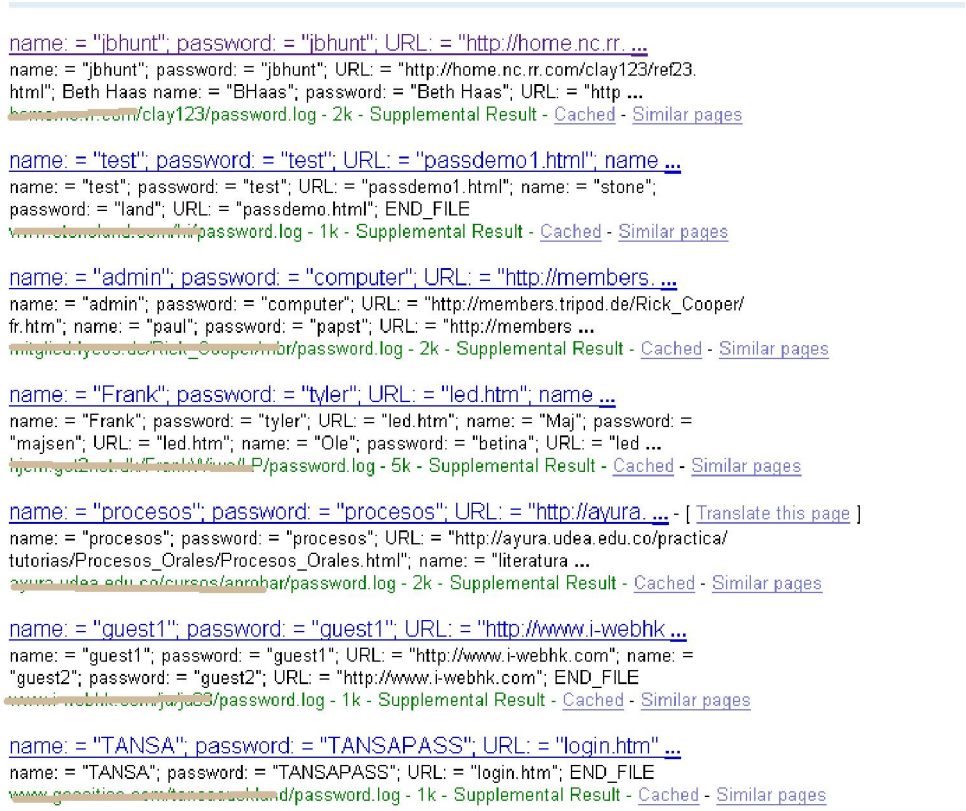
การใช้การค้นหาจาก google เพื่อค้นหาช่องโหว่ของระบบ ยกตัวอย่างเช่น เว็บไซต์ที่ใช้โปรแกรม EasyPHP ในการเขียนเว็บไซต์ อาจถูกค้นหาแบบ google โดยใช้การพิมพ์ว่า intitle:"[EasyPHP] – Administration" จะสามารถรู้ถึงหน้าบริหารจัดการของผู้ดูแลเว็บไซต์ได้

การเข้าสู่ folder ที่ไม่เปิดเผย ของ Web server IIS โดยค้นหาคำว่า " Microsoft-IIS/* server at" intitle:index.of จะพบว่ามองเห็น folder ที่เว็บไซต์ที่ไม่ได้เปิดให้คนทั่วไปเข้าถึงได้

ภาพที่ 8.1 การค้นหาโดยคำว่า Microsoft-IIS/* server at" intitle:index.of

8.1.3 การค้นหา Password โดยใช้ google

เทคนิคการค้นหา Password นั้นจะใช้คำว่า filetype:log inurl:"password.log" จะพบ password.log ที่เกิดขึ้นใน web server



ภาพที่ 8.2 Username และ Password ที่ได้มาจากการค้นหาของ google

ปัจจุบันเทคนิคดังกล่าว ได้เป็นที่รู้จักกันอย่างแพร่หลาย ผู้ไม่หวังดีอาจใช้เทคนิคหลอกล่อ ทำให้ผู้ที่คิดริลอง อาจติดมัลแวร์จากการทดลองใช้เทคนิคดังกล่าวได้

8.2 การค้นหารายชื่อบุคคล

8.2.1 การค้นหาชื่อบุคคล สามารถทำได้ โดยค้นหาจาก

- ใส่ชื่อ หรือ นามสกุล หรือ ทั้งชื่อ และนามสกุล ใส่เครื่องหมาย “ ” แล้วสืบค้นหาใน google, bing หรือ yahoo

- ค้นหาชื่อและประวัติการทำงานจากเว็บไซต์สมัครงาน หรือ เว็บชื่อ www.linkedin.com เป็นเว็บไซต์แสดง Profile และโดยส่วนมากแล้วคนไทยยังนิยมน้อยอยู่มาก

- ค้นหารายชื่อในเว็บไซต์สมุดหน้าเหลือง www.yellowpages.co.th โดยคลิกเมนูไปที่บุคคลใส่ข้อมูลชื่อ หรือนามสกุลที่ต้องการค้นหาส่วนนี้จะได้ที่อยู่ และเบอร์โทรศัพท์

8.2.2 การค้นหาที่อยู่ประกอบด้วย

- ที่อยู่ของบุคคล หากทราบเบอร์โทรศัพท์บ้านค้นหาได้ 2 ที่คือ เว็บไซต์สมุดหน้าเหลือง และ เว็บไซต์ Phonebook ของ TOT phonebook.tot.co.th

- ที่อยู่ของ IP Address ซึ่งส่วนนี้ต้องเป็น Public IP Address สำหรับตรวจสอบ IP ของตนเองสามารถตรวจสอบได้ที่ http://www.whatismyipaddress.com หรือใช้วิธีตรวจสอบผ่านเว็บไซต์ที่รองรับ GeoIP เช่น เว็บไซต์ http://www.liveipmap.com จะระบุตำแหน่งผ่านแผนที่ภูมิศาสตร์ได้ แต่อาจไม่ตรงความจริงนัก ส่วนเว็บไซต์ http://checkip.me เว็บนี้จะระบุได้ทั้ง GeoIP และ Location Base จะผ่านเครื่องคอมพิวเตอร์ก็สามารถระบุพิกัดที่อยู่ได้ ซึ่งหากใช้ผ่าน smart phone ก็สามารถติดต่อ GPS เพื่อระบุตำแหน่งที่ตั้งได้ จะมีความแม่นยำมากขึ้น

สำหรับตรวจสอบ IP ของผู้อื่น สามารถตรวจสอบได้จากค่า Log ที่ปรากฏขึ้นบนฝั่งผู้ให้บริการ และเว็บไซต์ที่ให้บริการ ซึ่งส่วนนี้จำเป็นต้องขอให้เจ้าหน้าที่พนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นผู้ขอหมายให้ตรวจสอบค่า IP Address ที่ฝั่งผู้ให้บริการอีกครั้ง (ซึ่งจะขยายความหมายในบทที่ 11 การเรียนรู้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550)

8.3 การค้นหาประวัติข้อมูล

การค้นหาข้อมูลย้อนหลังสามารถทำได้ อย่างน้อย 2 วิธี ได้แก่

- การค้นหาจาก google caching ซึ่งในบางครั้งข้อมูลที่ลบแล้ว แต่ยังสามารถดูย้อนหลังจาก google caching ได้เช่นกัน ซึ่งได้เสนอในเทคนิคการค้นหาข้อมูลไปแล้ว

- การค้นหาประวัติข้อมูล โดยการใช้ Way back หรือ อินเทอร์เน็ตอาร์ไคฟ์ (Internet Archive) เป็นองค์กรไม่แสวงหากำไรที่เก็บข้อมูลเว็บไซต์ทั่วไปในลักษณะของห้องสมุดดิจิตัล โดยมีสำนักงานตั้งอยู่ที่ เพรซีดีโอ ในซานฟรานซิสโก สหรัฐอเมริกา โดยมีศูนย์ข้อมูลอยู่ที่ ซานฟรานซิสโก เรดวูดซิตี และเมาน์เทนวิว ข้อมูลที่เก็บไว้ได้แก่ภาพหน้าจอของเว็บไซต์ในแต่ละช่วงเวลา และข้อมูลของเว็บไซต์นั้น ที่ตั้งของ Way back คือ http://www.Archive.org เป็นเว็บไซต์ที่เก็บข้อมูลเก่าของข้อมูลและสื่อต่างๆ ที่ปรากฏบนอินเทอร์เน็ต โดยทำการรวบรวมหน้าตาเว็บไซต์ ในแต่ละช่วงเวลาตั้งแต่อดีตจนถึงปัจจุบัน และมีการรวบรวมเว็บไซต์เก็บข้อมูลให้ใช้ฟรี สำหรับนักวิจัย และนักวิชาการเพื่อค้นคว้าในด้านประวัติทางอินเทอร์เน็ต สำนักงานตั้งอยู่ที่ เมืองซานฟรานซิสโก ใน รัฐแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา ก่อตั้งโดย บรูว์สเตอร์ เคล ในปี พ.ศ. 2539

บทที่ 9

ชนิดของเครือข่ายสังคมออนไลน์

ขอบเขต

ในบทนี้กล่าวถึงประวัติความเป็นมาของเครือข่ายสังคมออนไลน์, โครงสร้างพื้นฐาน, ปัญหาที่เกิดขึ้น รวมไปถึงชนิดของเครือข่ายสังคมออนไลน์ เพื่อความเข้าใจที่ถูกต้อง

วัตถุประสงค์

1. เพื่อให้มีความรู้เกี่ยวกับชนิดของเครือข่ายสังคมออนไลน์
2. เพื่อให้ทราบสถิติการใช้งานเครือข่ายสังคมออนไลน์
3. เพื่อตระหนักถึงภัยที่อาจเกิดขึ้นจากการใช้เครือข่ายสังคมออนไลน์

เนื้อหา

1. ประวัติความเป็นมา
2. โครงสร้างของเครือข่ายสังคมออนไลน์
3. ปัญหาของเครือข่ายสังคมออนไลน์
4. ชนิดของเครือข่ายสังคมออนไลน์
5. สถิติของเครือข่ายสังคมออนไลน์

เครือข่ายสังคมออนไลน์

คือ แพลตฟอร์ม (สภาวะแวดล้อมในการทำงานร่วมกัน) หรือเว็บไซต์ที่มุ่งเน้นไปในการสร้างและสะท้อนให้เห็นถึงเครือข่าย หรือความสัมพันธ์ทางสังคม ในกลุ่มคนที่มีความสนใจ หรือมีกิจกรรมร่วมกัน บริการเครือข่ายทางสังคม จะมีองค์ประกอบหลักที่ใช้เป็นตัวแทนของผู้ใช้งาน เช่น ข้อมูลส่วนตัว, ความสัมพันธ์เชื่อมโยงระหว่างแต่ละบุคคล และบริการเสริมต่างๆ ที่มีความหลากหลายบริการเครือข่ายทางสังคมเกือบทั้งหมด จะให้บริการผ่านหน้าเว็บ และให้มีการตอบโต้กันระหว่างผู้ใช้งานผ่านทางอินเทอร์เน็ต

บริการชุมชนออนไลน์ ในบางครั้งอาจเรียกได้ว่าเป็นบริการเครือข่ายทางสังคม แต่แท้ที่จริงแล้วบริการชุมชนออนไลน์เป็นเพียงศูนย์กลางของกลุ่มที่ผู้ใช้สามารถแบ่งปันความคิดเห็น กิจกรรม และผลประโยชน์กัน"ภายในเครือข่าย" เช่น กระดานข่าว (Webboard)

เครือข่ายทางสังคมออนไลน์ส่วนมากจะใช้ประเภทของสถานที่ เช่น โรงเรียน ปีที่จบการศึกษา เพื่อนร่วมห้อง นั่นก็เพื่อใช้ในการติดต่อเพื่อนๆ และดูถึงความสัมพันธ์เชื่อมโยงทีน่าเชื่อถือได้ โดยเว็บไซต์ที่นิยมใช้วิธีเหล่านี้เช่น Facebook และ Twitter ที่ใช้กันอย่างแพร่หลายทั่วโลก, Nexopia ในแคนาดา, Bebo Vkontakte Hi5 Hyves ในประเทศเนเธอร์แลนด์ และ Friendster Mixi Multiply Orkut Wretch renren Cyworld ในเอเชียและหมู่เกาะแปซิฟิก บริการเครือข่ายทางสังคมออนไลน์เหล่านี้ มีการผลักดันเป็นอย่างมากที่จะสร้างมาตรฐานในการบริการ เพื่อหลีกเลี่ยงข้อมูลที่ซ้ำซ้อนของเพื่อนในกลุ่มและสิ่งที่สนใจนั้น ๆ

9.1 ประวัติความเป็นมา

เครือข่ายคอมพิวเตอร์ได้กำเนิดขึ้นเพื่ออำนวยความสะดวกในการติดต่อสื่อสารในรูปแบบใหม่ๆ โดยในช่วงต้นของยุคก็มีความพยายามที่จะสนับสนุนเครือข่ายทางสังคมผ่านทางคอมพิวเตอร์ โดยในช่วงนั้นก็มีอยู่หลากหลาย อาทิเช่น Usenet, ARPANET, Listserver รวมไปถึงกระดานข่าวออนไลน์ (BBS)

ต้นแบบเครือข่ายสังคมออนไลน์บนเว็บไซต์ เริ่มต้นในรูปแบบของชุมชนออนไลน์ทั่วไป เช่น Theglobal.com (1995) GeoCities (1994) และ Tripod.com (1995) และมีผู้ใช้จำนวนมากนำไปใช้ในเชิงการชักจูงผู้คนเข้ามาร่วมกันสนทนาโต้ตอบผ่านทางห้องสนทนา มีการส่งเสริมให้แสดงความคิดเห็นผ่านทางหน้าเว็บไซต์ส่วนบุคคล ใช้เป็นช่องทางในการนำเสนองาน หรืออื่น ๆ ซึ่งมีตั้งแต่เสียเงินในราคาที่ไม่สูงนัก จนถึงไม่คิดค่าใช้จ่าย ชุมชนบางชุมชนเช่น Classmate.com ได้นำเอาวิธีการที่แตกต่างออกไป โดยใช้อีเมล์ที่ผู้ใช้มี เป็นสิ่งเชื่อมโยงบุคคลเข้าหากัน และทำให้ผู้ใช้แต่ละคนมีหน้าข้อมูลส่วนตัวเป็นตัวหลักในการรวบรวมเพื่อน หรือเพื่อดึงดูดด้วยความสนใจในการมีเพื่อนร่วมกัน

เครือข่ายทางสังคมออนไลน์ยุคใหม่ได้มีการพัฒนาตัวเองขึ้นในช่วงปลายของยุค 1990 และหลายเว็บไซต์มีความพยายามที่จะพัฒนาให้ระบบมีคุณลักษณะขั้นสูงเพื่อให้สามารถค้นหาเพื่อนได้มากขึ้น และทำให้มันกลายเป็นส่วนหนึ่งของอินเทอร์เน็ต เริ่มด้วย Friendster ตามมาด้วย MySpace และ Linkedin ในช่วงท้าย เครือข่ายทางสังคมมีความนิยมสูงขึ้นเรื่อยๆ และเป็นไปอย่างรวดเร็วในปี 2005 โดย MySpace ได้รายงานว่ามีการเปิดหน้าเว็บในแต่ละหน้า มากกว่า Google ในขณะนั้น

ส่วน Facebook ได้เปิดตัวขึ้นในปี 2004 แต่ ณ ขณะนี้ได้กลายมาเป็นเว็บไซต์เครือข่ายสังคมที่มีขนาดใหญ่ที่สุดในโลก และ ณ ปัจจุบัน มีเว็บไซต์ที่เกี่ยวกับเครือข่ายทางสังคมออนไลน์มากกว่า 200 เว็บไซต์ อีกทั้งยังมีความหลากหลายมากขึ้นด้วย

Facebook และเครื่องมืออื่นๆ ที่มากขึ้นกำลังเป็นเป้าหมายของการวิจัยทางวิชาการ นักวิชาการต่างๆ เริ่มเข้ามาตรวจสอบเว็บไซต์เครือข่ายทางสังคมถึงผลกระทบจากวิธีการเล่น ซึ่งอาจเป็นปัญหาต่อตัวตน ความเป็นส่วนตัว สังคม วัฒนธรรม และการศึกษา รวมไปถึงพลังของเครือข่ายทางสังคมที่มีผลเป็นอย่างมาก

9.2 โครงสร้างของเครือข่ายสังคมออนไลน์

เว็บไซต์เครือข่ายทางสังคมจะต้องมีความสามารถในการแบ่งปันข้อมูล โดยส่วนใหญ่ ผู้ใช้แต่ละคนจะมีหน้าข้อมูลส่วนตัวที่ถูกสร้างขึ้นและมีข้อมูลต่างๆ ที่เกี่ยวกับตัวเอง ผู้ใช้งานสามารถอัพโหลดภาพของตัวเอง โพสต์ข้อมูลลงในบล็อกเพื่อให้ผู้อื่นมาอ่าน นอกจากนี้อาจมีส่วนให้แสดงความคิดเห็นจากเพื่อนหรือคนอื่นๆ ด้วยในมุมมองของการปกป้องความเป็นส่วนตัวของผู้ใช้ จะต้องมีตัวควบคุมการเข้าถึงจากบุคคลทั่วไปที่จะต้องการเข้ามาดูในหน้าข้อมูลส่วนตัว

อีกทั้งในปี 2010 ยังได้กลายเป็นเรื่องปกติที่องค์กรต่างๆ ได้เข้ามาเพื่อสร้างรูปแบบการโฆษณาสินค้าหรือบริการในรูปแบบใหม่ด้วย

คุณสมบัติอื่นๆ

บางเครือข่ายทางชุมชน อาจมีการสร้างความสามารถเพิ่มเติมเช่น กลุ่ม เพื่อร่วมแบ่งปันสิ่งที่สนใจร่วมกัน นอกจากนี้ยังมีแนวโน้มมากขึ้นที่เครือข่ายทางสังคมจะสามารถทำงานร่วมกันผ่านทางเทคโนโลยี OpenID และ OpenSocial

เมื่อเร็วๆ นี้เครือข่ายสังคมมือถือกลายเป็นที่นิยม ในชุมชนมือถือส่วนใหญ่ผู้ใช้โทรศัพท์มือถือขณะนี้คุณสามารถสร้างโปรไฟล์ของตัวเองให้เพื่อนๆ มีส่วนร่วมในห้องสนทนา แบ่งปันภาพถ่ายวิดีโอและ บล็อกร่วมกันโดยใช้โทรศัพท์มือถือของตน

9.3 ปัญหาของเครือข่ายสังคมออนไลน์

ถึงแม้เครือข่ายทางสังคมจะมีประโยชน์ในการสร้างความสัมพันธ์ แต่ก็ยังมีอีกด้านที่สร้างปัญหาได้ไม่น้อย เช่น ปัญหาความเป็นส่วนตัว เครือข่ายทางสังคมมีการเจริญเติบโตมากขึ้น ความกังวลเกี่ยวกับผู้ใช้จำนวนเกินไป ข้อมูลส่วนบุคคลและภัยคุกคามทางเพศ ผู้ใช้บริการเหล่านี้ยังต้องมีการตระหนักถึง การโจรกรรมข้อมูล หรือไวรัสอีกด้วย นั่นอาจรวมไปถึงการใช้ที่ผิดประเภท ความเสี่ยงสำหรับความปลอดภัยของเด็ก การกลั่นแกล้ง หรืออาจนำไปถึงความเสียหายทางธุรกิจและสิทธิบัตรต่างๆ

พบว่าประเทศไทยที่มีเกิดภัยคุกคามจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) มากที่สุดคือมาจากประเทศอเมริกา พบว่า ได้รับข้อมูลขยะถึง 16.37 %

ข้อมูลที่มาจากโปรแกรมอันไม่พึงประสงค์ 39.39%

และที่น่าสนใจคือ ภัยคุกคามที่ไม่สามารถแยกแยะประเทศได้

เป็นข้อมูลขยะถึง 22.30%

เป็นข้อมูลจากโปรแกรมไม่พึ่งประสงค์ Malware ถึง 20.03%

9.4 ชนิดของเครือข่ายสังคมออนไลน์

บริการเครือข่ายสังคม (Social Network Service) คือ เป็นรูปแบบของเว็บไซต์ ในการสร้างเครือข่ายสังคม สำหรับผู้ใช้งานในอินเทอร์เน็ต เขียนและอธิบายความสนใจ และกิจการที่ได้ทำ และเชื่อมโยงกับความสนใจและกิจกรรมของผู้อื่น ในบริการเครือข่ายสังคมมักจะประกอบไปด้วย การแชท ส่งข้อความ ส่งอีเมล์ วิดีโอ เพลง อัพโหลดรูป บล็อก การทำงานคือคอมพิวเตอร์เก็บข้อมูลพวกนี้ไว้ในรูปฐานข้อมูล sql ส่วน video หรือ รูปภาพ อาจเก็บเป็น ไฟล์ก็ได้ บริการเครือข่ายสังคมที่เป็นที่นิยมได้แก่ Hi5 ไฮไฟว์ , Myspace มายสเปซ , Facebook เฟซบุ๊ก , Multiply มัลติพลาย , Youtube โดยเว็บไซต์เหล่านี้มีผู้ใช้มากมาย เช่น เฟสบุ๊คเป็นเว็บไซต์ที่คนไทยใช้มากที่สุดซึ่งจะแยกเครือข่ายสังคมออนไลน์ (Social Network) ออกได้เป็นกลุ่ม 7 ดังนี้

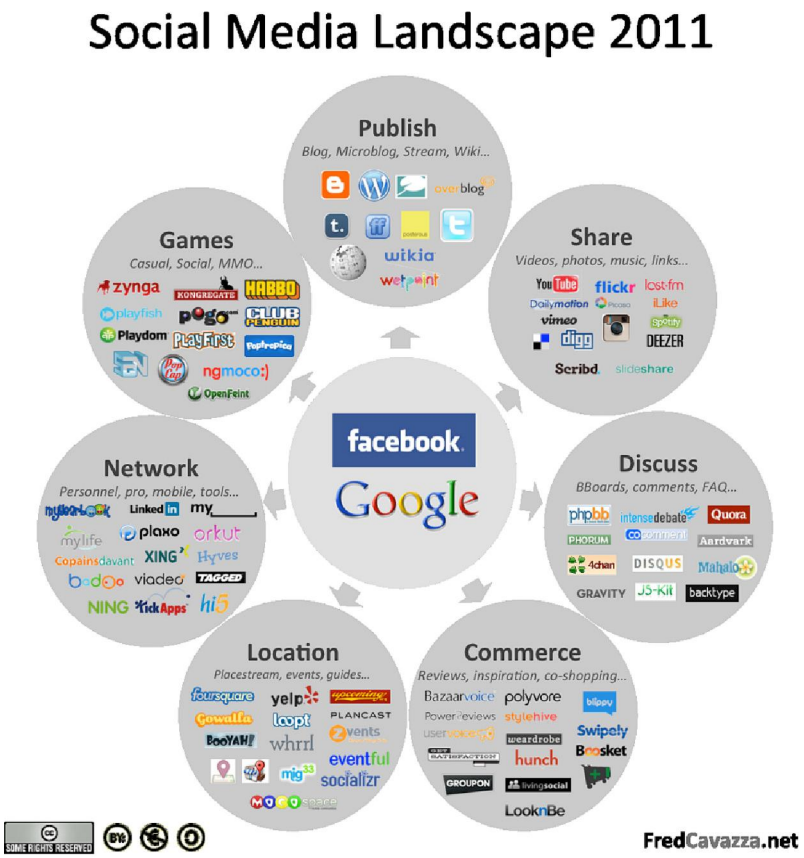
1. Publish การเผยแพร่ข้อมูล เอกสาร หรือบทความ
2. Share การแบ่งปันข้อมูล รูปภาพหรือความรู้
3. Discuss สังคมในการระดมความคิด

4. Commerce เครือข่ายสังคมที่เกี่ยวกับธุรกิจ

5. Location การแบ่งปันสถานที่ที่น่าสนใจ

6. Network เครือข่ายเพื่อน ธุรกิจ งาน

7. Game เครือข่ายของเกมส์



ภาพที่ 9.1 แสดงถึงกลุ่มของเครือข่ายสังคมออนไลน์

9.5 สถิติของเครือข่ายสังคมออนไลน์

สถิติจาก Markingcharts.com ในเดือนธันวาคม 2553 ที่ผ่านมา พบว่าสถิติอัตราการใช้งานเครือข่ายสังคมออนไลน์ ที่คนนิยมใช้มากที่สุดคือ Facebook รองลงมาคือ Youtube และ Myspace ตามลำดับ และข้อมูลที่น่าสนใจคือ ผู้หญิง มีสัดส่วนการเล่น Social Network มากกว่าผู้ชาย

ในปัจจุบันจำนวนผู้ใช้งาน Facebook สูงถึง 600 ล้านคน ซึ่งหากนับเป็นประเทศก็ใหญ่เป็นอันดับ 3 ของโลก และมีแนวโน้มที่จะขยายตัวผู้ใช้งานมากเป็นอัตราสูงขึ้นอยู่ทุกปี โดยสถิติอันดับประเทศที่ใช้ Facebook มากที่สุด 5 อันดับแรก ประเทศสหรัฐอเมริกามีผู้ใช้ Facebook เป็นอันดับหนึ่ง ประเทศอินโดเนียเซียเป็นอันดับสอง ประเทศอังกฤษเป็นอันดับสาม ประเทศตุรกีเป็นอันดับสี่ และประเทศฟิลิปินเป็นอันดับห้า ส่วนประเทศไทยอยู่อันดับที่ 19 ของโลก มีจำนวนผู้ใช้งานถึง 8.2 ล้านคนถ้าเทียบเป็นสถิติจำนวนบัญชี Facebook ของประเทศไทยมีอัตราจำนวนผู้ใช้งานสูงขึ้นทุกเดือนนับว่าเป็นเครือข่ายสังคมออนไลน์ (social network) ที่นิยมมากที่สุดในประเทศไทย

ผู้ใช้งาน Facebook ในประเทศไทย ส่วนใหญ่อายุอยู่ระหว่าง 18-24 ปี คิดเป็นเปอร์เซ็นต์ทั้งหมดของผู้ใช้งานถึง 40% ผู้หญิงมากกว่าผู้ชาย ซึ่งคิดเป็นจำนวนผู้หญิงที่ใช้ Facebook ถึง 46%

Facebook ถือได้ว่าเป็นเส้นทางใหม่สำหรับโลกการสื่อสาร เนื่องจากสถิติข้อมูลที่ได้จาก Facebook จะสามารถทราบถึงพฤติกรรมของผู้ใช้งานมากขึ้น ซึ่งด้วยเหตุนี้เองทำให้ Facebook มีมูลค่าสูงขึ้นและคิดว่าอาจเกิน google ในไม่ช้านี้ ด้วยความที่ Facebook มีผู้ใช้งานจำนวนมาก และหากผู้ขายสินค้าต่างๆ อาศัยช่องทาง Facebook ก็จะสามารถเข้าถึงผู้ใช้งานได้ตรงขึ้น ขายสินค้าได้ตรงกลุ่มเป้าหมายมากขึ้น และพฤติกรรมแต่ละคนมากขึ้น จะเห็นว่าในระยะหลัง หลายบริษัทเริ่มใช้ช่องทาง Social network ในการทำการตลาดมากขึ้น เป็นต้น

ส่วนในแง่ด้านความมั่นคง โดยเฉพาะการใช้ข้อมูลส่วนบุคคลจะกลายเป็นปัญหาใหญ่สำหรับ เครือข่ายสังคมออนไลน์มากขึ้น ซึ่งจากกล่าวในบทต่อไป

บทที่ 10

การรักษาความลับและความมั่นคงจากเครือข่ายสังคมออนไลน์

ขอบเขต

ในบทนี้กล่าวถึงวิธีการรักษาความลับความมั่นคง และรวมไปถึงความเป็นส่วนตัวจากการใช้เครือข่ายสังคมออนไลน์ ได้ทดลองปฏิบัติกับการใช้งานจริง และเรียนรู้ถึงการป้องกันอย่างเหมาะสมอย่างยืดหยุ่นกับตัวเอง

วัตถุประสงค์

มีความรู้และความเข้าใจถึงภัยคุกคามที่เกิดขึ้นจากการใช้เครือข่ายสังคมออนไลน์ และสามารถแนะนำให้ผู้อื่นป้องกันข้อมูลและความมั่นคงปลอดภัยจากการใช้ข้อมูลเครือข่ายสังคมออนไลน์ ซึ่งประกอบด้วย 2 ส่วนได้แก่

1.การตั้งค่าความเป็นส่วนตัว Facebook

2.การตั้งค่าความเป็นส่วนตัว Twitter

เนื้อหา

1. ประวัติความเป็นมาของ Twitter และ Facebook
2. การตั้งค่าความเป็นส่วนตัว Twitter
3. การตั้งค่าความเป็นส่วนตัว Facebook

10.1 ประวัติความเป็นมาของ Twitter และ Facebook

ทวิตเตอร์ (Twitter) เป็นบริการเครือข่ายสังคมออนไลน์จำพวกไมโครบล็อก โดยผู้ใช้สามารถส่งข้อความยาวไม่เกิน 140 ตัวอักษร ว่าตัวเองกำลังทำอะไรอยู่ หรือ ทวีต (tweet - เสียงนกร้อง) ทวิตเตอร์ก่อตั้งโดยบริษัท Obvious Corp เมื่อเดือนมีนาคม ค.ศ. 2006 ที่ซานฟรานซิสโก สหรัฐอเมริกา

ข้อความอัพเดตที่ส่งเข้าไปยังทวิตเตอร์จะแสดงอยู่บนเว็บเพจของผู้ใช้คนนั้นบนเว็บไซต์ และผู้ใช้คนอื่นสามารถเลือกรับข้อความเหล่านี้ทางเว็บไซต์ทวิตเตอร์, อีเมล์, เอสเอ็มเอส (SMS), เมสเซนเจอร์ (IM), RSS, หรือผ่านโปรแกรมเฉพาะอย่าง Twitterific Twhirl ปัจจุบันทวิตเตอร์มีหมายเลขโทรศัพท์สำหรับส่งเอสเอ็มเอส (SMS)ใน 3 ประเทศ คือ สหรัฐอเมริกา แคนาดา และสหราชอาณาจักร

ความสำเร็จของทวิตเตอร์ส่งผลให้มีบริการคล้ายคลึงกันออกมาเป็นจำนวนมาก ปัจจุบันประเทศไทยเองก็มีบริการลักษณะนี้เช่นกัน นั่นคือ Noknok และ Kapook OnAir เว็บไซต์แห่งหนึ่งถึงกับรวบรวมบริการแบบเดียวกับ ทวิตเตอร์ได้ถึง 111 แห่ง

ค.ศ. 2009 ทวิตเตอร์ได้รับความนิยมสูงขึ้นอย่างมาก จนนิตยสารไทม์ฉบับวันที่ 15 มิ.ย. 2009 ได้นำเอาทวิตเตอร์ขึ้นปก เป็นเรื่องเด่นประจำฉบับ และบทบรรณาธิการกล่าวถึงการเปลี่ยนแปลงการนำเสนอข่าวที่มีมาจากเทคโนโลยีใหม่อย่างทวิตเตอร์

ภาพที่ 10.1 สัญลักษณ์ Twitter

เฟซบุ๊ก (Facebook) เป็นบริการเครือข่ายสังคมและเว็บไซต์เปิดใช้งานเมื่อ 4 กุมภาพันธ์ ค.ศ. 2004 ดำเนินงานและมีเจ้าของคือ บริษัท เฟซบุ๊ก (Facebook, Inc.) จากข้อมูลเดือนกรกฎาคม ค.ศ. 2010 เฟซบุ๊กมีผู้ใช้ประจำ 500 ล้านบัญชี ผู้ใช้สามารถสร้างข้อมูลส่วนตัว เพิ่มรายชื่อผู้ใช้อื่นในฐานะเพื่อน และแลกเปลี่ยนข้อความ รวมถึงได้รับแจ้งโดยทันทีเมื่อพวกเขาปรับปรุงข้อมูลส่วนตัว นอกจากนั้นผู้ใช้ยังสามารถร่วมกลุ่มความสนใจส่วนตัว จัดระบบตาม สถานที่ทำงาน โรงเรียน มหาวิทยาลัย หรืออื่นๆ ชื่อของเฟซบุ๊กนั้นมาจากชื่อเรียกภาษาพูดของสมุดที่ให้กับนักเรียนเมื่อ เริ่มแรกเรียนในสถาบันอุดมศึกษา ที่มอบให้โดยคณะบริหารมหาวิทยาลัยในสหรัฐอเมริกา เพื่อช่วยให้นักเรียนสามารถรู้จักผู้อื่นได้ดีมากขึ้น เฟซบุ๊กอนุญาตให้ใครก็ได้เข้าสมัครลงทะเบียนกับเฟซบุ๊ก โดยต้องมีอายุมากกว่า 13 ปีขึ้นไป เฟซบุ๊กก่อตั้งขึ้นโดย มาร์ก ซักเคอร์เบิร์ก ร่วมกับเพื่อนร่วมห้องในวิทยาลัยของเขา และเป็นนักเรียนวิทยาศาสตร์ คอมพิวเตอร์ที่ชื่อ เอ็ดวาร์โด ซาเวริน, ดิสติน มอสโควิตซ์ และคริส ฮิวส์ เดิมทีสมาชิกของเว็บไซต์จะจำกัดเฉพาะกลุ่มผู้ก่อตั้งและนักเรียนมหาวิทยาลัยฮาวาร์ด แต่ต่อมาขยับขยายไปสู่มหาวิทยาลัยอื่นในแถบบอสตัน, กลุ่มไอวีลีก, และมหาวิทยาลัยสแตนฟอร์ด แล้วค่อยๆ เพิ่มนักเรียนจากมหาวิทยาลัยอื่น จนกระทั่งเปิดให้กับนักเรียนระดับไฮสคูล จนในที่สุดทุกคนก็สามารถเข้าสมัครได้โดยอายุมากกว่า 13 ปีขึ้นไป

สำหรับติดต่อแลกข้อมูลข่าวสาร เปิดใช้งานเมื่อ 4 กุมภาพันธ์ พ.ศ. 2547 โดย มาร์ก ซักเคอร์เบิร์ก นักศึกษาจากมหาวิทยาลัยฮาร์เวิร์ด ในช่วงแรกนั้นเฟซบุ๊กเปิดให้ใช้งานเฉพาะนักศึกษามหาวิทยาลัยฮาร์เวิร์ด ซึ่งต่อมาได้ขยายตัวออกไป

สำหรับมหาวิทยาลัยทั่วสหรัฐอเมริกา และตั้งแต่ 11 กันยายน พ.ศ. 2549 ได้ขยายมาสำหรับผู้ใช้ทั่วไปทุกคนเหมือนในปัจจุบัน

จากการศึกษาของเว็บ คอมพีต.คอม ในเดือนมกราคม ค.ศ. 2009 เฟซบุ๊กถือเป็นบริการเครือข่ายสังคมที่มีคนใช้มากที่สุด เมื่อดูจากผู้ใช้ประจำรายเดือน รองลงมาคือ มายสเปซ เอ็นเตอร์เทนเมนต์วีกลี ให้อยู่ในรายชื่อ สิ่งที่ดีที่สุดในสิ้นทศวรรษและควอนต์แคสต์ ประเมินว่า เฟซบุ๊ก มีผู้ใช้ต่อเดือนราว 135.1 ล้านคน นับเฉพาะในสหรัฐอเมริกา

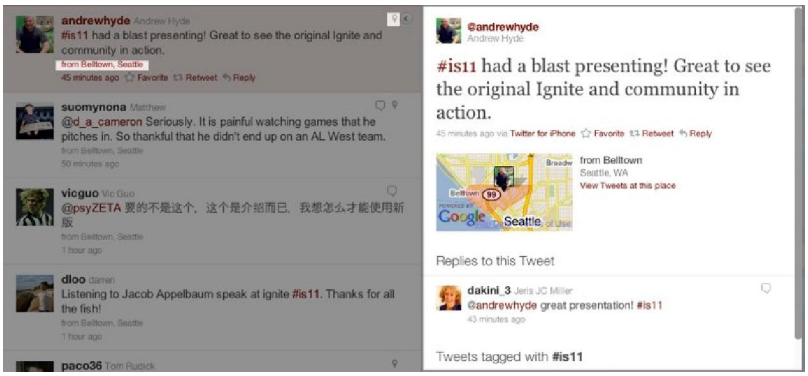
ภาพที่ 10.2 ผู้ก่อตั้งเว็บไซต์ Facebook มาร์ก ซักเคอร์เบิร์ก

วิธีรักษาความลับและความมั่นคงจากเครือข่ายสังคมออนไลน์

10.2 การตั้งค่าความเป็นส่วนตัว Twitter

Tweet Location คือคุณลักษณะในการบอกตำแหน่งที่อยู่ไปยังข้อความที่ Tweet แต่ละข้อความ โดยคุณลักษณะนี้จะตั้งไว้ที่ “ปิด” ซึ่งหากจะใช้งานต้องไปทำการเปิดใช้เสียก่อนโดยเมื่อเลือกใช้แล้วนั้น จะสามารถเพิ่มข้อมูลที่ตั้งของผู้ใช้ไปยังบุคคล, Tweets ใหม่ใน Twitter.com และผ่านทางโปรแกรมประยุกต์อื่นๆ โทรศัพท์มือถือที่สนับสนุนคุณสมบัตินี้ หรือข้อมูลสถานที่สาธารณะที่ใช้ร่วมกันจะเป็นได้ทั้งตำแหน่งที่แน่นอนของผู้ใช้ หรือสถานที่ของผู้ใช้ (เช่นเดียวกับพื้นที่ใกล้เคียงหรือเมือง) เพื่อช่วยเพิ่มบริบทในการสนทนา

ยกตัวอย่าง เช่น @andrewhyde ต้องการให้รู้ว่าเขามีงานนำเสนอในบริเวณ Belltown, Seattle เป็นต้น



ภาพที่ 10.3 ตัวอย่างการใช้ Tweet Location

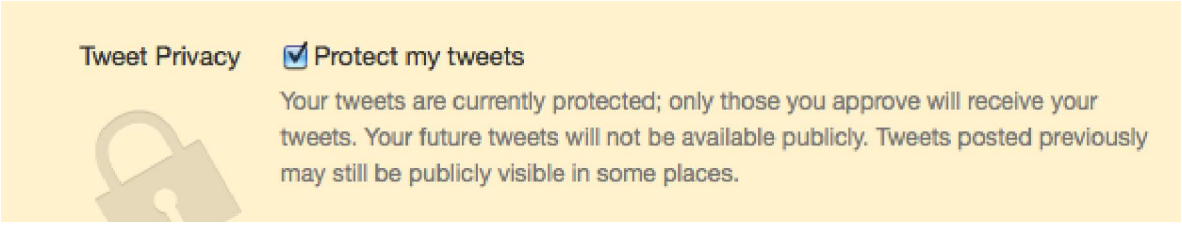
เมื่อเปิดใช้งาน Tweet Location แล้ว ต้องสามารถควบคุมวิธีการและข้อมูลที่ตั้งของผู้ใช้ ต้องระวังและรอบคอบเกี่ยวกับปริมาณของข้อมูลที่แบ่งปัน โปรดจำไว้ว่าเมื่อเลือกที่จะ Tweet กับตำแหน่งของผู้ใช้ ผู้ใช้ยังสามารถเลือกที่จะไม่ใช้ตำแหน่งของผู้ใช้สำหรับ Tweets

เมื่อการเปิดเผยตำแหน่ง อาจไม่เป็นเรื่องที่น่าเปิดเผยอีกต่อไป Twitter จึงทำระบบ ลบข้อมูลตำแหน่งที่ผ่านมาทั้งหมดได้ด้วยคลิกเดียว โดยในส่วนกำหนดค่า Tweet Location ให้ทำการปิดการใช้งาน และหากต้องการลบข้อมูลตำแหน่งที่ผ่านมา ให้ Click ที่ “delete all location information” ซึ่งในกระบวนการนี้ อาจใช้เวลานานกว่า 30 นาที

Tweet Privacy หรือความเป็นส่วนตัวในการ Tweet

เมื่อลงทะเบียน Twitter ในครั้งแรก Twitter จะตั้งตัวเลือกของการรักษาข้อมูลสาธารณะของบัญชี (การตั้งค่าบัญชีค่าเริ่มต้น) หรือการป้องกันบัญชีเป็นแบบ สาธารณะ นั่นหมายความว่า ไม่ว่าใครก็ได้ สามารถที่จะเห็นความเคลื่อนไหวข้อความ ที่ได้ Tweet ไป แม้จะไม่ได้เป็นสมาชิก Twitter ก็ตาม

คุณสมบัติการปกป้องข้อมูลส่วนตัว สามารถทำได้โดย เข้าไปในส่วนของ “การตั้งค่าบัญชี” และเปิดการใช้งาน “Tweet Privacy” หลังจากนั้นให้ทำการบันทึก (“Save”)



ภาพที่ 10.4 แสดงการตั้งค่าความเป็นส่วนตัวของ Twitter

หลังจากตั้งค่าสิ่งที่เกิดขึ้นมีดังนี้ บุคคลที่ต้องการติดตามข้อมูลต้องได้รับการยอมรับหรือเห็นชอบเสียก่อน (Approve) เพราะฉะนั้นข้อมูลทั้งหมด จะเห็นหรือเข้าถึงได้เฉพาะบุคคลที่ผ่านการยอมรับแล้วเท่านั้น

HTTPS

Twitter ได้เล็งเห็นถึงความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูล จึงได้เปิดให้มีการใช้งานระบบเข้ารหัสเพื่อเพิ่มการรักษาความปลอดภัยของบัญชีที่ดีกว่า ป้องกันจากการดักข้อมูล ถ้าใช้ Twitter ผ่านการเชื่อมต่ออินเทอร์เน็ตที่ไม่มีหลักประกันด้านความปลอดภัยเช่นเครือข่าย WiFi สาธารณะ Twitter จะใช้ HTTPS ในการป้องกันรหัสผ่านเมื่อผู้ใช้เข้าสู่ระบบสามารถทำได้โดย เข้าไปในส่วนของ “การตั้งค่าบัญชี” และเปิดการใช้งาน “HTTPS Only” หลังจากนั้นให้ทำการบันทึก (“Save”)

การรักษาความปลอดภัยของ Facebook

ตามเอกสาร “คำแถลงของสิทธิและความรับผิดชอบ” และ “การตั้งค่าความเป็นส่วนตัว” ของ Facebook ในปี ค.ศ.2010 ที่กล่าวถึงสิทธิและความรับผิดชอบต่างๆ ที่มาจากหลักการของ Facebook และกำหนดความสัมพันธ์ของเรากับผู้ใช้และคนอื่นๆ ที่มีปฏิสัมพันธ์กับ Facebook โดยการใช้หรือการเข้าถึง Facebook

โดยการใช้งาน Facebook นั้น จะต้องเป็นไปตามข้อตกลงต่างๆ ดังนี้

- ไม่ส่งหรือโพสต์การสื่อสารในเชิงพาณิชย์ไม่ได้รับอนุญาต (เช่นขยะ) ใน Facebook
- ไม่ได้อัพโหลดไวรัสหรือรหัสที่เป็นอันตรายอื่นๆ
- ไม่เรียกร้องหรือการเข้าถึงข้อมูลการเข้าสู่ระบบบัญชีที่เป็นของคนอื่น
- ไม่พาล, ข่มขู่, หรือก่อกวนผู้ใช้ใดๆ
- ไม่โพสต์เนื้อหาที่ แสดงความเกลียดชังข่มขู่หรือลามกอนาจาร ความรุนแรง หรือมีภาพเปลือย
- ไม่ใช้ Facebook ทำอะไรผิดกฎหมายทำให้เข้าใจผิดที่เป็นอันตรายหรือเลือกปฏิบัติ
- ไม่ทำอะไรที่สามารถปิดการใช้งานสร้างภาระหนักหรือทำให้เสียการทำงานที่เหมาะสมของ Facebook, เช่นการปฏิเสธการโจมตีบริการ
- ไม่ใช้ Facebook หากผู้ใช้มีอายุไม่เกิน 13 ปี
- ไม่ใช้ Facebook ไปในทางกระทำผิดทางเพศ
- ไม่เปิดเผยรหัสผ่าน, (หรือในกรณีของนักพัฒนา, รหัสลับของผู้ใช้) ให้คนอื่นเข้าถึงบัญชีหรือทำอะไรอื่นที่อาจเป็นอันตรายต่อความปลอดภัยของบัญชี
- ไม่โพสต์เนื้อหาหรือดำเนินการใด ๆ ใน Facebook ที่เป็นการละเมิดหรือฝ่าฝืนสิทธิของผู้อื่นหรือผิดกฎหมาย

10.3 การตั้งค่าความเป็นส่วนตัว Facebook

ในส่วนของความเป็นส่วนตัว Facebook ได้เล็งเห็นถึงความสำคัญเป็นอย่างสูง จึงได้ออกแบบระบบ ให้มีการใช้ “นโยบายข้อมูลส่วนบุคคล” เพื่อให้การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับวิธีการที่ผู้ใช้สามารถใช้ Facebook เพื่อแบ่งปันกับคนอื่นๆ และวิธีการที่เราจะเก็บและสามารถใช้ข้อมูลเป็นไปตามที่ผู้ใช้ต้องการ

นโยบายความเป็นส่วนตัว ถูกออกแบบมาเพื่อช่วยให้ผู้ใช้เข้าใจวิธีการที่เรารวบรวมและใช้ข้อมูล สามารถเข้าถึงโดยไปที่ “บัญชีผู้ใช้” บริเวณด้านบนขวา และเลือก “ตั้งค่าความเป็นส่วนตัว”

ในการตั้งค่าต่างๆ สามารถที่จะเลือกเพื่อควบคุมแอพพลิเคชั่น และคนอื่นๆ ที่สามารถเห็นข้อมูลส่วนตัวได้ รวมไปถึงการใช้ข้อมูลร่วมกันระหว่างเพื่อน และกลุ่มเพื่อนทุกคน โดยสามารถปรับแต่งการตั้งค่าทั้งหมดได้ โดยการปรับแต่งจะถูกแบ่งออกเป็น 4 ส่วนใหญ่ๆ ดังนี้

1. การแบ่งปันบน Facebook

เป็นส่วนที่จะควบคุมการเข้าถึงเนื้อหาทั้งหมดที่ได้ทำการโพสต์ (เช่นการปรับปรุงสถานะ, ภาพถ่ายและวิดีโอ) นอกจากนี้ยังมีเรื่องของข้อมูลส่วนตัวที่จะเปิดเผย (วันเกิดและข้อมูลที่ติดต่อ) และข้อมูลที่คนอื่นมาแบ่งปันข้อมูลกับผู้ใช้ (แสดงความเห็นในบทความและภาพถ่ายและวิดีโอที่ผู้ใช้ได้รับการติดแท็ก) โดยสามารถเลือกได้ภายในการคลิกเพียงครั้งเดียว แต่ขอแนะนำให้ใช้การปรับแต่งค่าอย่างเหมาะสมเพื่อให้สามารถควบคุมระดับความเป็นส่วนตัวอย่างเหมาะสมที่สุด

2. การเชื่อมต่อบน Facebook

เป็นส่วนที่จะกำหนดถึงข้อมูลที่บุคคลอื่น สามารถใช้ค้นหาตัวเรา (ชื่อ, รูป, ภาพโปรไฟล์, เพศ) นี้เป็นสิ่งที่จะช่วยให้ผู้ใช้เชื่อมต่อกับเพื่อน และครอบครัวของผู้ใช้ข้อมูลอื่นๆ ในส่วนนี้รวมไปถึงกิจกรรม, บ้านเกิดและประสบการณ์ เปิดให้ทุกคนโดยเริ่มต้นจะช่วยให้ติดต่อกับเพื่อนและได้รับประโยชน์สูงสุด

3. แอพพลิเคชั่นและเว็บไซต์

ส่วนนี้จะควบคุมข้อมูลที่จะใช้ร่วมกันกับแอพพลิเคชั่นและเว็บไซต์รวมถึงเครื่องมือค้นหา (แอพพลิเคชั่นและเว็บไซต์ที่ผู้ใช้ และเพื่อนของผู้ใช้ใช้อยู่แล้วมีสิทธิ์เข้าถึง ชื่อของผู้ใช้, รูปภาพโปรไฟล์, เพศ, เครือข่ายรายชื่อเพื่อน, ID ผู้ใช้, ชื่อผู้ใช้และข้อมูลอื่นๆ กับทุกคน) สามารถดูรายการแอพพลิเคชั่น หรือปิดแพลตฟอร์มที่ไม่ต้องการ (การปิดแพลตฟอร์มหมายความว่าผู้ใช้จะไม่สามารถใช้งานแอพพลิเคชั่นแพลตฟอร์มใดๆ หรือเว็บไซต์และจะไม่เปิดเผยข้อมูล)

4. รายชื่อที่ถูกบล็อก

ส่วนนี้จะช่วยให้สามารถปิดกั้นคนอื่นๆ จากการติดต่อหรือโต้ตอบกันหรือดูข้อมูลใน Facebook สามารถระบุเพื่อนที่จะไม่สนใจคำเชิญจากแอพพลิเคชั่น และดูรายชื่อของแอพพลิเคชั่นที่เฉพาะเจาะจงว่าได้ถูกปิดกั้นจากการเข้าถึงข้อมูล และการติดต่อ

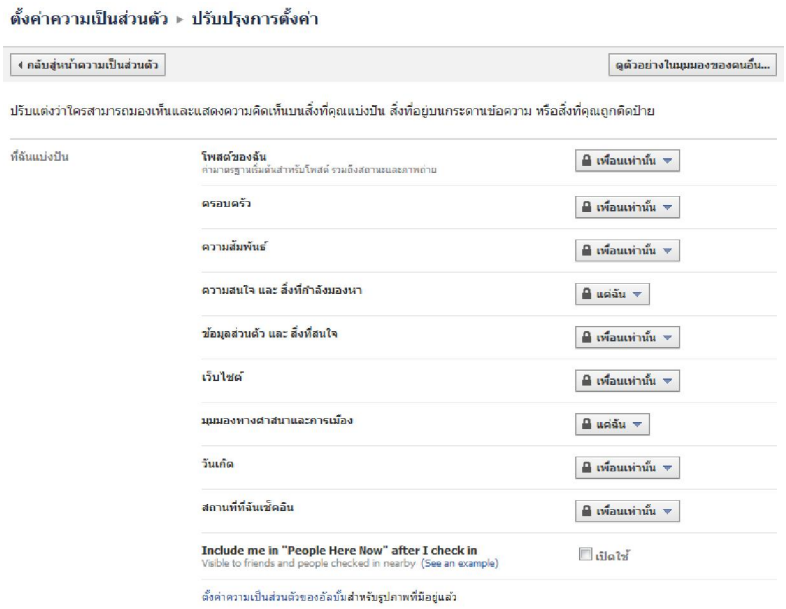
การตั้งค่าความเป็นส่วนตัว

การ “ปรับปรุงการตั้งค่า” อย่างเหมาะสม เป็นทางเลือกที่ดีเพื่อให้สามารถควบคุมระดับความเป็นส่วนตัวอย่างเหมาะสมที่สุดในส่วนนี้สามารถปรับแต่งว่าใครสามารถมองเห็นและแสดงความคิดเห็นบนสิ่งที่ผู้ใช้แบ่งปัน สิ่งที่อยู่บนกระดานข้อความ หรือสิ่งที่ผู้ใช้ถูกติดป้าย ซึ่งเราสามารถแบ่งออกได้เป็น 3 ส่วนคือ

ส่วนที่ 1 เกี่ยวข้องกับข้อมูลส่วนตัวที่สามารถแบ่งปันให้ผู้อื่นเห็นได้

ที่แบ่งปัน คือ ข้อมูลส่วนตัวของผู้ใช้งานต่างๆ ที่จะเปิดเผยสามารถควบคุมระดับความเป็นส่วนตัวได้ตามหัวข้อต่อไปนี้ๆ

- โพสต์ของฉัน - ตั้งค่ามาตรฐานเริ่มต้นสำหรับข้อความเผยแพร่รวมถึงสถานะและภาพถ่าย
- ครอบครัว – กำหนดระดับการมองเห็นรายชื่อคนในครอบครัว
- ความสัมพันธ์ – เช่น โสด, กำลังคบหา, หมั้น, แต่งงาน ฯลฯ
- ความสนใจ และ สิ่งที่กำลังมองหา
- ข้อมูลส่วนตัว และ สิ่งที่สนใจ
- เว็บไซต์
- มุมมองทางศาสนาและการเมือง
- วันเกิด – ในส่วนนี้ จะแสดงมาก แสดงน้อย อยู่ในส่วนของ “ข้อมูลเบื้องต้น” ของแต่ละคนด้วย ว่ากำหนดไว้แบบใด
- สถานที่ที่ฉันเช็คอิน
- Include me in "People Here Now" after I check in –เป็นหน้าที่บอกว่าตอนนี้ มีใครอยู่ในบริเวณที่อยู่ โดยให้เพิ่มเราเข้าไปในรายการพื้นที่นั้นๆ ด้วย
- ตั้งค่าความเป็นส่วนตัวของอัลบั้มสำหรับรูปภาพที่มีอยู่แล้ว

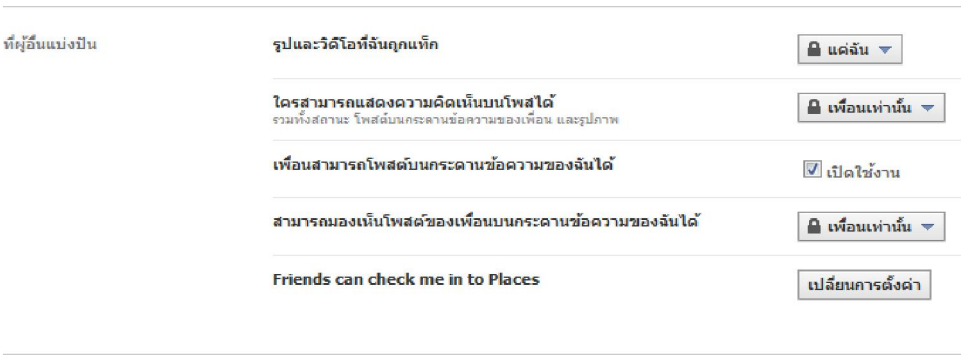


ภาพที่ 10.5 แสดงหน้าจอการตั้งค่า “ที่ฉันแบ่งปัน”

ส่วนที่ 2 เกี่ยวข้องกับข้อมูลที่ผู้อื่นสามารถแบ่งปันให้กับตัวผู้ใช้งาน ผ่านทางกระดานข้อความการปรับแต่งจะแบ่งออกเป็นส่วนต่างๆ ดังต่อไปนี้

ส่วนที่ผู้อื่นแบ่งปัน คือส่วนที่ผู้อื่นสามารถแบ่งปันให้กับตัวผู้ใช้งาน ผ่านทางกระดานข้อความของผู้ใช้งาน

- รูปและวิดีโอที่ฉันถูกแท็ก – ตั้งระดับให้ผู้ใช้งานในระดับใดๆ สามารถติดป้ายอ้างอิงถึง
- ใครสามารถแสดงความคิดเห็นบนโพสต์ ได้
- เพื่อนสามารถโพสต์ บนกระดานข้อความของฉันได้
- สามารถมองเห็นโพสต์ของเพื่อนบนกระดานข้อความของฉันได้
- เพื่อนสามารถเช็คอินฉันใน Places

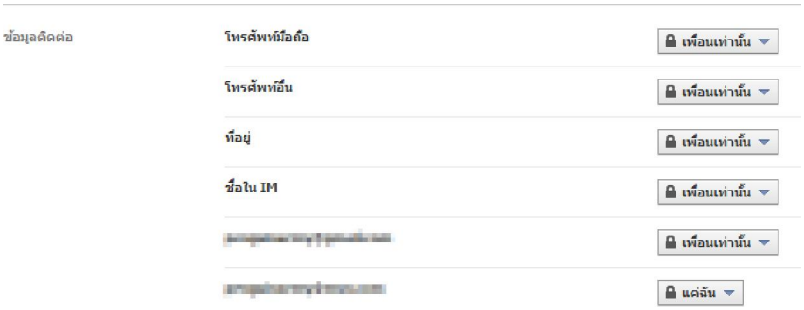


ภาพที่ 10.6 แสดงหน้าจอการตั้งค่า “ที่ผู้อื่นแบ่งปัน”

ส่วนที่ 3 เกี่ยวข้องกับข้อมูลส่วนตัวที่ใช้ในการติดต่อภายนอกการปรับแต่งจะแบ่งออกเป็นส่วนต่างๆ ดังต่อไปนี้

ข้อมูลติดต่อ คือข้อมูลส่วนตัวที่ใช้ในการติดต่อในช่องทางต่างๆ

- โทรศัพท์มือถือ
- โทรศัพท์บ้าน
- ที่อยู่
- ชื่อใน IM
- อีเมล์



ภาพที่ 10.7 แสดงหน้าจอการตั้งค่า “ข้อมูลติดต่อ”

บทที่ 11

การเรียนรู้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ขอบเขต

ในบทนี้กล่าวถึงความเป็นมาของกฎหมายเทคโนโลยีสารสนเทศและการสื่อสารในประเทศไทย รวมถึงคำจำกัดความตามมาตราในพระราชบัญญัติทางคอมพิวเตอร์ในแต่ละมาตรา และให้ความเข้าใจที่ถูกต้องเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยนำกรณีศึกษามาเป็นตัวช่วยในการเสริมความเข้าใจ

วัตถุประสงค์

การเรียนรู้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีความรู้ดังนี้

1.การเข้าใจถึงคำจำกัดความตามมาตราในพระราชบัญญัติทางคอมพิวเตอร์ พ.ศ.2550

2.การเข้าใจเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ (Log)

เนื้อหา

1. ความเป็นมาของการพัฒนากฎหมายเทคโนโลยีสารสนเทศ และการสื่อสารในประเทศไทย
2. คำจำกัดความตามมาตราในพระราชบัญญัติทางคอมพิวเตอร์ พ.ศ.2550
3. ความเข้าใจเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ (Log)
4. กรณีศึกษา

11.1 ความเป็นมาของการพัฒนากฎหมายเทคโนโลยีสารสนเทศ และการสื่อสารในประเทศไทย

เพื่อให้ประเทศมีโครงสร้างพื้นฐานทางกฎหมายรองรับด้านสังคมสารสนเทศ ซึ่งถือว่าเป็นปัจจัยสำคัญของการดำรงอยู่ของสังคมในศตวรรษที่ ๒๑ ใน พ.ศ. ๒๕๔๐ คณะรัฐมนตรีได้เห็นชอบให้มีการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น ๖ ฉบับ โดย ๓ ฉบับแรก เป็นกฎหมายที่ส่งเสริมการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิงสร้างสรรค์ อันเอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์หรือพาณิชย์อิเล็กทรอนิกส์ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ส่วนกฎหมายในลำดับที่ ๔ และ ลำดับ ๕ เป็นกฎหมายที่จะใช้เป็นมาตรการในการคุ้มครองหรือปกป้องสังคมจากการประยุกต์ ใช้เทคโนโลยีสารสนเทศและการสื่อสารในเชิงไม่สร้างสรรค์ และฉบับสุดท้ายเป็นกฎหมายฉบับที่จะสร้างกลไกเพื่อลดความเหลื่อมล้ำของสังคม สารสนเทศ โดยกฎหมายดังกล่าวปรากฏตามรายการ ดังต่อไปนี้

- กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เพื่อรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ มีผลบังคับใช้เมื่อวันที่ ๓ เมษายน ๒๕๔๕ และมีการตั้ง คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นเพื่อดำเนินการต่างๆ ตามพระราช บัญญัตินี้ (อ่าน ตัว พ.ร.บ.นี้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔)
- กฎหมายลายมือชื่ออิเล็กทรอนิกส์ เพื่อรองรับผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์ ไม่ได้มีการจัดทำแยกเป็นอีกหนึ่งฉบับ เพราะได้มีการรวมหลักการไว้กับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมีผลบังคับใช้แล้วเมื่อวันที่ ๓ เมษายน ๒๕๔๕
- กฎหมายการโอนเงินทางอิเล็กทรอนิกส์ ได้มีการจัดทำขึ้นเพื่อรองรับการโอนเงิน และการชำระเงินทางอิเล็กทรอนิกส์ เดิมจะพัฒนาเป็นกฎหมายลำดับพระราชบัญญัติ แต่หลังจากที่มีการดำเนินงานของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว คณะกรรมการฯได้จัดทำเป็นกฎหมายลำดับรองภายใต้มาตรา ๓๒ ของกฎหมายธุรกรรมทางอิเล็กทรอนิกส์แทน เรียกว่าร่างพระราชกฤษฎีกากำกับดูแลธุรกิจบริการเกี่ยวกับการชำระเงินทางอิเล็กทรอนิกส์ เพื่อให้คล่องตัวและเร็วขึ้นกว่าการทำเป็นพระราชบัญญัติ ขณะนี้คณะรัฐมนตรีได้รับหลักการและมอบหมายให้สำนักงานคณะกรรมการกฤษฎีกาตรวจ พิจารณาต่อไป
- กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ร่างกฎหมายฉบับนี้ได้จัดทำขึ้นเพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ เมื่อผ่านการรับหลักการของคณะรัฐมนตรี และเข้าสู่การพิจารณาโดยคณะกรรมการกฤษฎีกา (นายมีชัย ฤชุพันธุ์ ประธาน)แล้ว ได้เปลี่ยนชื่อเป็น ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เนื่องจากคณะกรรมการเห็นว่า การกระทำบางลักษณะไม่น่าจะเป็น “อาชญากรรม (Crime)” ร่างกฎหมายนี้ เข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติไปเมื่อวันที่ ๑๕ พ.ย. ๒๕๔๙ ขณะนี้ อยู่ระหว่างการพิจารณาของคณะกรรมาธิการวิสามัญ พิจารณาร่าง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ สภานิติบัญญัติแห่งชาติ (อ่านตัวร่าง พ.ร.บ. นี้ ร่าง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ผ่าน สคก.แล้ว)
- ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ได้จัดทำขึ้นเพื่อคุ้มครองสิทธิขั้นพื้นฐานในความเป็นส่วนตัว โดยมุ่งคุ้มครองข้อมูลส่วนบุคคล ที่อาจมีการละเมิดและสามารถนำไปใช้ในทางมิชอบได้โดยง่าย (ในการทำธุรกรรมทางออนไลน์หรือการใช้อินเทอร์เน็ต) ทั้งนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ให้ความเห็นชอบให้ สนง.ปลัดนายก รัฐมนตรี (โดย สนง.ข้อมูลข่าวสารของราชการ) ทำหน้าที่ร่วมร่างกฎหมายฉบับดังกล่าวเข้ากับร่างกฎหมายที่จัดทำโดย สขร. โดยยังคงยืนยันให้มีการจัดตั้งสำนักงานที่จะดูแลการคุ้มครองข้อมูลส่วน บุคคลอยู่ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งหมดนี้เมื่อกำหนดเป็นพระราชบัญญัติว่าด้วยการกระทำความผิด

เกี่ยวกับคอมพิวเตอร์ พ.ศ.2550เกิดขึ้นแล้ว สาระสำคัญ ที่ถือว่าเป็นแก่นแท้ของกฎหมายนี้คือ "ต้องการหาผู้กระทำความผิดมาลงโทษให้ได้"

เมื่อพิจารณาความเป็นจริงบนโลกอินเทอร์เน็ตแล้วจะพบว่าการจะสืบค้นหาผู้กระทำความผิดนั้นจะเกิดขึ้นได้ก็ต่อเมื่อต้องมีหลักฐาน ซึ่งหลักฐานทางการรับ-ส่งข้อมูลนั้นจะเกิดขึ้นจาก Log หรือเรียกว่าเป็นข้อมูลจราจรทางคอมพิวเตอร์นั้นเอง ซึ่งจะขยายความในเอกสารต่อจากนี้ แต่ให้เข้าใจว่า Log file จะเป็นกุญแจสำคัญในการค้นหาผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ ซึ่ง Log เองก็เป็นเพียงเครื่องมือหนึ่งในการสืบสวน และสอบสวนเพื่อหาผู้กระทำความผิดนั้นเอง

ในมาตราที่ 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะเป็นมาตราที่ให้คำนิยาย ซึ่งประกอบด้วย

1. ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
2. ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
3. ข้อมูลจราจรทางคอมพิวเตอร์ หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
4. ผู้ให้บริการ ซึ่งประกอบด้วย 2 ส่วนคือ ผู้ให้บริการแก่ผู้อื่นในการเข้าสู่อินเทอร์เน็ต และผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์กับบุคคลอื่น

(ขยายความผู้ให้บริการ)

ผู้ให้บริการ นอกจากจะหมายถึง ISP (Internet Service Provider) ทั่วไปแล้ว ยังหมายถึง ผู้ดูแลเว็บ และครอบคลุมถึงหน่วยงานที่มีการจัดบริการออนไลน์ บริการใช้อินเทอร์เน็ตและเครือข่ายทั่วไปในหน่วยงานของตนเองอีกด้วย เจ้าของร้านอินเทอร์เน็ต เจ้าของเว็บไซต์ รวมทั้งเจ้าของเว็บบอร์ด ล้วนแล้วเข้าข่ายที่จะเป็นผู้ให้บริการทั้ง สิ้น หากผู้ใช้เปิดบริการให้สาธารณชน เข้ามาใช้บริการเข้าถึงอินเทอร์เน็ต หรือสามารถแพร่ข้อความ ภาพ และเสียง ผ่านเว็บที่ผู้ใช้เป็นเจ้าของ

- ผู้ให้บริการตามกฎหมายนี้ ต้องทำตามหน้าที่ของ ผู้ให้บริการ ตามที่บัญญัติไว้ในพระราชบัญญัติฯนี้ กล่าวคือ
    - มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษ เฉพาะรายและเฉพาะคราวก็ได้
    - ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้ สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็น เวลาไม่น้อยกว่า 90 วัน (เก้าสิบวัน)นับตั้งแต่การใช้บริการสิ้นสุดลง
    - ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

5. ผู้ใช้บริการ คือ ผู้ใช้งานทั่วไปที่เข้าถึงอินเทอร์เน็ตในฐานะบุคคลธรรมดาผู้ใช้ไม่ควรทำในสิ่งต่อไปนี้ เพราะอาจจะเป็นหนทางที่นำไปสู่ "กระทำความผิด" ตาม พ.ร.บ.นี้

A. อย่าบอก password ของผู้ใช้แก่ผู้อื่น

ผู้ใช้ไม่มีทางทราบว่าผู้อื่นจะนำไปใช้งานเข้าสู่ระบบเมื่อใด หรือนำไปใช้ในการกระทำความผิดหรือไม่ หากผู้ที่แอบอ้างเป็นผู้ใช้ไปกระทำความผิด ตามมาตรา ๕ ถึง มาตรา ๑๖ ได้ทุกรูปแบบ กว่าผู้ใช้จะพิสูจน์ได้ว่าไม่ใช่ตัวผู้ใช้ทำเอง ต้องใช้เวลาในการพิสูจน์นาน ทางที่ดี ไม่ต้องบอก password ให้แก่ผู้ใด และไม่ควรเขียนลงบนกระดาษทีมีคนพบได้ ส่วน User ID อย่างเดียว บางครั้งก็สามารถปิดได้แต่บ่อยครั้งที่เราต้องใช้ User ID เพื่อใช้ในการสื่อสารกับผู้อื่น ให้คนทราบก็ไม่ก่อให้เกิดความเสียหายใด

บทแทรก การกำหนด password ให้เป็นที่จำง่ายหรือเดาง่ายเกินไป ก็เป็นภัยต่อตัวผู้ใช้เองได้เช่นกัน เพราะฉะนั้นควรหลีกเลี่ยงการตั้ง password เป็นชื่อลูก ชื่อคนรัก หรือชื่อสัตว์เลี้ยง หรือเลขหมายโทรศัพท์ที่อาจจะมีคนเดาได้ การตั้ง password ไม่ดี เสี่ยงเท่ากับการบอก password ให้แก่ผู้อื่น

B. อย่าให้ผู้อื่นยืมใช้เครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่เพื่อเข้าอินเทอร์เน็ต ถ้าผู้ใช้ได้สั่งให้เครื่องจำ user ID และ password เอาไว้เพื่อความสะดวกในการเข้าสู่ระบบข้อมูลหรือเครือข่ายอินเทอร์เน็ต เหตุการณ์แบบนี้ไม่แตกต่างไปจากความเสี่ยงข้อแรก คือเท่ากับการบอก password แก่ผู้อื่น แล้วผู้นั้นเอาไปกระทำความผิดได้หลายรูปแบบ

C. อย่าติดตั้งระบบเครือข่ายไร้สายในบ้านหรือที่ทำงานโดยไม่ใช้มาตรการการตรวจสอบผู้ใช้งานและการเข้ารหัสลับการทำเช่นนี้ทำให้คนทั่วไปที่อยู่ริมถนน หรือข้างบ้าน สามารถเข้าร่วมใช้ระบบไร้สายของผู้ใช้ได้ ผู้ใช้จะทราบได้อย่างไร คนที่ผ่านหน้าบ้านหรือสำนักงานที่ติด wireless LAN นั้นจะไม่ใช่ผู้ประสงค์ร้ายที่อาจจะมาเข้าอินเทอร์เน็ตของผู้ใช้เพื่อไปกระทำความผิด แล้วเขาก็ลอยนวล

D. อย่าเข้าสู่ระบบด้วย user ID และ password ที่ไม่ใช่ของผู้ใช้เองอันนี้ ถ้าทำไปแล้ว จะผิดตรงๆ ตามมาตรา ๕ และ อาจจะผิดตามมาตรา ๗ ด้วยอย่านำ user ID และ password ของผู้อื่นไปใช้งานหรือเผยแพร่อันนี้ ถ้าทำไปแล้ว จะผิดตรงๆตามมาตรา ๖

E. อย่าส่งต่อซึ่งภาพหรือข้อความ หรือภาพเคลื่อนไหวที่ผิดกฎหมาย ("ผิดกฎหมาย" ได้แก่กรณีที่ภาพหรือข้อความที่ ลามกอนาจาร ละเมิดทรัพย์สินทางปัญญา หมิ่นพระบรมเดชานุภาพ สร้างปัญหาความมั่นคง ทำให้บุคคลเสียชื่อเสียง/หมิ่นประมาท ฯลฯ) หากผู้ใช้ได้รับสิ่งเหล่านี้แล้ว ให้ลบทิ้งไปจากเครื่องของผู้ใช้ ถ้าผู้ใช้ได้ส่งต่อให้ผู้อื่น หรือเก็บไว้ในเครื่องของผู้ใช้ จะมีความผิดตามมาตรา ๑๔ เอาได้

F. อย่ากด "remember me" หรือ "remember password" ที่เครื่องคอมพิวเตอร์สาธารณะ และอย่า log-in เพื่อทำธุรกรรมทางการเงินที่เครื่องสาธารณะ ถ้าผู้ใช้ไม่มีความรู้ทาง computer security คอมพิวเตอร์สาธารณะ ได้แก่ เครื่องคอมพิวเตอร์ที่บริการให้กับคนทั่วไป เช่น ในห้องสมุด สนามบิน ร้านกาแฟ ร้านอินเทอร์เน็ต ผู้ใช้มีความเสี่ยงจากการถูกดักข้อมูล ดักแป้นพิมพ์ และการแอบบันทึก IDและ Password โดยเจ้าของร้าน หรือโดยผู้ใช้ที่เคยแอบมาติดตั้งโปรแกรมไม่พึงประสงค์ ในเครื่องนั้น หากผิดพลาดเพียงครั้งเดียว ข้อมูลเกี่ยวกับตัวผู้ใช้ที่เคยป้อนลงในเครื่องสาธารณะ อาจจะถูกบันทึก และแอบ

นำไปใช้งาน ยิ่งไปกว่านั้น คอมพิวเตอร์สาธารณะ อาจจะเก็บข้อมูลจอภาพที่ผู้ใช้ไปชม รวมทั้ง cookies ซึ่งล้วนแล้วแต่จะทำให้บุคคลอื่นสามารถปลอมเป็นตัวผู้ใช้เวลาเข้าไปในเว็บไซต์ ที่ผู้ใช้เคยเรียกดูได้ทั้งสิ้น กล่าวคือ หากผู้ใช้ยังไม่มีความชำนาญเรื่องการระงับการบันทึกข้อมูลส่วนบุคคลใน PC ผู้ใช้ไม่ควรเข้าไปทำธุรกรรมทางการเงิน ณ เครื่องคอมพิวเตอร์สาธารณะที่ไหนเลย ยกเว้นว่าผู้ใช้สามารถตรวจการตั้งค่าต่างๆ ของ Windows (Network setting และ IE Setting) ได้อย่างคล่องแคล่ว แม้จะเข้าไปเช็ค email ทาง hotmail หรือ gmail หรือ yahoo เครื่องสาธารณะต่าง ๆ จะ "จดจำ" password ทุกตัวของผู้ใช้เพื่อให้เข้าใช้ครั้งต่อไปโดยอัตโนมัติทั้งสิ้น คนที่รอใช้เครื่องหลังจากผู้ใช้ มีวิธีการที่จะทราบว่าผู้ใช้ไปชมเว็บไซต์ไหนบ้าง โดยการกดปุ่ม "Go" ตามด้วย "History" ใน Internet Explorer แล้วเข้าสู่เว็บไซต์ราวกับเป็นตัวผู้ใช้ได้เลย

G. อย่าใช้ WiFi (Wireless LAN) ที่เปิดให้ใช้ฟรี โดยปราศจากการเข้ารหัสลับข้อมูล ควรระวัง หากผู้ใช้คิดจะทำรายการด้านการเงินบนเครื่องประเภทนี้ ข้อมูลที่ควรจะเป็นความลับของผู้ใช้ อาจถูกดักรับได้จากเครื่องคอมพิวเตอร์ในรัศมีคลื่นวิทยุของ WiFi (รัศมี 8 กิโล line of sight) (โปรดแสวงหา WPA หรือ WEP เพื่อการใช้ระบบเข้ารหัสลับมาตรฐาน ในการเข้าใช้ wireless LAN)

H. อย่าทำผิดตามมาตรา ๑๔ ถึง ๑๖ เสียเอง ไม่ว่าโดยบังเอิญ หรือโดยรู้เท่าไม่ถึงการณ์ การเขียนข่าวลงในเว็บสาธารณะ หรือการส่งข้อมูลเท็จ ข้อมูลที่ทำให้เกิดการตื่นตระหนกในวงกว้าง ทำภาพตัดต่อที่ทำให้บุคคลอื่นเสียหาย ฯลฯ ล้วนแล้วแต่ไม่ควรทำทั้งสิ้น ในเวลาเดียวกัน การปล่อย User ID และ password ให้ผู้อื่นทราบ ก็อาจจะเป็นเหตุให้ผู้ใช้เดือดร้อนได้ เพราะหากผู้ที่ทราบไปลงมือกระทำ หรือเอาไปเผยแพร่ต่อให้บุคคลอื่นๆ ทราบ ความผิดก็จะตกอยู่แก่ผู้ใช้ เพราะผู้ใช้อาจจะไม่มีทางพิสูจน์ได้ว่าใครเป็นคนกระทำ แค่ปฏิเสธว่าตนเองไม่ได้ทำอาจจะไม่เพียงพอในการอธิบายต่อพนักงานเจ้าหน้าที่ หรือ การสู้คดีในศาล

11.2 คำจำกัดความ ตามมาตราในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

หมวดที่ 1 ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้น มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้น เป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้ง ปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคล ทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อ ประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็น เครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบาง ส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความ ตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการ ก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อน ร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือ บุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

หมวดที่ 2 พนักงานเจ้าหน้าที่

A. อำนาจของพนักงานเจ้าหน้าที่

มาตรา ๑๘ อำนาจทั่วไปของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้ง แบ่งเป็น

(๑) อำนาจที่ดำเนินการได้โดยไม่ต้องใช้อำนาจศาล

- มีหนังสือสอบถาม เพื่อให้ส่งคำชี้แจง ให้ข้อมูล
- เรียกข้อมูลจราจรคอมพิวเตอร์
- สั่งให้ส่งมอบข้อมูลตาม ม.๒๖

(๒) อำนาจที่ต้องขออนุญาตศาล

- ทำสำเนาข้อมูล
- เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์
- ถอดรหัสลับ
- ยึดอายัดระบบคอมพิวเตอร์

B. ข้อจำกัด/การตรวจสอบการใช้อำนาจพนักงานเจ้าหน้าที่

มาตรา ๑๙ การจำกัดการใช้อำนาจของพนักงานเจ้าหน้าที่ ซึ่งมีเงื่อนไขการใช้อำนาจทั่วไปตามมาตรา ๑๘ ประกอบด้วย

- การขออนุญาตศาล
- การส่งคำร้องขอศาล
- ระยะเวลาในการยึด/อายัดระบบคอมพิวเตอร์ ๓๐ วัน หรือ ๖๐ วัน

C. การปิดกั้นเว็บไซต์ (Block Website)

มาตรา ๒๐ ในกรณีที่การกระทำความผิดเป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่

๑. อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

๒. ที่มีลักษณะขัดต่อ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับ การทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูล คอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

D. ห้ามมิให้พนักงานเผยแพร่ข้อมูลที่ได้มาตาม มาตรา ๑๘

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำ

๑. เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้

๒. เพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

๓. เป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

E. พนักงานที่ประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูล

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

F. ความรับผิดชอบ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

G. การรับฟังพยานหลักฐาน

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

H. หน้าที่ของผู้ให้บริการ

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า เก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่ง ให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

I. หากมีการฝ่าฝืนคำสั่งศาล หรือพนักงานเจ้าหน้าที่

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับ ไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

J. การแต่งตั้งพนักงานเจ้าหน้าที่

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้ และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

K. การรับคำร้องทุกข์กล่าวโทษ จับ ควบคุม ค้นและการกำหนดระเบียบแนวทางและวิธีปฏิบัติ

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวล กฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้ ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการ ตามอำนาจหน้าที่ต่อไป ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติ และรัฐมนตรีมีอำนาจ ร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

11.3 ความเข้าใจเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ (Log) หลักเกณฑ์ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวกับกฎหมาย

ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้น่าเชื่อถือ ให้ผู้ใช้ยึดหลักการดังนี้

- ข้อมูลที่เก็บ ต้องมีรายการที่สามารถระบุว่า ผู้ใช้คอมพิวเตอร์ เป็นใคร เข้ามาทางเครือข่ายใด (Port Services) มีหมายเลข IP Address อะไร ใช้โปรแกรมประยุกต์อะไร ในช่วงเวลาใด
- นาฬิกาของเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสาร ต้องมีการตั้งเวลาให้ตรงกับนาฬิกาอะตอมที่ใช้อ้างอิง เช่น ที่ NIST (สหรัฐอเมริกา) กรมอุทกศาสตร์ (กองทัพเรือ) สถาบันมาตรวิทยา (กระทรวงวิทยาศาสตร์และเทคโนโลยี) หรือใช้เทียบเวลากับเครื่อง time server ผ่านทางอินเทอร์เน็ต เช่น เนคเทค (ntp://clock.nectec.or.th) ซึ่งอุปกรณ์เครือข่ายทั่วไป รวมทั้งเครื่องคอมพิวเตอร์มาตรฐานทั่วไป สามารถตั้งเวลาให้ตรงกับเวลามาตรฐานโลกได้ด้วยความแม่นยำในระดับ 1 มิลลิวินาทีหรือดีกว่านี้
- ข้อมูลจราจร ต้องมีการจัดเก็บอย่างปลอดภัย ไม่เสี่ยงต่อการถูกแก้ไข หรือสื่อข้อมูลเสื่อมคุณภาพ ในระยะเวลาไม่น้อยกว่า 90 วัน

Log File มาจากไหน?

1) เหตุการณ์ที่เกิดขึ้นภายในเครื่อง (Local Host Log)
    1. เหตุการณ์ที่เกิดจากเครื่องคอมพิวเตอร์ เรียกว่า System Log แบ่งเป็นเหตุการณ์ที่เกิดจากค่า Error ที่พบในการเข้าถึงระบบปฏิบัติการ (OS log error) สำหรับรายชื่อผู้ใช้งานในเครื่อง และการตั้งค่ารีโมตผ่านทางระบบเครือข่าย (Network), เหตุการณ์ที่ส่งผลกระทบกับระบบ Kernel (Kernel Log) เป็นต้น
    2. เหตุการณ์ที่เกิดขึ้นจากการใช้งาน Application เรียกว่า Application Log สามารถแบ่งแยกตาม

โปรแกรมที่ติดตั้งลงในเครื่อง ได้แก่ Web Server, Mail Server, Proxy Server, โปรแกรมที่เกี่ยวกับการสนทนาออนไลน์ หรือโปรแกรมอื่นๆ ที่ลงบนเครื่อง รวมถึงผลการเข้าใช้งาน Application User ในแต่ละ Application เป็นต้น

กล่าวโดยสรุป ค่า Local Host Log ประกอบด้วย System Log และ Application Log ที่ถูกเก็บบันทึกไว้ รวมเรียกว่า "ค่า syslog"

2) เหตุการณ์ที่เกิดขึ้นบนระบบเครือข่าย (Network Log) เป็นการเก็บบันทึกการไหลเวียนข้อมูลสารสนเทศบนระบบเครือข่าย ทั้งข้อมูลที่ไหลจากภายในเครือข่ายออกสู่ภายนอก (ไม่ว่าจะเป็นระบบ Extranet หรือ Internet) หรือข้อมูลจากภายนอกเข้าสู่ระบบเครือข่ายภายในองค์กร ข้อมูลที่กล่าวถึงคือ ระบบงานที่ใช้ตามโปรโตคอลมาตรฐาน เช่น การเปิดเว็บ (HTTP, HTTPS), การส่ง files (Upload/Download), การรับ-ส่งอีเมล์ (เช่น SMTP, POP3, IMAP), การใช้โปรแกรมสนทนาออนไลน์ เป็นต้น

อย่างไรก็ตาม ปัญหาที่พบมากในเรื่องของการเก็บบันทึก Log File หรือ Traffic Data คือ การมองข้ามความต้องการพื้นฐานของกฎหมายที่ต้องการเก็บหลักฐานเพื่อหาผู้กระทำผิดมาลงโทษ จึงทำให้การเก็บข้อมูลหลักฐานดังกล่าวไม่สอดคล้องกับความต้องการของพนักงานเจ้าหน้าที่ ซึ่งรวมถึงเจ้าหน้าที่ตำรวจ, DSI หรือหน่วยงานใดๆ ที่เกี่ยวข้อง จนไม่สามารถนำหลักฐานดังกล่าวนี้ไปใช้เพื่อหาผู้กระทำความผิด หรือใช้เป็นหลักฐานอ้างอิงในชั้นศาลได้

ความเข้าใจผิด 3 อันดับแรก ที่นำมาสู่การเก็บหลักฐานอย่างไม่ถูกต้อง

ความเข้าใจผิดประการที่ 1 กฎหมายสนใจเฉพาะเรื่องการ Authentication หรือการระบุตัวตนของการใช้งานเครือข่ายเท่านั้น จริงหรือไม่?

คำตอบคือถูกแต่ไม่ทั้งหมด ทั้งนี้เพราะการที่สามารถระบุตัวบุคคลได้แต่ไม่มีหลักฐานยืนยันว่าบุคคลผู้นั้นได้กระทำการนั้นๆ จริง ก็ไม่ถือว่ามีหลักฐานครบถ้วนสมบูรณ์ตามที่กฎหมายต้องการ เช่นเดียวกัน หากมีการเก็บ Log File เพื่อระบุตัวบุคคล พร้อมระบุด้วยว่าบุคคลนั้นได้กระทำการนั้นๆ จริง รวมทั้งมีการเก็บ Log File ที่บอกได้ครบถ้วนว่า ใคร ทำอะไร ที่ไหน เวลาใด อย่างไร แล้ว แต่การเก็บ Log File นั้นเป็นแบบกระจัดกระจาย ไม่เป็นองค์ประกอบเดียวกัน ก็อาจทำให้หลักฐานอ่อนไม่เพียงพอต่อการดำเนินคดีได้เช่นกัน

นอกจากนี้ แม้มีการเก็บ Log File ครบถ้วนทุกประการ แต่ไม่ได้มีการยืนยันความถูกต้องและสมบูรณ์ของ Log File นั้น เช่น Log File นั้นๆ ไม่ได้มีการทำ Data Hashing เก็บควบคู่กับ Log File ต้นฉบับเพื่อยืนยันความถูกต้องแล้ว Log File ที่ส่งมอบให้พนักงานเจ้าหน้าที่อาจไม่สามารถนำไปใช้เป็นหลักฐานในชั้นศาลได้ ด้วยไม่อาจแน่ใจได้ว่าหลักฐานชิ้นนั้นได้ถูกแก้ไขเปลี่ยนแปลงเพื่อสร้างหลักฐานเท็จหรือไม่

ความเข้าใจผิดประการที่ 2 โปรแกรม Open Source ที่ช่วยในการเก็บ Log File ก็สามารถเอามาใช้ได้ จริงหรือ?

คำตอบคือ "ได้" แต่ต้องมีการนำมาปรับปรุงเพิ่มเติม เนื่องจากโปรแกรม Open Source เหล่านั้นถูกสร้างขึ้นโดยมีวัตถุประสงค์เพื่อเก็บ Log File ที่เกิดจากอุปกรณ์ในเครือข่ายชนิดต่างๆ แล้วนำมาวิเคราะห์หาความผิดพลาดหรือนำมาปรับปรุงเพื่อให้มีการใช้งานเครือข่ายนั้นๆ อย่างมีประสิทธิภาพ ไม่ได้ถูกสร้างมาเพื่อเก็บหลักฐานที่เกี่ยวข้องกับคดีความทางคอมพิวเตอร์แต่อย่างใด ดังนั้นหากมีการนำโปรแกรม Open Source มาใช้ก็ต้องคำนึงถึงผลลัพธ์ที่ได้ว่าตรงตามที่กฎหมาย

ต้องการหรือไม่ เช่น เก็บ Log File ได้ก็จริงแต่ไม่ได้เก็บอย่างครบถ้วนเป็นองค์ประกอบเดียวกัน หรือไม่ได้มีการทำการยืนยันความถูกต้องของ Log File นั้นๆ เป็นต้น

ความเข้าใจผิดประการที่ 3 การจะเก็บ Log File ให้ครบถ้วนหมายถึงต้องลงทุนทำ SIM/SEM หรือ SIEM?

คำตอบคือไม่จำเป็น ตามที่ได้กล่าวไปแล้วข้างต้นว่าความต้องการของกฎหมายฉบับนี้คือต้องการหาผู้กระทำผิดมารับโทษ โดยต้องมีหลักฐานประกอบอย่างถูกต้อง และยอมรับได้ในชั้นศาล ดังนั้นกระบวนการที่จะได้มาซึ่งหลักฐานจึงไม่ได้บังคับว่าจะมาด้วยกระบวนการใด หากแต่ต้องถูกต้อง ครบถ้วน และยืนยันความถูกต้องของ Log File ได้ และศาลเชื่อในหลักฐานนี้เท่านั้น ดังนั้นการมีวิธีการอื่นใดที่ได้มาซึ่ง Log File ที่ครบถ้วน สามารถบอกได้ว่าบุคคลใด ทำอะไร ที่ไหน เวลาใด และอย่างไร ตลอดจนเป็น Log File ที่มีการยืนยันความถูกต้องแล้ว ย่อมเพียงพอสำหรับการหาระบบเพื่อรองรับตามกฎหมายฉบับนี้

นอกจากเรื่องการเก็บ Log File แล้ว ยังมีบางประเด็นปลีกย่อยที่มีความเข้าใจคลาดเคลื่อนกันอยู่บ้าง เช่น เรื่องเกี่ยวกับ Sniffer หรือการดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 8 ที่ระบุไว้ว่า "ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ" นั้น บางคนยังมีความเข้าใจผิดว่า การที่หน่วยงาน เช่น บริษัท ห้างร้าน หรือหน่วยงานรัฐ ซึ่งเข้าข่ายเป็นผู้ให้บริการ ได้ติดตั้งอุปกรณ์ที่เฝ้าระวังภัยคุกคามในเครือข่าย ยกตัวอย่างเช่น IPS/IDS Antivirus Gateway หรือ Content Filtering เพื่อป้องกันไม่ให้พนักงานหรือเจ้าหน้าที่ในองค์กรใช้ระบบสารสนเทศในองค์กรอย่างไม่เหมาะสมนั้น ถือว่าเข้าข่ายกระทำผิดตามมาตรานี้ ซึ่งแท้จริงแล้วไม่ถูกต้อง เนื่องจากหน่วยงานเหล่านั้นเป็นเจ้าของเครือข่ายและให้เจ้าหน้าที่ในหน่วยงานใช้เพื่อประโยชน์แห่งหน่วยงาน ดังนั้นการกระทำใดๆ ต่อเครือข่ายของตนย่อมเป็นการชอบด้วยกฎหมาย ต่างจากกรณีมีผู้ไม่ประสงค์ดีจงใจสร้างเครือข่ายไร้สายหนึ่งขึ้นมาเพื่อหลอกให้บุคคลอื่นหลงคิดว่าเป็นเครือข่ายสาธารณะ เพื่อทำการดักรับข้อมูลคอมพิวเตอร์ของบุคคลนั้น การกระทำอย่างหลังนี้ ถือเป็นการกระทำโดยมิชอบ ดังนั้นจึงเข้าข่ายการกระทำความผิดตามมาตรา 8 เป็นต้น

11.4 กรณีศึกษา การหมิ่นประมาทออนไลน์ หลักฐานใดเชื่อถือได้

บทบาทของอินเทอร์เน็ตในปัจจุบันนั้น นอกจากจะเป็นแหล่งเผยแพร่ข้อมูลข่าวสาร, ตลาดนัดออนไลน์, ตลาดแรงงาน, สถานีวิทยุ/โทรทัศน์ ที่เข้าถึงได้ง่าย ประหยัดทั้งเวลาและค่าใช้จ่ายแล้ว ยังวิวัฒน์จนกลายเป็นสังคมเสมือน ที่ผู้คนทุกเพศ ทุกวัย สามารถพูดคุย แลกเปลี่ยนทัศนคติและข้อมูลที่มีอยู่ได้ ผ่านเครือข่ายสังคม “Social Networking” ถือเป็นจุดเปลี่ยนทางสังคม ซึ่งคนรุ่นใหม่น้อยคนนัก ที่ไม่เคยสื่อสารผ่านช่องทางนี้ การใส่ความผู้อื่นต่อบุคคลที่สาม หรือการหมิ่นประมาท จึงไม่จำเป็นต้องเกิดบนเวทีปราศรัย, บทสัมภาษณ์ผ่านสื่อ ฯลฯ อีกต่อไป หากเกิดขึ้นง่ายดายโดยมี คำถามคือ หากเกิดคดีความขึ้น หลักฐานใดเชื่อถือได้ในชั้นศาล?

หากนาย ก. โพสต์ว่าร้ายนาย ข. ลงบน Hi5 ของนาย ก. เอง มีคนเข้าอ่านมากมายจนรู้ถึงหู นาย ข. นาย ข. เข้ามาเห็น จึง save หน้าจอ และพิมพ์ข้อความเก็บไว้เป็นหลักฐาน พร้อมแจ้งความดำเนินคดีกับนาย ก. ข้อหาหมิ่นประมาท

กระดาษแผ่นนั้นถือเป็นหลักฐานได้หรือไม่? เทคโนโลยีที่ก้าวล้ำสามารถสร้างและแต่งเติมข้อความหรือรูปภาพได้ด้วยคอมพิวเตอร์ แล้วจะเชื่อได้อย่างไรว่านาย ข. มิได้สร้างหลักฐานเท็จขึ้นมาใส่ความ นาย ก. อีกมุมหนึ่ง หากนาย ก. กระทำผิดจริง และได้ลบข้อความนั้นออกไปแล้ว ก็ย้อนสู่คำถามเดียวกัน ศาลจะประทับรับฟ้องด้วยหลักฐานกระดาษพิมพ์ข้อความหรือ? พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กำหนดให้ผู้ให้บริการเว็บไซต์ต้องเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อใช้เป็นหลักฐานหากเกิดคดีความออนไลน์ขึ้น แต่หากผู้ดูแลเว็บไซต์ เป็นผู้กระทำความผิดเสียเอง เราจะมั่นใจได้อย่างไรว่าจะไม่เกิดการลบหรือแก้ไขข้อความเพื่อให้ตนพ้นผิด

ด้วยเหตุนี้ เจ้าของเว็บไซต์ ทั้งเว็บไซต์ส่วนบุคคลและเว็บไซต์องค์กร/หน่วยงานต่างๆ โดยเฉพาะเว็บไซต์ที่ให้บริการเว็บบอร์ด เว็บบล็อก จึงควรใช้โปรแกรมเก็บบันทึกข้อมูลการใช้งานเว็บไซต์ของตน เพื่อให้ทราบว่ามีใครเข้ามาใช้บริการ ที่เพจไหน ทำอะไร เมื่อไร อย่างไร โดยจัดเก็บข้อมูลดังกล่าวไว้ไม่ต่ำกว่า 90 วัน สามารถสืบค้นย้อนหลัง และยืนยันได้ว่าข้อความดังกล่าวจะไม่ถูกแก้ไข สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่ออำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ ให้สามารถตรวจสอบหลักฐานย้อนหลังได้ หากเกิดคดีความออนไลน์ ซึ่งคาดว่าจะมีแนวโน้มเพิ่มสูงขึ้น ตามสภาพสังคมที่เปลี่ยนแปลงไป

บทที่ 12

จริยธรรมและคุณธรรมการใช้คอมพิวเตอร์และอินเทอร์เน็ต

ขอบเขต

ในบทนี้กล่าวถึงหลักศีลธรรม จริยธรรม วัฒนธรรมของสังคมออนไลน์ของการกระทำที่ยอมรับกันโดยทั่วไป และการปฏิบัติตนอย่างถูกต้องตามทำนองครองธรรม

วัตถุประสงค์

เพื่อต้องการให้เข้าใจถึงการสร้างจิตสำนึกอันดีในการใช้ข้อมูลสารสนเทศ ซึ่งถือได้ว่าเป็นบทเรียนที่สำคัญบทหนึ่งสำหรับการเป็นลูกเสือไซเบอร์

เนื้อหา

1. คุณธรรม-จริยธรรมในการใช้คอมพิวเตอร์
2. จรรยาบรรณการใช้อินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
3. บัญญัติ 10 ประการในการใช้อินเทอร์เน็ต และเครือข่ายทางสังคม

12.1 คุณธรรม-จริยธรรมในการใช้คอมพิวเตอร์

จริยธรรม หมายถึง "หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ" ในทางปฏิบัติแล้ว การระบุว่าการกระทำสิ่งใดผิดจริยธรรมนั้น อาจกล่าวได้ไม่ชัดเจนมากนัก ทั้งนี้ ย่อมขึ้นอยู่กับวัฒนธรรมของสังคมในแต่ละประเทศด้วย อย่างเช่น กรณีที่เจ้าของบริษัทใช้กล้องในการตรวจจับหรือเฝ้าดูการทำงานของพนักงาน เป็นต้น ตัวอย่างของการกระทำที่ยอมรับกันโดยทั่วไปว่าเป็นการกระทำที่ผิดจริยธรรม เช่นการใช้คอมพิวเตอร์ทำร้ายผู้อื่นให้เกิดความเสียหายหรือก่อความรำคาญ เช่น การนำภาพหรือข้อมูลส่วนตัวของบุคคลไปลงบนอินเทอร์เน็ตโดยไม่ได้รับอนุญาต การใช้คอมพิวเตอร์ในการขโมยข้อมูลการเข้าถึงข้อมูลหรือคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาตการละเมิดลิขสิทธิ์ โดยทั่วไป เมื่อพิจารณาถึงจริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศแล้ว จะกล่าวถึงใน 4 ประเด็น ที่รู้จักกันในลักษณะตัวย่อว่า PAPA ประกอบด้วย 4 ประการ

1. ความเป็นส่วนตัว (Information Privacy)
2. ความถูกต้อง (Information Accuracy)
3. ความเป็นเจ้าของ (Information Property)
4. การเข้าถึงข้อมูล (Data Accessibility) ความเป็นส่วนตัว (Information Privacy)

1.ความเป็นส่วนตัว (Information Privacy)

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ โดยทั่วไปหมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ใช้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล และองค์การต่างๆ ปัจจุบันมีประเด็นเกี่ยวกับความเป็นส่วนตัวที่เป็นข้อหน้าสังเกตดังนี้

1.การเข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลลงในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก-แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร

2.การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล เช่น บริษัทใช้คอมพิวเตอร์ในการตรวจจับหรือเฝ้าดูการปฏิบัติงาน/การใช้บริการของพนักงาน ถึงแม้ว่าจะเป็นการติดตามการทำงานเพื่อการพัฒนาคุณภาพการใช้บริการ แต่กิจกรรมหลายอย่างของพนักงานก็ถูกเฝ้าดูด้วย พนักงานสูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

3.การใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ในการขยายตลาด

4.การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเทอร์เน็ตที่มีการใช้โปรโมชั่น หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต และที่อยู่อีเมลความถูกต้อง (Information Accuracy)

2.ความถูกต้อง (Information Accuracy)

ความน่าเชื่อถือของข้อมูล ทั้งนี้ข้อมูลจะมีความน่าเชื่อถือมากน้อยเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูลด้วย ประเด็นด้านจริยธรรมที่เกี่ยวข้องกับความถูกต้องของข้อมูล โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่

ในการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูลนั้น คุณลักษณะที่สำคัญประการหนึ่ง คือ ความน่าเชื่อถือของข้อมูล เช่น ในกรณีที่องค์การให้ลูกค้าลงทะเบียนด้วยตนเอง หรือกรณีของข้อมูลที่เผยแพร่ผ่านทางเว็บไซต์ อีกประเด็นหนึ่ง คือ จะทราบได้อย่างไรว่าข้อผิดพลาดที่เกิดขึ้นนั้นไม่ได้เกิดจากความจงใจ และผู้ใดจะเป็นผู้รับผิดชอบหากเกิดข้อผิดพลาด

ดังนั้น ในการจัดทำข้อมูลและสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ นอกจากนี้ ควรให้สิทธิแก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลของตนเองได้ เช่น ผู้สอนสามารถดูคะแนนของนักศึกษาในความรับผิดชอบ หรือที่สอนเพื่อตรวจสอบว่าคะแนนที่ป้อนไม่ถูกแก้ไขเปลี่ยนแปลง

3.ความเป็นเจ้าของ (Information Property)

ความเป็นเจ้าของ (Information Property) สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น บทเพลง โปรแกรมคอมพิวเตอร์ แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่างๆ ได้ เช่น สิ่งพิมพ์ เทป ซีดีรอม เป็นต้น

ในสังคมของเทคโนโลยีสารสนเทศ มักจะกล่าวถึงการละเมิดลิขสิทธิ์ซอฟต์แวร์ เมื่อท่านซื้อโปรแกรมคอมพิวเตอร์ที่มีการจดลิขสิทธิ์ นั่นหมายความว่าท่านได้จ่ายค่าลิขสิทธิ์ในการใช้ซอฟต์แวร์นั้น สำหรับท่านเองหลังจากที่ท่านเปิดกล่องหรือบรรจุภัณฑ์แล้ว หมายถึงว่าท่านได้ยอมรับข้อตกลงเกี่ยวกับลิขสิทธิ์ในการใช้สินค้านั้น

ซึ่งลิขสิทธิ์ในการใช้จะแตกต่างกันไปในแต่ละสินค้าและบริษัท บางโปรแกรมคอมพิวเตอร์จะอนุญาตให้ติดตั้งได้เพียงครั้งเดียว หรือไม่อนุญาตให้ใช้กับคอมพิวเตอร์เครื่องอื่นๆ ถึงแม้ว่าคอมพิวเตอร์เครื่องนั้นๆ ท่านเป็นเจ้าของ และไม่มีผู้อื่นใช้ก็ตาม ในขณะที่บางบริษัทอนุญาตให้ใช้โปรแกรมนั้นได้หลายๆ เครื่อง ตราบใดที่ท่านยังเป็นบุคคลที่มีสิทธิในโปรแกรมคอมพิวเตอร์ที่ซื้อมา การคัดลอกโปรแกรมคอมพิวเตอร์ให้กับเพื่อน เป็นการกระทำที่จะต้องพิจารณาให้รอบคอบก่อนว่าโปรแกรมที่จะทำการคัดลอกนั้น เป็นโปรแกรมคอมพิวเตอร์ที่ท่านมีสิทธิ์ในระดับใด

4. การเข้าถึงข้อมูล (Data Accessibility)

เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิในการใช้งานระบบเช่น การบันทึก การแก้ไข/ปรับปรุง และการลบ เป็นต้น ดังนั้น ในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงของผู้ใช้ และการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ก็ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนบุคคล ในการใช้งานคอมพิวเตอร์และเครือข่าย

ร่วมกันให้เป็นระเบียบ หากผู้ใช้ร่วมใจกันปฏิบัติตามระเบียบและข้อบังคับของแต่ละหน่วยงานอย่างเคร่งครัดแล้ว การผิดจริยธรรมตามประเด็นดังที่กล่าวมาข้างต้นก็คงจะไม่เกิดขึ้น

บนเครือข่ายอินเทอร์เน็ตมีคำสั่งให้ใช้ในการโต้ตอบกันอย่างออนไลน์หลายคำสั่งเช่น write, talk หรือมีการสนทนาเป็นกลุ่มเช่น IRC เป็นต้น ในการเรียกหาหรือเปิดการสนทนาตลอดจนการสนทนาจะต้องมีมารยาทที่สำคัญได้แก่

- ควรเรียกสนทนาจากผู้ที่เรารู้จักและต้องการสนทนาด้วย หรือมีเรื่องสำคัญที่จะติดต่อด้วย ควรระลึกเสมอว่าการขัดจังหวะผู้อื่นที่กำลังทำงานอยู่อาจสร้างปัญหาให้ได้

- ก่อนการเรียกคู่สนทนาควรสอบสถานะ การใช้งานของคู่สนทนาที่ต้องการเรียกเพราะการเรียกแต่ละครั้งจะมีข้อความไปปรากฏบนจอภาพของฝ่ายถูกเรียกซึ่งอาจสร้างปัญหาการทำงานได้ เช่น ขณะกำลังทำงานค้าง ftp ซึ่งไม่สามารถหยุดได้

- หลังจากเรียกไปชั่วขณะคู่ที่ถูกเรียกไม่ตอบกลับ แสดงว่าคู่สนทนาอาจติดงานสำคัญ ขอให้หยุดการเรียกเพราะข้อความที่เรียกไปปรากฏบนจออย่างแน่นอนแล้ว

- ควรให้วาจาสุภาพ และให้เกียรติซึ่งกันและกัน การแทรกอารมณ์ขัน ควรกระทำกับคนที่รู้จักคุ้นเคยแล้วเท่านั้น

ระบบข่าวสารที่ให้บริการในสังคมอินเทอร์เน็ตมีหลายระบบ เช่น ยูสเน็ตนิวส์ (UseNet News) ระบบสมาชิกแจ้งข่าวหลายสมาคม บอกรับสมาชิกและให้ข่าวสารที่สม่ำเสมอกับสมาชิกด้วยการส่งเป็นจดหมายอิเล็กทรอนิกส์ ที่เรียกว่า Mailing lists ผู้เสนอ ข่าวและผู้อภิปรายเรื่องต่าง ๆ ที่เขียนลงไปจะกระจายออกไปทั่วโลก เช่นข่าวบนยูสเน็ตนิวส์แต่ละกลุ่มเมื่อส่งออกจะกระจาย ไปยังเซิร์ฟเวอร์อื่น ๆ ทั่วโลก ผู้ใช้บริการโดยเฉพาะที่ต้องการเขียนข่าวสารบนกระดานข่าวจะต้องเคารพกฎกติกามารยาทโดยเคร่งครัดข้อปฏิบัติที่สำคัญได้แก่

- ให้เขียนเรื่องให้กระชับ ข้อความควรสั้นและตรงประเด็นไม่กำกวม ใช้ภาษาที่เรียบง่าย สุภาพเข้าใจได้

- ในแต่ละเรื่องที่เขียนให้ตรงโดยข้อความที่เขียนควรจะมีหัวข้อเดียวต่อเรื่อง

- ในการเขียนพาดพิงถึงผู้อื่น ให้ระมัดระวังในการละเมิดหรือสร้างความเสียหายให้ผู้อื่น การให้อีเมลอาจตรงประเด็นกว่า

- ให้แหล่งที่มาของข้อความ ควรอ้างอิงแหล่งข่าวได้ ไม่เรียกว่าโคมลอยหรือข่าวลือหรือเขียนข่าวเพื่อความสนุกโดยขาดความรับผิดชอบ

- จำกัดความยาวของข่าว และหลีกเลี่ยงตัวอักษรควบคุมพิเศษอื่น ๆ เพราะหลายเครื่องที่อ่านข่าวอาจมีปัญหาในการแสดงผล

- ข่าวบางข่าวมีการกระจายกันมาเป็นลำดับ และอ้างอิงต่อ ๆ กันมา การเขียนข่าวจึงควรพิจารณาในประเด็นนี้ด้วยโดยเฉพาะอย่าส่งจดหมายตอบโต้ไปยังผู้รายงานข่าวผู้แรก

- ไม่ควรใช้เครือข่ายของมหาวิทยาลัยเพื่อประโยชน์ทางการค้าหรืองานเฉพาะของตนเพื่อประโยชน์ส่วนตนในเรื่องการค้า

- การเขียนข่าวทุกครั้งจะต้องลงชื่อ และลายเซ็นต์ ตอนล่างของข้อความเพื่อบอกชื่อ ตำแหน่งแอดเดรสที่อ้างอิงได้ทางอินเทอร์เน็ต หรือให้ที่อยู่และหมายเลขโทรศัพท์ที่ติดต่อได้

- ในการทดสอบการส่งไม่ควรทำบ่อยครั้งจนเกินไป การทดสอบควรกระทำในกลุ่มข่าวท้องถิ่นที่เปิดให้ทดสอบการส่งข่าวอยู่แล้ว เพราะการส่งข่าวแต่ละครั้งจะกระจายไปทั่วโลก

- หลีกเลี่ยงการใช้ตัวอักษรใหญ่ที่มีความหมายถึงการตะโกนหรือการแสดงความไม่พอใจในการเน้นคำให้ใช้เครื่องหมาย * ข้อความ* แทน

- ไม่ควรนำข้อความที่ผู้อื่นเขียนไปกระจายต่อโดยไม่ได้รับอนุญาตจากเจ้าของเรื่อง

- ไม่ควรใช้ข้อความตลกขบขันคำเฉพาะ คำกำกวม หรือคำหยาบคายในการเขียนข่าว

- ให้ความสำคัญในเรื่องลิขสิทธิ์ไม่ควรละเมิดลิขสิทธิ์ผู้อื่น

- ไม่ควรคัดลอกข่าวจากที่อื่นเช่น จากหนังสือพิมพ์ทั้งหมดโดยไม่มีการสรุปย่อ เมื่อส่งข่าวย่อจะต้องอ้างอิงที่มา

- ไม่ควรใช้กระดานข่าวเป็นที่ตอบโต้หรือละเมิดผู้อื่น

- เมื่อต้องการใช้คำย่อ ควรใช้คำย่อที่เป็นที่รู้จักกันทั่วไป เช่น

IMHO-in my humble / honest opinion

FYI-for your information

BTW-by the way

- การเขียนข้อความจะต้องไม่ใช้อารมณ์หรือความรู้สึกส่วนตัวและระลึกเสมอว่าข่าวที่เขียนหรืออภิปรายนี้กระจายไปทั่วโลก และมีผู้อ่านข่าวจำนวนมาก

- ในการเขียนคำถามลงในกลุ่มข่าวจะต้องส่งลงในกลุ่มที่ตรงกับปัญหาที่เขียนนั้น และเมื่อจะตอบก็ต้องให้ตรงประเด็น

- ในการบอกรับข่าวด้วย mailing list และมีข่าวเข้ามาจำนวนมากทางอีเมล์จะต้องอ่านข่าว และโอนมาไว้ที่เครื่องตน (พีซี) หรือลบออกจาก mail box และหากไม่อยู่หรือไม่ได้เปิดตู้จดหมายเกินกว่าหนึ่งสัปดาห์จะต้องส่งไปบอกยกเลิกการรับ เพื่อว่าจะได้ไม่มีจดหมายส่งเข้ามามาก

12.2 จรรยาบรรณการใช้เครือข่ายสังคมออนไลน์

- ให้ระมัดระวังในการละเมิดหรือสร้างความเสียหายให้ผู้อื่น
- ให้แหล่งที่มาของข้อความ ควรอ้างอิงแหล่งข่าวได้
- ไม่กระทำการรบกวนผู้อื่นด้วยการโฆษณาเกินความจำเป็น
- ดูแลและแก้ไขหากตกเป็นเหยื่อจากโปรแกรมอันไม่พึงประสงค์ เพื่อป้องกันมิให้คนอื่นเป็นเหยื่อต่อ

12.3 บัญญัติ 10 ประการ

- ต้องไม่ใช้คอมพิวเตอร์ทำร้าย หรือละเมิดผู้อื่น
- ต้องไม่รบกวนการทำงานของผู้อื่น
- ต้องไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลของผู้อื่น
- ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร

- ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
- ต้องมีจรรยาบรรณการใช้เครือข่ายสังคมออนไลน์
- ให้ระมัดระวังในการละเมิดหรือสร้างความเสียหายให้ผู้อื่น
- ให้แหล่งที่มาของข้อความ ควรอ้างอิงแหล่งข่าวได้
- ไม่กระทำการรบกวนผู้อื่นด้วยการโฆษณาเกินความจำเป็น
- ดูแลและแก้ไขหากตัวเองเป็นเหยื่อจากโปรแกรมอันไม่พึงประสงค์ เพื่อป้องกันมิให้คนอื่นเป็นเหยื่อต่อ