SAFETY NET

คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย สำหรับผู้ใช้งานทั่วไป

คณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

SAFETY NET คู่มือการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย สำหรับผู้ใช้งานทั่วไป

โดย คณะอนุกรรมการด้านความมั่นคง ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ISBN 974-229-720-7

พิมพ์ครั้งที่ 1 (เมษายน 2548)
จำนวน 1,000 เล่ม
เอกสารเผยแพร่

จัดทำโดย

ThaiCERT NECTEC NSTDA
โครงการเทคโนโลยีสารสนเทศเพื่อความมั่นคง
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี
112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน
ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี 12120
โทรศัพท์ 02-564-6900 โทรสาร 02-564-6901..2
URL: http://thaicert.nectec.or.th/ e-mail: thaicert@nectec.or.th

การใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย

กล่าวนำ

เครือข่ายอินเทอร์เน็ตได้กลายมาเป็นเครื่องมือสื่อสารที่สำคัญในศตวรรษที่ 21 เราจะถือได้ว่าเครือข่ายอินเทอร์เน็ตนี้เป็นการปฏิวัติครั้งสำคัญโดยจะเห็นได้จากการที่ผู้คนจำนวนกว่า 500 ล้านคนทั่วโลกเข้ามาใช้งานและมีส่วนร่วมกับเครือข่ายนี้ เครือข่ายอินเทอร์เน็ตเปลี่ยนแปลงวิถีที่เราติดต่อกับคนอื่นและกับโลกภายนอก ขณะนี้เราสามารถติดต่อและเข้าถึงผู้คน สถานที่ และข้อมูลที่เราไม่เคยสามารถติดต่อได้มาก่อน การปฏิบัติงานทางธุรกิจและราชการมีประสิทธิภาพสูงขึ้น ญาติมิตรที่อยู่ห่างไกลกันสามารถติดต่อกันได้อย่างง่ายดาย นักเรียนประถมสามารถติดต่อกับมนุษย์อวกาศในสถานีอวกาศได้ ซึ่งทั้งหมดนี้สามารถกระทำผ่านทางเครือข่ายอินเทอร์เน็ตได้ เครือข่ายอินเทอร์เน็ตนั้นได้แทรกซึมไปอยู่ทุกหนทุกแห่งและเข้ามาเกี่ยวข้องกับทุกแง่มุมในชีวิตของเรา เครือข่ายอินเทอร์เน็ตกำลังเปลี่ยนแปลงวิถีการดำเนินชีวิตของเรา

อย่างไรก็ตาม ท่านอาจจะยังมีความลังเลหรือกังวลกับการที่จะเข้าไปในเครือข่ายอินเทอร์เน็ตหรือที่เราเรียกกันว่าโลกออนไลน์ เนื่องจากมีสิ่งที่น่ากลัวต่างๆ อยู่ โดยที่ท่านอาจเคยได้ทราบเรื่องของไวรัส โทรจัน การขโมยข้อมูลส่วนตัว ความไม่ชัดเจนของกฎหมายคุ้มครองผู้บริโภคสำหรับการค้าอิเล็กทรอนิกส์ การหลอกลวงบนเครือข่าย หรือแม้แต่สิ่งที่เรียกว่าเว็บบัก (web bugs) แต่ถึงกระนั้น เครือข่ายอินเทอร์เน็ตนั้นคือวิถีทางแห่งอนาคตและในที่สุดแล้วท่านคงไม่สามารถหลีกเลี่ยงการเข้าไปเกี่ยวข้องกับโลกออนไลน์นี้ได้ และการสิ่งที่ดีที่สุดที่จะปกป้องท่านได้ก็คือการเรียนรู้ที่จะป้องกันปัญหาเหล่านี้มิให้เกิดขึ้นได้

คู่มือนี้เป็นแนวทางสำหรับทั้งผู้เริ่มต้นและผู้ที่มีประสบการณ์กับเครือข่ายอินเทอร์เน็ตในการสร้าง “ตะข่าย” หรือ เซฟตี้เน็ต (safety net) เพื่อปกป้องตัวท่านจากการหลอกลวงในโลกออนไลน์ ถึงแม้ว่าจะมีความเสี่ยงเข้ามาเกี่ยวข้องกับเรื่องทุกอย่างที่เราทำและไม่มีอะไรที่มีความปลอดภัย 100% แต่เราก็สามารถลด

ความเสี่ยงลงได้อย่างมากหากเราจะยอมเสียเวลาเล็กน้อยในการที่จะเรียนรู้วิธีการอันมิชอบต่างๆ ที่ผู้ไม่ประสงค์ดีทั้งหลายชอบใช้และใช้มาตรการป้องกันที่เหมาะสมเพื่อปกป้องตัวเราเอง ซึ่งหากท่านปฏิบัติตามคำแนะนำอย่างง่ายๆ ในคู่มือนี้ท่านจะสามารถหลีกเลี่ยงปัญหาต่างๆ ได้ก่อนที่ปัญหาเหล่านั้นจะเกิดขึ้นและการใช้เครือข่ายอินเทอร์เน็ตของท่านจะเป็นประสบการณ์ที่มีความสุขและน่าประทับใจ

โดยพื้นฐานแล้วเราควรจะต้องถามคำถาม 4 คำถามดังที่เห็นด้านล่างนี้

- เราจะทำให้เครื่องคอมพิวเตอร์ของเราปลอดภัยได้อย่างไร
- เราจะปกป้องข้อมูลส่วนตัวของเราได้อย่างไร
- เราจะเชื่อถือการซื้อขายสินค้าออนไลน์ได้หรือไม่
- เราจะหลีกเลี่ยงการหลอกลวง กับดัก และปัญหาต่างๆ ในเครือข่ายอินเทอร์เน็ตได้อย่างไร

คู่มือนี้ได้รับการจัดทำขึ้นโดยมีจุดมุ่งหมายที่จะตอบคำถามด้านบนนี้อย่างง่ายๆ และตรงไปตรงมาโดยไม่เข้าไปเกี่ยวข้องกับเรื่องทางเทคนิคหรือรายละเอียดมากเกินไป โดยคู่มือนี้จะแบ่งออกเป็น 24 หัวข้อโดยครอบคลุมประเด็นด้านความปลอดภัยต่างๆ และจัดเรียงหัวข้อตามความเกี่ยวข้องกับคำถามด้านบน ในแต่ละหัวข้อจะมีคำจำกัดความของปัญหาที่อาจเกิดขึ้น คำแนะนำสำหรับวิธีการหลีกเลี่ยงปัญหาก่อนที่ปัญหานั้นจะเกิดขึ้น และการอ้างอิงไปยังเว็บไซต์ที่เกี่ยวข้องสำหรับความช่วยเหลือหรือข้อมูลเพิ่มเติม

ท่านสามารถหาข้อมูลเพิ่มเติมและข้อมูลที่ได้รับการปรับปรุงล่าสุดในหัวข้อเหล่านี้ รวมถึงแหล่งอ้างอิงข้อมูลทางเศรษฐกิจต่างๆ สำหรับประเทศสมาชิกเอเปกได้ที่เว็บไซต์ www.aoema.org/safetynet

คณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สารบัญ

หน้า

การคุ้มครองผู้บริโภค....11
คุกกี้....13
ลายมือชื่ออิเล็กทรอนิกส์....14
ไฟร์วอลล์ส่วนตัว....16
การสวมรอยบุคคล....18
ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต....19
การละเมิดทรัพย์สินทางปัญญา....21
การถูกหลอกให้หมุนโมเด็มต่อเน็ต....22
อีเมล์หลอกลวง....24
ประเด็นทางกฎหมาย....26
การเฝ้าดูการใช้งานอินเทอร์เน็ต....27
การหมิ่นประมาทหรือการทำให้ผู้อื่นเสียชื่อเสียง....28
การไกล่เกลี่ยความขัดแย้งบนเครือข่าย....29
การถูกติดตามบนเครือข่าย....31
รหัสผ่าน....33
ความลับของข้อมูลส่วนตัว....34
การใช้งานอินเทอร์เน็ตในที่สาธารณะ....35
เว็บเพจที่มีการเสริมความปลอดภัย....36
การปรับปรุงซอฟต์แวร์....38
สแปม....39

หน้า

การปลอมแปลงอีเมล์ 41
สปายแวร์ 42
โปรแกรมโทรจัน 44
ไวรัส 46

แนวทางปฏิบัติ

แนวทางปฏิบัติสำหรับการรับส่งอีเมล์ 48
แนวทางปฏิบัติสำหรับการใช้งานเมล์ลิ่งลิสต์ 49
แนวทางการสร้างเว็บไซต์ที่แสดงถึงการประกอบการที่ดีต่อผู้บริโภค 51
แนวทางปฏิบัติในการสั่งซื้อสินค้าบนเครือข่ายอย่างปลอดภัย 53
แนวทางปฏิบัติในการประมูลสินค้าบนเครือข่าย 55

แบบทดสอบความปลอดภัย 2 นาที

ทำแบบทดสอบความปลอดภัย 2 นาทีนี้เพื่อหลีกเลี่ยงปัญหาด้านความปลอดภัยก่อนที่จะเชื่อมต่อเครือข่ายอินเทอร์เน็ต

ขณะนี้ท่านอาจจะยังไม่มีคำถามอะไร หรือท่านอาจจะคิดว่าท่านสามารถควบคุมความปลอดภัยของเครื่องคอมพิวเตอร์และทรัพยากระบบของท่านได้ แต่ถึงกระนั้นอย่างน้อยที่สุดเราขอแนะนำให้ท่านทำแบบทดสอบความปลอดภัย 2 นาทีนี้เพื่อตรวจสอบสอบว่าท่านได้พิจารณาประเด็นเรื่องความปลอดภัยที่สำคัญครบทุกด้านแล้วหรือไม่

คำถาม	ใช่	ไม่ใช่	ข้อมูลเพิ่มเติม
1. ท่านได้ติดตั้งโปรแกรมป้องกันไวรัสลงบนระบบของท่านหรือไม่			ดูหน้า 46
2. ท่านทราบหรือไม่ว่าโปรแกรมป้องกันไวรัสที่ท่านใช้นั้นเป็นเวอร์ชันล่าสุด			ดูหน้า 46
3. ท่านได้สั่งให้โปรแกรมป้องกันไวรัสของท่านปรับปรุงรายชื่อไวรัสโดยอัตโนมัติหรือไม่ (automatic update virus definitions)			ดูหน้า 46
4. ในช่วงเวลา 7 วันที่ผ่านมานี้ท่านได้ดาวน์โหลดรายชื่อไวรัสมาปรับปรุงโปรแกรมป้องกันไวรัสของท่านหรือไม่			ดูหน้า 46
5. ท่านได้ติดตั้งโปรแกรมไฟร์วอลล์ส่วนตัว (personal firewall) ลงบนระบบของท่านหรือไม่			ดูหน้า 16
6. โปรแกรมไฟร์วอลส่วนตัวของท่านเป็นเวอร์ชันล่าสุดหรือไม่			ดูหน้า 16
7. เมื่อท่านไม่ได้ใช้เครือข่ายอินเทอร์เน็ตท่านยกเลิกการเชื่อมต่อจากเครือข่าย (disconnect) หรือไม่			ดูหน้า 27
8. รหัสผ่านที่ท่านใช้ประกอบด้วยการผสมกันของตัวเลขและตัวอักษรทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่หรือไม่			ดูหน้า 34
9. ท่านได้เปลี่ยนแปลงรหัสผ่านของท่านในช่วง 30 วันที่ผ่านมาหรือไม่			ดูหน้า 33
10. ท่านสามารถจำรหัสผ่านของท่านโดยที่ไม่ต้องจดไว้หรือไม่			ดูหน้า 33
11. โปรแกรมระบบปฏิบัติการ เว็บบราวเซอร์ อีเมล์ และโปรแกรมใช้งานต่างๆ ของท่านเป็นเวอร์ชันล่าสุดหรือไม่			ดูหน้า 38

12. ท่านได้สั่งให้โปรแกรมทั้งหมดปรับปรุงตัวเองโดยอัตโนมัติ (automatic update) หรือไม่ (ถ้าสามารถสั่งได้)			ดูหน้า 38
13. ท่านทราบหรือไม่ว่าในโปรแกรมเว็บบราวเซอร์ของท่านได้มีการตั้งค่าสำหรับคุกกี้ (cookies) ไว้อย่างไร			ดูหน้า 13

หากท่านตอบว่า “ไม่ใช่” สำหรับคำถามใดคำถามหนึ่งด้านบน เป็นสิ่งสมควรอย่างยิ่งที่ท่านจะต้องเข้าไปศึกษาในหัวข้อตามหน้าที่ระบุไว้เพื่อให้เกิดความคุ้นเคยกับหัวข้อดังกล่าวมากขึ้น

ท่านจะหาคำตอบได้จากที่ใด

เราจะทำให้เครื่องคอมพิวเตอร์ของเราปลอดภัยได้อย่างไร	หาคำตอบได้จากหัวข้อ
1. จะป้องกันไม่ให้แฮกเกอร์เข้ามาในระบบคอมพิวเตอร์ได้อย่างไร	ไฟร์วอลล์ส่วนตัว หน้า 16
2. จะกันไม่ให้เด็กๆ เข้าไปดูเว็บลามกและเว็บที่มีอันตรายต่างๆ ได้อย่างไร	การเฝ้าดูการใช้งานอินเทอร์เน็ต หน้า 27
3. จะเป็นไรหรือไม่ถ้าจะใช้ชื่อสุนัขของเรามาเป็นรหัสผ่าน เพื่อจะได้จำได้ง่ายๆ	รหัสผ่าน หน้า 33
4. เพราะเหตุใดจึงต้องปรับปรุงซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดในเมื่อเราไม่ได้ต้องการความสามารถใหม่ๆ อยู่แล้ว	การปรับปรุงซอฟต์แวร์ หน้า 38
5. เป็นเรื่องจริงหรือไม่ที่มีโปรแกรมที่สามารถเข้ามาขัดขวางการทำงานของเครื่องคอมพิวเตอร์หรือสร้างปัญหาให้กับเครื่องคอมพิวเตอร์เครื่องอื่นๆ ได้	โปรแกรมโทรจัน หน้า 44
6. จะป้องกันไม่ให้ไวรัสเข้ามาในระบบคอมพิวเตอร์ได้อย่างไร	ไวรัส หน้า 47

เราจะปกป้องข้อมูลส่วนตัวของเราได้อย่างไร	หาคำตอบได้จากหัวข้อ
1. จะป้องกันไม่ให้เว็บไซต์นำเอาข้อมูลส่วนตัวจากเครื่องคอมพิวเตอร์ของเราได้อย่างไร	คุกกี้ หน้า 13
2. ห้องสนทนาเป็นที่ที่ปลอดภัยสำหรับการพบปะผู้คนและแลกเปลี่ยนข้อมูลหรือไม่	ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต หน้า 19
3. จะป้องกันไม่ให้บริษัทธุรกิจออนไลน์นำเอาข้อมูลส่วนตัวของเราไปใช้โดยที่เราไม่ทราบได้อย่างไร	ความลับของข้อมูลส่วนตัว หน้า 34
4. ในขณะที่ใช้เครือข่ายอินเทอร์เน็ตจากที่สาธารณะ เช่น ห้องสมุด หรืออินเทอร์เน็ตคาเฟ่เราจะสามารถป้องกันตัวเองได้อย่างไร	การใช้งานอินเทอร์เน็ตในที่สาธารณะ หน้า 35
5. อีเมล์ขยะเป็นสิ่งน่ารำคาญมาก แต่อีเมล์เหล่านี้สามารถก่อให้เกิดปัญหาด้านความปลอดภัยหรือไม่	สแปม หน้า 39
6. โปรแกรม “สอดแนม” ที่สามารถเข้ามาสอดแนมในเครื่องคอมพิวเตอร์นั้นมีอยู่จริงหรือไม่	สปายแวร์ หน้า 42

เราจะเชื่อถือการซื้อขายสินค้าออนไลน์ได้หรือไม่	หาคำตอบได้จากหัวข้อ
1. เราจะป้องกันตัวเองจากพวกหลอกลวงในโลกออนไลน์ได้อย่างไร	การคุ้มครองผู้บริโภค หน้า 11
2. เป็นไปได้หรือไม่ที่จะมีการลงนามในเอกสารทางกฎหมายและทำสัญญาทางการค้าแบบออนไลน์	ลายมือชื่ออิเล็กทรอนิกส์ หน้า 14
3. จะทราบได้อย่างไรว่าสิ่งใดเป็นสิ่งถูกกฎหมายหรือผิดกฎหมายในโลกออนไลน์	ประเด็นทางกฎหมาย หน้า 26
4. จะมีการไกล่เกลี่ยความขัดแย้งในการซื้อขายของออนไลน์ได้อย่างไรหากผู้ซื้อและผู้ขายอยู่กันคนละซีกโลก	การไกล่เกลี่ยความขัดแย้งบนเครือข่าย หน้า 29
5. ถ้าหากจะซื้อสินค้าจากเว็บไซต์หนึ่ง เราจะทราบได้อย่างไรว่าเว็บไซต์นั้นมีความปลอดภัย	เว็บเพจที่มีการเสริมความปลอดภัย หน้า 36

เราจะหลีกเลี่ยงการหลอกลวง กับดัก และปัญหาต่าง ๆ ในเครือข่ายอินเทอร์เน็ตได้อย่างไร	หาคำตอบได้จากหัวข้อ
1. จะมั่นใจได้อย่างไรว่าไม่มีใครนำเอาข้อมูลส่วนตัวของเราไปใช้แอบอ้างว่าเป็นตัวเรา	การสวมรอยบุคคล หน้า 18
2. สามารถนำข้อมูลต่างๆ บนเครือข่ายอินเทอร์เน็ตไปใช้ได้โดยอิสระหรือไม่	การละเมิดทรัพย์สินทางปัญญา หน้า 21
3. มีบางคนได้รับใบแจ้งค่าโทรศัพท์ที่ราคามากเกินจริง เราจะป้องกันไม่ให้เหตุการณ์นี้เกิดกับเราได้อย่างไร	การถูกหลอกให้หมุนโมเด็มต่อเน็ต หน้า 22
4. จะทราบได้อย่างไรว่าช่องทางการประกอบธุรกิจต่างๆ ที่มีอยู่ในเครือข่ายอินเทอร์เน็ตนั้นเป็นเรื่องจริงและไม่หลอกลวง	อีเมล์หลอกลวง หน้า 24
5. จะทำอย่างไรหากมีผู้กล่าวหาโจมตีว่าร้ายตัวเราหรือธุรกิจของเราบนเครือข่ายอินเทอร์เน็ต	การหมิ่นประมาทหรือการทำให้ผู้อื่นเสียชื่อเสียง หน้า 28
6. จะทำอย่างไรหากมีคนมาคอยรบกวนเราโดยการส่งอีเมล์หรือก่อกวนเราในห้องสนทนา	การถูกติดตามบนเครือข่าย หน้า 31
7. เป็นไปได้อย่างไรที่มีคนได้รับอีเมล์จากเราทั้งๆ ที่เราไม่ได้ส่งอีเมล์ไปถึงคนนั้น	การปลอมแปลงอีเมล์ หน้า 41

การคุ้มครองผู้บริโภค
(Consumer Protection)

ในการสั่งซื้อสินค้าทางอินเทอร์เน็ต ผู้บริโภคจำเป็นอย่างยิ่งที่จะต้องระมัดระวัง เช่นเดียวกับการเข้าไปซื้อของในร้านค้าทั่วไป อาทิ การรับประกันสินค้าหลังการขายเป็นอย่างไร ซื้อแล้วสามารถคืนสินค้าได้หรือไม่ หากคืนได้ให้คืนภายในกี่วัน เป็นต้น

คำแนะนำ

- ให้ศึกษาข้อมูลของบริษัทที่จะทำการสั่งซื้อสินค้า ก่อนที่จะตัดสินใจสั่งซื้อ
- ให้ตรวจสอบนโยบายการขายสินค้าของเว็บไซต์ที่ต้องการสั่งซื้อสินค้า ได้แก่ การเก็บข้อมูลส่วนบุคคลของลูกค้าไว้เป็นความลับ การรับประกันสินค้า การรับประกันความพึงพอใจของลูกค้าการคืนสินค้า ตลอดจนการสั่งซื้อสินค้าต้องมีความปลอดภัย
- ให้ตรวจสอบว่ากระบวนการสั่งซื้อสินค้าผ่านทางเว็บต้องเป็นไปอย่างปลอดภัย
- ให้ปฏิเสธไม่รับคุกกี้ (Cookies) ที่ไม่มีความจำเป็น (ให้ดูในหัวข้อ “คุกกี้” เพิ่มเติมด้วย) คุกกี้อาจเก็บข้อมูลส่วนตัวหรือข้อมูลที่บ่งบอกถึงลักษณะและความชอบส่วนตัวรวมไปถึงข้อมูลอื่นๆ ของผู้ใช้งานเว็บบราวเซอร์
- ให้ติดตั้งโปรแกรมอุดช่องโหว่ให้กับเว็บบราวเซอร์ที่ใช้งาน เพื่อให้บราวเซอร์มีความปลอดภัย
- ให้ตรวจสอบและทำความเข้าใจในกระบวนการส่งสินค้าและการคืนสินค้า
- หากบนเว็บไซต์มี FAQ (Frequently Asked Questions) ให้อ่าน FAQ อย่างละเอียด
- ในการให้ข้อมูลส่วนตัวเพื่อประกอบกระบวนการสั่งซื้อสินค้าผ่านทางเว็บไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น
- ไม่เปิดเผยรหัสผ่านในการเข้าเว็บไซต์ให้กับบุคคลหนึ่งบุคคลใดทราบ

- เก็บรายละเอียดข้อมูลเกี่ยวกับการสั่งซื้อไว้ทั้งหมด อาทิ ก่อนจบกระบวนการสั่งซื้อ อาจมีหน้าเว็บที่บอกรายละเอียดของสินค้าที่สั่งซื้อนั้น ให้ทำการบันทึกข้อมูลนั้นเก็บไว้ในเครื่องคอมพิวเตอร์ของเราเอง หรือเก็บอีเมล์ที่ยืนยันการสั่งซื้อสินค้าของเราเอาไว้ เมื่อพบปัญหาเกิดขึ้นในภายหลัง เช่น สินค้าไม่ตรงตามที่สั่งซื้อ จำนวนเงินที่จะต้องชำระทางบัตรเครดิตไม่ถูกต้อง เป็นต้น จะได้ใช้ข้อมูลที่บันทึกเก็บไว้นั้นเป็นหลักฐานได้
- ให้ตรวจสอบ Statements บัตรเครดิตที่ทางธนาคารส่งมาให้เป็นประจำ เช่น ทุกเดือน เพื่อดูว่าเกิดความผิดพลาดใดๆ หรือมีการใช้บัตรเครดิตโดยบุคคลอื่นหรือไม่ และเมื่อพบความผิดพลาด ให้ดำเนินการแจ้งธนาคารโดยทันที
- ให้ระมัดระวังบริษัทที่โอ้อวดเกินความเป็นจริง
- ให้ตรวจสอบเงื่อนไขการสั่งซื้อให้ชัดเจน เช่น การคืนสินค้า การคืนเงิน การประกันสินค้า การส่งสินค้า เป็นต้น
- ให้ใช้บัตรเครดิตในการสั่งซื้อมากกว่าบัตรเดบิต เพราะเมื่อมีการสั่งซื้อด้วยบัตรเดบิต เงินในบัญชีของบัตรเดบิตจะถูกหักออกทันที ซึ่งจะทำให้เกิดความยุ่งยากในการแก้ไขปัญหาที่อาจตามมาในภายหลัง
- หากเป็นไปได้ ให้ทำการตรวจสอบกฎหมายการคุ้มครองสิทธิผู้บริโภคด้วย

แหล่งข้อมูลเพิ่มเติม

www.econsumer.gov

www.bbbonline.org

คุกกี้ (Cookies)

คุกกี้คือข้อมูลที่เก็บไว้ในเว็บบราวเซอร์ซึ่งเก็บข้อมูลส่วนบุคคล ข้อมูลความสนใจส่วนตัวในสินค้าบางประเภท หรืออาจเป็นข้อมูลอื่นๆ ที่เกี่ยวข้องกับผู้ใช้งานบราวเซอร์ ข้อมูลนี้อาจจะได้รับการติดตั้งลงไปในเครื่องในขณะที่ผู้ใช้งานบราวเซอร์ทำการท่องเว็บเข้าไปในเว็บไซต์ใดเว็บไซต์หนึ่ง ในครั้งถัดไปเมื่อผู้ใช้เข้าไปในเว็บไซต์นั้นอีกครั้ง หน้าเว็บที่ปรากฏต่อสายตาจะได้รับการปรับแต่งให้ตรงกับความสนใจหรือความชอบส่วนตัวของผู้ใช้นั้น

ตัวอย่างเช่น ผู้ใช้ที่เข้าไปซื้อหนังสือกับทางเว็บไซต์แห่งหนึ่งและได้ทำการเลือกซื้อหนังสือที่อยู่ในความสนใจจำนวนหนึ่ง ในระหว่างที่ทำการซื้ออยู่นั้นคุกกี้ซึ่งเก็บข้อมูลส่วนตัวของท่าน รวมทั้งประเภทหนังสือที่ท่านสนใจ อาจได้รับการติดตั้งลงไปในเครื่องคอมพิวเตอร์ของท่าน และในครั้งถัดไปเมื่อท่านเข้าใช้เว็บไซต์นี้อีกครั้งหนึ่ง หน้าตาเว็บเพจอาจจะแสดงการต้อนรับและมีชื่อของท่านปรากฏอยู่ที่ด้านบนของบราวเซอร์ รวมทั้งอาจมีรายการหนังสือใหม่ๆ ที่อาจจะอยู่ในความสนใจของท่านแสดงให้ดูด้วย

คุกกี้เป็นจำนวนมากเป็นคุกกี้ที่ถือได้ว่าไม่มีพิษไม่มีภัยจึงเป็นที่ยอมรับได้

เช่น ในกรณีของคุกกี้ที่เกิดจากการเข้าไปสั่งซื้อหนังสือดังกล่าว แต่ก็มีคุกกี้อีกเป็นจำนวนไม่น้อยที่ถือได้ว่าละเมิดสิทธิส่วนบุคคลรวมทั้งสร้างความรำคาญให้แก่ผู้ใช้ด้วย คุกกี้ประเภทหลังนี้เรียกกันว่า Third-Party Cookies ซึ่งอาจเกิดจากการที่ผู้ใช้เข้าไปท่องเว็บแห่งหนึ่งซึ่งมีผู้โฆษณาอื่นๆ ได้ทำการโฆษณาสินค้าของตนไว้บนเว็บนั้นด้วย ผู้โฆษณาเหล่านั้น (ซึ่งถือได้ว่าเป็นพวก Third Party) อาจจะพยายามที่จะเรียนรู้และเก็บข้อมูลความสนใจของผู้ใช้นั้นเป็นคุกกี้ลงไปยังเครื่องของผู้ใช้โดยที่ผู้ใช้เองหลายๆ ครั้งจะไม่ต้องการให้ติดตั้งคุกกี้นั้นลงไปในเครื่องของตน คุกกี้ประเภทนี้จะก่อให้เกิดหน้าจอเล็กๆ ที่ Pop-Up เป็นโฆษณาขึ้นมาเป็นจำนวนมากที่ไม่ได้อยู่ในความสนใจหรือความต้องการของผู้ใช้เลย

คำแนะนำ

- ให้ใช้โปรแกรมเพื่อควบคุมหรือกำจัดคุกกี้ที่ไม่พึงประสงค์ซึ่งสามารถดาวน์-โหลดได้จากเว็บ www.cookiecentral.com และ www.lavasoft.de
- ให้ตรวจสอบดูนโยบายการขายสินค้าของเว็บไซต์ที่อยู่ในความสนใจ เพื่อดูว่าได้มีการกล่าวถึงการนำข้อมูลในคุกกี้ (ซึ่งเป็นข้อมูลส่วนบุคคลของผู้ใช้) ไปใช้งานอย่างไร เว็บไซต์ที่ดีและซื่อตรงต่อลูกค้าควรจะได้มีการกล่าวถึงในเรื่องนี้อย่างชัดเจน
- ให้ตรวจสอบการปรับแต่งค่าของคุกกี้เพื่อให้ตรงกับความต้องการใช้งานให้มากที่สุด สำหรับบราวเซอร์ IE ให้เข้าไปที่ “Tools”, “Internet Options”และตามด้วย “Privacy” เสร็จแล้วให้ทำการปรับแต่งค่าให้ตรงกับความต้องการใช้งานให้มากที่สุด

แหล่งข้อมูลเพิ่มเติม

www.cookiecentral.com

www.lavasoft.de

ลายมือชื่อดิจิทัล (Digital Signature)

เอกสารกระดาษในสำนักงานทั่วไป เช่น จดหมายบันทึกหรืออื่นๆ ที่ต้องการการรับรองจากผู้ส่ง จะต้องมีการลงลายมือชื่อของผู้ส่งเอาไว้ เพื่อเป็นการรับรองหรือยืนยันว่าข้อความที่ปรากฏนั้นมาจากผู้ส่งดังกล่าว ในโลกแห่งคอมพิวเตอร์เราก็มีวิธีลงลายมือชื่อเช่นเดียวกัน ซึ่งเราเรียกกันว่า “Digital Signature” หรือลายมือชื่อดิจิทัล ในประเทศไทยเราในอนาคตอันไม่ไกลนี้ คาดว่าจะได้มีการใช้งานกันอย่างแพร่หลายมากยิ่งขึ้น

ลายมือชื่อดิจิทัลดังกล่าวนี้จะแตกต่างกันกับสแกนลายมือชื่อของเราจากกระดาษแล้วนำมาเก็บไว้ในเครื่องคอมพิวเตอร์ ลายมือชื่อแบบหลังนี้เรียกว่า

“Digitized Signature” ซึ่งในทางกฎหมายแล้วไม่สามารถใช้เป็นเครื่องผูกพันกับเจ้าของลายมือชื่อได้

การใช้ลายมือชื่อดิจิทัลจำเป็นต้องมีคู่กุญแจซึ่งถูกสร้างขึ้นมาจากสมการทางคณิตศาสตร์ที่ซับซ้อน คู่กุญแจประกอบไปด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) กุญแจส่วนตัวนี้จะต้องเก็บไว้กับผู้เป็นเจ้าของเท่านั้น ห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาดและใช้ในการลงลายมือชื่อดิจิทัลกับเอกสารอิเล็กทรอนิกส์ต่างๆ เพื่อเป็นการรับรองเอกสารนั้น เช่น อีเมล์ เป็นต้น ส่วนกุญแจสาธารณะในจุดประสงค์หนึ่งจะเอาไว้ใช้ในการตรวจสอบว่าเอกสารอิเล็กทรอนิกส์ที่ส่งมานั้นเป็นเอกสารที่ส่งมาจากเจ้าของกุญแจส่วนตัวหรือไม่ รวมทั้งกุญแจสาธารณะที่เป็นคู่ของกุญแจส่วนตัวจะสามารถเปิดดูเอกสารนั้นได้ โดยปกติกุญแจสาธารณะจะสามารถดาวน์โหลดได้จากทางเว็บไซต์หรือไม่ก็ได้รับทางอีเมล์

การรับรองกุญแจทั้งสองอย่างเป็นทางการโดยปกติจะต้องมีหน่วยงานที่ทำหน้าที่นี้ หน่วยงานนี้จะมีชื่อเรียกกันว่า Certificate Authority หรือ CA ซึ่งทำหน้าที่ออกใบรับรองอิเล็กทรอนิกส์ (Electronic Certificate) ให้กับผู้ร้องขอพร้อมทั้งให้การรับรองกุญแจทั้งสองด้วย (เช่นเดียวกับที่ว่าการอำเภอซึ่งทำหน้าที่ออกบัตรประชาชนให้แก่ผู้ร้องขอ) การออกใบรับรองนี้จะต้องได้รับการลงนามรับรองด้วยลายมือชื่ออิเล็กทรอนิกส์ของ CA โดยปกติใบรับรองจะอยู่คู่กับกุญแจสาธารณะ แต่สำหรับกุญแจส่วนตัวผู้เป็นเจ้าของเท่านั้นจะต้องเก็บไว้และห้ามเปิดเผยโดยเด็ดขาด

นอกจากการลงนามโดยผู้เป็นเจ้าของกุญแจส่วนตัวเพื่อส่งเอกสารอิเล็กทรอนิกส์ไปให้แก่ผู้รับ (ซึ่งจะต้องถือกุญแจสาธารณะไว้) ผู้รับยังสามารถส่งเอกสารอิเล็กทรอนิกส์ของตนกลับไปให้กับผู้ส่ง (ซึ่งถือกุญแจส่วนตัว) ได้โดยใช้กุญแจสาธารณะเพื่อเข้ารหัสเอกสารนั้น แล้วจึงส่งไปให้แก่ผู้ส่ง วิธีการเข้ารหัสนี้จะทำให้ไม่มีผู้อื่นสามารถเปิดอ่านเอกสารนี้ได้ ยกเว้นผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้น

คำแนะนำ

- ห้ามเปิดเผยกุญแจส่วนตัวของตนให้กับผู้อื่นทราบโดยเด็ดขาด

แหล่งข้อมูลเพิ่มเติม

www.apectelwg.org/apecdata/telwg/eaTG/crypto.html

searchsecurity.techtarget.com

ไฟร์วอลล์ส่วนตัว (Personal Firewall)

ไฟร์วอลล์ส่วนตัวคือซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัว ซึ่งทำหน้าที่ช่วยป้องกันผู้บุกรุกหรือผู้ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ ส่วนตัวของเรา หรือช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดีทั้งหลาย เช่น ไวรัส โทรจัน สปายแวร์ ถูกติดตั้งลงไปในเครื่องคอมพิวเตอร์ส่วนตัวโดยที่เราเองอาจไม่ทราบหรือไม่รู้ตัว

ไฟร์วอลล์ทำงานโดยทำการตรวจสอบข้อมูลทั้งหมด (ไวรัส โทรจัน สปาย-แวร์ ก็ถือเป็นข้อมูลด้วย) ที่เข้าหรือออกจากเครื่องคอมพิวเตอร์ส่วนตัว และจะอนุญาตให้ผ่านไปได้ก็ต่อเมื่อตรวจสอบแล้วและพบว่าไม่ละเมิดกับกฎเกณฑ์ของไฟร์วอลล์ที่กำหนดไว้ ในทางตรงกันข้ามหากมีการละเมิด ไฟร์วอลล์ก็จะไม่อนุญาตให้ผ่านไป

ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลอาจคิดว่าเครื่องของตนไม่มีทรัพย์สินหรือข้อมูลใดๆ ที่จะเป็นประโยชน์ต่อผู้บุกรุก ดังนั้นจึงไม่มีเหตุผลที่จะบุกรุกเข้ามา แต่มีเหตุผลอยู่อีกจำนวนหนึ่งดังนี้ ซึ่งมีความสำคัญที่ผู้ใช้อาจต้องทบทวนความคิดนี้ใหม่อีกครั้ง

- **การทำลายทรัพย์สินสารสนเทศให้เสียหาย**
  เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกอาจทำให้เครื่องคอมพิวเตอร์นั้นเกิดความเสียหายได้ เช่น ทำให้เครื่องบูตไม่ได้

- **การขโมยข้อมูลในเครื่องคอมพิวเตอร์**
  เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกอาจทำการขโมยข้อมูลที่สำคัญๆ ของผู้ใช้งาน ได้แก่ บัญชีผู้ใช้ (account) และรหัสผ่าน (Password) ข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผย หรือข้อมูลสำคัญอื่นๆ
- **การจู่โจมเครื่องคอมพิวเตอร์อื่นบนอินเทอร์เน็ต**
  เมื่อบุกรุกเข้ามาได้แล้ว ผู้บุกรุกจะใช้เครื่องของผู้ใช้นั้นเพื่อทำการบุกรุกเครื่องคอมพิวเตอร์อื่นๆต่อไป หรือเพื่อทำการส่งสแปมเมล์ออกไป

มีซอฟต์แวร์ทูล (Software Tool) บนอินเทอร์เน็ตมากมายที่ผู้บุกรุกสามารถดาวน์โหลดมาใช้งานได้ เช่น ทูลประเภทที่สามารถสแกนหาเครื่องคอมพิวเตอร์ที่ต่ออินเทอร์เน็ตอยู่ รวมทั้งช่องทางการสื่อสารคอมพิวเตอร์ที่เปิดอยู่หรือที่เรียกกันว่ามีพอร์ต (Port) เปิดอยู่ ซึ่งผู้บุกรุกสามารถใช้เป็นทางเข้าไปสู่เครื่องคอมพิวเตอร์ของผู้ใช้ได้ เมื่อเข้าไปได้แล้ว ผู้บุกรุกจะสามารถสร้างความเสียหายทั้งสามนั้นได้

คำแนะนำ

- ให้ตัดการเชื่อมต่อจากอินเทอร์เน็ตทันทีที่ไม่มีการใช้งานเครื่องคอมพิวเตอร์ส่วนตัว
- ให้ติดตั้งไฟร์วอลล์ส่วนตัวโดยสามารถดาวน์โหลดได้จากเว็บ

  www.zonelabs.com

  www.symantec.com

  www.sygate.com

แหล่งข้อมูลเพิ่มเติม

www.zonelabs.com

www.symantec.com

www.sygate.com

การสวมรอยบุคคล (Identity Theft)

การขโมยเอกสารสำคัญที่ใช้ในการระบุตัวตน เช่น บัตรประจำตัวประชาชน และกระทำการฉ้อฉลต่อเอกสารดังกล่าว หรือแม้กระทั่งปลอมแปลงเอกสารสำคัญนั้น ถือเป็นคดีที่มีความผิดทางกฎหมาย โดยที่ผู้กระทำฉ้อฉลนั้นมักจะมีแรงจูงใจทางด้านการเงินเป็นเหตุผลสำคัญ

ในปัจจุบันการขโมยและการกระทำการฉ้อฉลนั้นสามารถกระทำได้กับเอกสารอิเล็กทรอนิกส์ที่อยู่ในเครื่องคอมพิวเตอร์ (นอกเหนือจากการขโมยและการกระทำการฉ้อฉลกับเอกสารกระดาษที่เกิดขึ้นอยู่แล้ว) ซึ่งเป็นเรื่องที่จะมีความสำคัญเพิ่มมากขึ้นเรื่อยๆ ทั้งนี้เนื่องจากในปัจจุบันเอกสารสำคัญที่ใช้ระบุตัวตนมากมายได้ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์และอาจเข้าถึงได้ อาทิ โดยผู้บุกรุกโดยผ่านเครือข่ายอินเทอร์เน็ต

การขโมยเอกสารสำคัญนั้น เมื่อเกิดขึ้นแล้ว อาจนำไปสู่การสวมรอยเป็นตัวบุคคลผู้เป็นเจ้าของเอกสารนั้น และอาจใช้ในการดำเนินการเรื่องต่างๆ แทนตัวผู้เป็นเจ้าของโดยมิได้รับมอบหมายซึ่งเป็นการกระทำที่ผิดกฎหมาย เช่น การขโมยบัญชีผู้ใช้และรหัสผ่าน (Password) เพื่อทำการล็อกอินเข้าไปซื้อสินค้าในเว็บแห่งหนึ่ง ผลที่จะเกิดขึ้นต่อผู้ที่ถูกสวมรอย ได้แก่ เสียประวัติทางด้านการเงิน ก่อให้เกิดหนี้สินมากมาย ต้องคดีที่มิได้เป็นผู้ก่อ เสียชื่อเสียง และอื่นๆ

แหล่งข้อมูลเพิ่มเติม

www.idtheftcenter.org

www.privacyrights.org/identity.htm

www.consumer.gov/idtheft/

คำแนะนำ

- ให้ระมัดระวังไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น ซึ่งรวมถึงเลขที่บัตรต่างๆ เช่น บัตรประจำตัวประชาชน บัตรเครดิต ใบขับขี่ บัตรประจำตัวผู้เสียภาษีอากร เป็นต้น หมายเลขดังกล่าวในหลายๆ กรณี จะถูกใช้เป็นข้อมูล

สำคัญในการล็อกอินเข้าสู่เว็บไซต์ หรือจะถูกสอบถามทางโทรศัพท์ก่อนที่เจ้าหน้าที่ของธนาคารจะเปิดเผยข้อมูลทางการเงินของผู้สอบถามให้ทราบ

- ให้ระมัดระวังข้อมูลบัญชีธนาคารหรือข้อมูล Statement รายเดือนที่ธนาคารส่งมา มิให้เปิดเผยหรือล่วงรู้โดยไม่มีความจำเป็น
- ให้ระมัดระวังการให้ข้อมูลเกี่ยวกับบัตรเครดิต จะให้ก็ต่อเมื่อมีความจำเป็นจริงๆ เท่านั้น
- ในกรณีที่ต้องให้ตัวบัตรเครดิตแก่ผู้ขาย เช่น ที่สถานีเติมน้ำมันเชื้อเพลิง ให้คอยจับตาดูพฤติกรรมการนำบัตรนั้นไปรูดเพื่อชำระเงิน
- ในการซื้อสินค้าทางเว็บ นอกจากระมัดระวังการให้ข้อมูลบัตรเครดิตแล้ว ต้องตรวจสอบก่อนที่จะสั่งซื้อว่าการประมวลผลการสั่งซื้อของเว็บนั้นมีความปลอดภัยพอเพียงหรือไม่ (การประมวลผลที่ไม่ปลอดภัยอาจนำไปสู่การแอบดักดู ข้อมูลส่วนตัวของผู้ซื้อได้)
- ให้ยกเลิกบัญชีธนาคารที่ไม่ได้มีการใช้งานมาเป็นระยะเวลานาน เช่น นานกว่า 6 เดือน
- ให้ระมัดระวังไม่ให้ผู้อื่นซึ่งอาจยืนอยู่ในบริเวณข้างเคียง เห็นรหัสผ่านของบัตร ATM ส่วนตัว
- ให้ใช้รหัสผ่านที่ยากต่อการเดาและเปลี่ยนรหัสผ่านบ่อยๆ
- หมั่นตรวจตรา Statement ทางการเงินที่ได้รับจากธนาคารเพื่อดูว่ามีความผิดปกติเกิดขึ้นในบัญชีธนาคารของเราหรือไม่

ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต (Instant Messaging, Chat Rooms, File Sharing)

การสนทนากันบนอินเทอร์เน็ตทำได้หลายวิธี วิธีการหนึ่งคือการสนทนาบนเว็บ ซึ่งจะมีการจัดเป็นห้องสนทนาบนเว็บไว้ให้ โดยวิธีนี้ผู้ใช้มีเพียงเว็บบราวเซอร์ก็สามารถเข้าไปสนทนาในห้องสนทนาที่จัดไว้ให้ได้ วิธีที่สองคือการใช้โปรแกรม Instant Relay Chat (IRC) ซึ่งทำให้ผู้ใช้จำเป็นต้องติดตั้งโปรแกรม IRC ก่อนที่จะใช้

งานได้ โปรแกรมดังกล่าวอาจดาวน์โหลดได้จากทางเว็บหรือไม่ก็ต้องทำการจัดซื้อมาแล้วทำการติดตั้ง

การส่งข้อความฉับพลันหรือที่เรียกกันว่า Instant Messaging เป็นวิธีการสนทนาอีกรูปแบบหนึ่งซึ่งผู้ใช้ต้องทำการติดตั้งโปรแกรมก่อนใช้งานเช่นกัน โปรแกรมนี้จะทำให้ผู้ใช้สามารถสนทนากับเพื่อนที่ล็อกอินเข้ามาใช้งานได้อย่างทันทีทันใด รวมทั้งจะอนุญาตให้ผู้ใช้เก็บรายชื่อของเพื่อนที่มีความสนใจร่วมกันหรือเรามักสนทนาด้วยกันบ่อยๆ เอาไว้ในโปรแกรมและยังสามารถตรวจสอบดูได้ว่ามีเพื่อนคนใดบ้าง ณ ขณะนี้ที่ได้ทำการล็อกอินเข้ามาแล้ว

ทั้งการสนทนาในห้องสนทนาและการใช้ข้อความฉับพลันได้มีการใช้งานกันอย่างแพร่หลายในธุรกิจหลากหลายประเภท ไม่ว่าจะเป็นภาครัฐหรือภาคเอกชน ถึงแม้ว่าการสนทนาในทั้งสองรูปแบบจะมีประโยชน์มากในการแลกเปลี่ยนความคิดเห็นหรือข้อมูลต่างๆ กัน ทว่าหากมิได้เตรียมการป้องกันไว้ให้ดีแล้ว ผลในทางลบก็อาจเกิดขึ้นได้ เช่น การติดไวรัสหรือโทรจันในเครื่องของผู้ที่รับไฟล์ที่ส่งมาให้ การเปิดเผยข้อมูลส่วนตัว เป็นต้น

การแชร์ไฟล์ระหว่างเพื่อนบนอินเทอร์เน็ตเป็นรูปแบบหนึ่งของการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต (การสนทนาทั้งสองประเภทที่ได้กล่าวถึงไปแล้วนั้นก็อาจนำไปสู่การแลกเปลี่ยนข้อมูลระหว่างผู้ใช้ด้วย) ซึ่งหากไม่ได้เตรียมการป้องกันไวรัสไว้ให้ดีแล้ว อาจเปิดโอกาสให้ผู้บุกรุกเข้ามานำไฟล์ในเครื่องของผู้ใช้งานไปได้ หรือแม้แต่เครื่องคอมพิวเตอร์ที่ใช้งานได้รับความเสียหายได้ โปรแกรมสำหรับการแชร์ไฟล์นี้ ได้แก่ Kazaa, Morpheus, LimeWire เป็นต้น ซึ่งจะทำให้สามารถเข้าไปเอาไฟล์ในเครื่องของเพื่อนได้โดยตรง

คำแนะนำ

- ให้หลีกเลี่ยงไม่ใช้งานทั้งการส่งข้อความฉับพลัน การสนทนาในห้องสนทนาและการแชร์ไฟล์บนอินเทอร์เน็ต ทั้งนี้เนื่องจากวิธีการทั้งสามนี้อาจก่อให้เกิด

การละเมิดความเป็นส่วนตัว การติดตั้งโปรแกรมที่ไม่ประสงค์ดี และการแพร่กระจายของไวรัสได้ ถ้าจำเป็นต้องใช้ ให้ทำการศึกษาให้ดีก่อนเริ่มต้นใช้งาน

- ให้ติดตั้งไฟร์วอลล์ส่วนบุคคล
- ให้ติดตั้งโปรแกรมป้องกันไวรัสและหมั่นทำการปรับปรุงไฟล์รูปแบบไวรัสอย่างสม่ำเสมอ
- สำหรับการแชร์ไฟล์ ให้ตรวจสอบการปรับแต่งค่าที่ใช้งานในโปรแกรมแชร์ไฟล์และให้แชร์เฉพาะไฟล์ที่ตนต้องการให้ผู้อื่นได้รับทราบข้อมูลจริงๆ
- ให้ระมัดระวังการไม่ละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของไฟล์

แหล่งข้อมูลเพิ่มเติม

www.tio.com.au/FAQ/int_dumping.htm

การละเมิดทรัพย์สินทางปัญญา (Intellectual Property Rights)

ทรัพย์สินทางปัญญาหมายถึงสิ่งที่มีคุณค่าที่เกิดจากการประดิษฐ์คิดค้นของมนุษย์ ในโลกแห่งอินเทอร์เน็ตผู้ใช้จะได้ประสบกับทรัพย์สินทางปัญญาอย่างมากมายที่มีอยู่บนอินเทอร์เน็ต เช่น ซอฟต์แวร์ หนังสือ ภาพกราฟิก ภาพศิลปะ ภาพยนตร์ ดนตรี ภาพถ่าย เป็นต้น ซึ่งเป็นสิ่งที่ถ่ายทอดจากสติปัญญาหรือความคิดของมนุษย์ ไปสู่ผลงานดังกล่าวในรูปแบบของไฟล์อิเล็กทรอนิกส์

การนำทรัพย์สินทางปัญญาดังกล่าวที่ผู้ใช้พบในขณะทำการท่องเว็บมาใช้งานจำเป็นต้องมีการตรวจสอบอย่างรอบคอบก่อนว่าจะมีการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือการละเมิดอื่นๆ หรือไม่ รวมทั้งผู้ใช้จะต้องตระหนักและทำความเข้าใจกฎหมายที่เกี่ยวข้องกับทรัพย์สินทางปัญญา ทั้งที่เป็นกฎหมายของประเทศและกฎหมายในระดับนานาชาติด้วย

คำแนะนำ

- ให้ระมัดระวังไม่ละเมิดทรัพย์สินทางปัญญาไม่ว่าจะเป็นของบุคคลหรือขององค์กรหนึ่งก็ตาม การละเมิดที่อาจเกิดขึ้น ได้แก่ การนำภาพกราฟิกมาใช้งานก่อนที่จะได้รับอนุญาต การขโมยความคิดของผู้อื่นมาเป็นของตน การแชร์ไฟล์ดนตรีที่มีลิขสิทธิ์ เป็นต้น

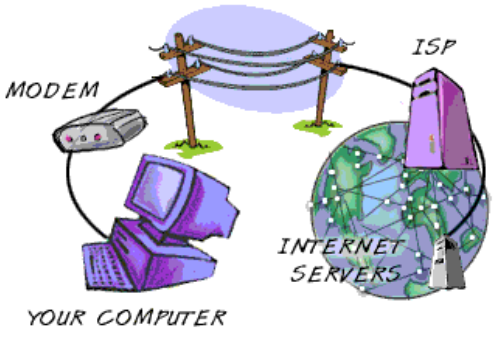
แหล่งข้อมูลเพิ่มเติม

www.wipo.int

www.apecipeg.org

การถูกหลอกให้หมุนโมเด็มต่อเน็ต
(Internet Dumping or Modem Hijacking)

Internet Dumping หรือ Modem Hijacking คือ การที่โปรแกรมหนึ่งที่ผู้ใช้ดาวน์โหลดมาใช้งาน ตัดการเชื่อมต่อกับอินเทอร์เน็ตที่ผู้ใช้กำลังใช้งานอยู่โดยผ่านทางโมเด็ม แล้วหมุนผ่านโมเด็มนั้นเข้าไปที่เบอร์โทรศัพท์อีกเบอร์หนึ่งเพื่อต่ออินเทอร์เน็ต ซึ่งอาจเป็นเบอร์ในต่างประเทศหรือเป็นเบอร์โทรศัพท์ที่เมื่อโทรเข้าไปแล้วจะถูกคิดค่าใช้จ่ายทันที ในกรณีส่วนใหญ่ที่เกิดขึ้นผู้ใช้จะไม่รู้ตัวว่าตนเองได้ถูกตัดการเชื่อมต่อกับอินเทอร์เน็ตที่ตนเองใช้งานอยู่ตามปกติและหมุนเข้าไปที่อีกเบอร์โทรหนึ่ง จนกระทั่งได้รับบิลค่าโทรศัพท์ที่เกิดจากการหมุนเข้าไปที่เบอร์โทรเหล่านั้น ณ ขณะที่ได้รับบิลนั้นผู้ใช้อาจคิดว่าเป็นค่าใช้จ่ายที่น่าจะผิดพลาดหรือไม่ควรจะเป็นค่าใช้จ่ายของตน



การถูกหลอกนี้ส่วนใหญ่จะมีสาเหตุมาจากเว็บไซต์สำหรับผู้ใหญ่ประเภทเว็บภาพอนาจารได้พยายามที่จะหลอกล่อให้ผู้ใช้นั้นเข้าไปในเว็บของตนโดยผ่านทางเบอร์โทรศัพท์อีกเบอร์หนึ่งซึ่งจะมีการคิดค่าบริการจากการเข้าไปดู เมื่อผู้ใช้หลงเชื่อก็จะทำการดาวน์โหลดโปรแกรมสำหรับดูเว็บนั้นเข้ามาติดตั้งในเครื่องของตน โดยปกติก่อนการดาวน์โหลดโปรแกรมมาใช้งาน เงื่อนไขจะประกอบด้วยการใช้เบอร์โทรศัพท์อีกเบอร์หนึ่งเพื่อต่ออินเทอร์เน็ตเข้าไปดูเว็บนั้น เมื่อผู้ใช้ไม่ได้สนใจที่จะอ่านเงื่อนไขเหล่านั้นอย่างรอบคอบ ก็จะดาวน์โหลดโปรแกรมมาและเริ่มต้นใช้งานทันที ซึ่งจะก่อให้เกิดเป็นค่าใช้จ่ายในบิลโทรศัพท์นั่นเอง การขอยกเลิกบิลค่าโทรศัพท์นี้โดยทั่วไปจะไม่สามารถทำได้ ทั้งนี้เนื่องจากผู้ใช้ได้ทำการตกลงยอมรับในเงื่อนไขนั้นแล้ว

คำแนะนำ

- ให้ความรู้แก่บุตรหลาน พนักงาน หรือผู้ใช้คอมพิวเตอร์ เกี่ยวกับปัญหาการถูกหลอกให้ต่ออินเทอร์เน็ตนี้ เพื่อที่จะไม่หลงเชื่อและตกเป็นเหยื่อของเว็บไซต์ดังกล่าว
- ให้เปิดเสียงของโมเด็มไว้ เพื่อเอาไว้คอยสังเกตว่ามีเสียงของการหมุนโมเด็มใหม่เกิดขึ้นหรือไม่
- ให้เก็บ “History” ในเว็บบราวเซอร์ ซึ่งเก็บรายชื่อของเว็บไซต์ที่เข้าไปเยือนไว้ให้มากที่สุดเท่าที่จะทำได้ เมื่อมีปัญหาเกิดขึ้น จะได้สามารถย้อนกลับเข้าไปที่เว็บนั้นได้อีกครั้งหนึ่ง
- ให้ล็อกการโทรศัพท์ออกต่างประเทศจากเครื่องโทรศัพท์ที่ใช้งาน หรือล็อกเฉพาะเบอร์โทรศัพท์ที่ขึ้นต้นด้วยหมายเลขพิเศษ
- ให้ระมัดระวังที่จะอ่านเงื่อนไขโดยละเอียดก่อนที่จะเข้าชมเว็บไซต์สำหรับผู้ใหญ่

แหล่งข้อมูลเพิ่มเติม

www.tio.com.au/FAQ/int_dumping.html

อีเมล์หลอกลวง (Instant Scams)

ในปัจจุบันได้มีอีเมล์ประเภทหลอกลวงให้ผู้ที่ได้รับอีเมล์หลงเชื่อซึ่งหลายๆ ครั้งจะทำให้ผู้รับอีเมล์ได้รับความเสียหาย เช่น เสียเงิน เสียเวลา และจะเป็นการยากที่จะเรียกร้องหรือขอกลับคืนเมื่อได้เสียไปแล้ว ในปัจจุบันองค์กร Federal Trade Commision (FTC) ของสหรัฐอเมริกาได้ระบุอีเมล์ประเภทหลอกลวงนี้ไว้ 12 ประเภท ซึ่งผู้ใช้ต้องให้ความระมัดระวัง

1. การสร้างโอกาสทางธุรกิจ อีเมล์ประเภทนี้จะเสนอรายได้ก้อนใหญ่โดยที่ไม่ต้องทำอะไรมากหรือไม่มีค่าใช้จ่ายในการลงทุน
2. อีเมล์ขายสินค้าที่มีกลุ่มผู้ใช้งานเป็นจำนวนมาก (Bulk E-mail) อีเมล์ประเภทนี้จะเสนอรายชื่อกลุ่มผู้ใช้งานอีเมล์ซึ่งมีเป็นจำนวนมากและชักชวนว่าสามารถโฆษณาหรือขายสินค้าลงไปยังกลุ่มผู้ใช้งานอีเมล์นี้ได้ ผู้ให้บริการอินเทอร์เน็ตส่วนใหญ่จะไม่อนุญาตอีเมล์ขายสินค้าในลักษณะเช่นนี้
3. อีเมล์ลูกโซ่ อีเมล์ประเภทนี้จะชักชวนให้ผู้รับส่งเงินจำนวนเล็กน้อยไปยังผู้ส่งและส่งต่ออีเมล์นี้ไปให้เพื่อนหรือผู้อื่นต่อไป
4. การทำงานที่บ้านโดยลงแรงเพียงเล็กน้อย (Work-at-home Schemes) อีเมล์ประเภทนี้จะเสนอการมีรายได้อย่างสม่ำเสมอโดยลงแรงเพียงเล็กน้อย ผู้รับอีเมล์จะต้องจ่ายค่าธรรมเนียมแรกเข้าและทำงานตามที่ในอีเมล์ขอให้ทำ (โดยหวังจะได้รับค่าตอบแทนก้อนใหญ่) แต่ผู้รับก็จะไม่มีทางได้รับค่าตอบแทนใดๆ ทั้งสิ้นกลับคืน
5. การรักษาสุขภาพและการควบคุมน้ำหนัก อีเมล์ประเภทนี้จะเสนอยาประเภทต่างๆ อาทิ สูตรสมุนไพร การรักษาการหมดสมรรถภาพ การรักษาอาการผมร่วง เป็นต้น การหลงเชื่อคำโฆษณาและซื้อผลิตภัณฑ์มาใช้งานส่วนใหญ่แล้วจะเป็นการเสียเงินไปโดยเปล่าประโยชน์
6. รายได้ก้อนใหญ่โดยไม่ต้องเสียแรงมากนัก อีเมล์ประเภทนี้จะเสนอวิธีที่จะร่ำรวยได้อย่างรวดเร็ว

7. สินค้าฟรี อีเมล์ประเภทนี้จะเสนอให้สินค้าฟรีโดยชำระเงินเพียงเล็กน้อย เช่น เพื่อเข้าเป็นสมาชิก เป็นต้น
8. โอกาสในการลงทุนที่มีผลตอบแทนสูง อีเมล์ประเภทนี้จะเสนอผลตอบแทนที่สูงกับการลงทุนที่ไม่มีความเสี่ยง เงินที่ลงทุนไปก็จะสูญไปโดยเปล่าประโยชน์
9. ชุดอุปกรณ์เชื่อมต่อเคเบิ้ลทีวี (Cable De-scambler Kits) อีเมล์ประเภทนี้จะเสนอขายชุดอุปกรณ์สำหรับเชื่อมต่อเข้ากับเคเบิลทีวีได้โดยไม่ต้องเสียค่าสมาชิกอีก เช่น เป็นรายเดือน ชุดอุปกรณ์ดังกล่าวแม้ว่าจะทำได้จริงก็เป็นสิ่งผิดกฎหมาย
10. การให้เงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่ายๆ อีเมล์ประเภทนี้จะเสนอเงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่ายๆ สถาบันทางการเงินที่ถูกต้องตามกฎหมายจะไม่ใช้วิธีนี้ในการให้เงินกู้หรือสินเชื่อ
11. การเคลียร์สินเชื่อ อีเมล์ประเภทนี้จะเสนอช่วยเคลียร์หรือล้างข้อมูลสินเชื่อที่ติดลบในบัญชีธนาคาร การทำตามที่เสนอถือเป็นการกระทำที่มีความผิดทางกฎหมาย
12. การเสนอให้รางวัลไปเที่ยวฟรี อีเมล์ประเภทนี้จะเสนอว่าท่านเป็นผู้ที่ได้รับรางวัลชนะเลิศให้ไปท่องเที่ยวฟรี ในภายหลังท่านจะพบว่าข้อเสนอนั้นไม่ได้เป็นอย่างที่คิด หรือไม่ก็ต้องชำระเงินเพิ่มเติม ซึ่งมิได้มีการอธิบายหรือแจ้งให้ทราบเอาไว้ก่อน

คำแนะนำ

- ให้ระมัดระวังโฆษณาชวนเชื่อในลักษณะดังกล่าว ซึ่งมักจะไม่มีทางเป็นจริงได้
- ให้หมั่นคอยติดตามดูประเภทของอีเมล์หลอกลวงได้จากเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

www.ftc.gov

www.crimes-of-persuasion.com

ประเด็นทางกฎหมาย (Legal Issues)

การใช้งานอินเทอร์เน็ตในแต่ละประเทศมีกฎหมายที่รองรับการใช้งานที่แตกต่างกัน บางเรื่องเป็นสิ่งที่ผิดกฎหมายในทุกประเทศทั่วโลก อาทิ ปัญหาสื่อลามกซึ่งเป็นภาพของเยาวชน การบุกรุกเครื่องคอมพิวเตอร์ เป็นต้น ในขณะที่บางเรื่อง เช่น การพนัน อาจจะเป็นสิ่งที่ผิดกฎหมายหรือไม่ผิดกฎหมายได้ในบางประเทศ ผู้ใช้จึงต้องระมัดระวังและศึกษากฎหมายที่รองรับการใช้งานอินเทอร์เน็ตในประเทศของตน กิจกรรมบนอินเทอร์เน็ตที่โดยทั่วไปถือเป็นความผิดทางกฎหมาย ได้แก่

- การเล่นการพนัน
- การซื้ออาวุธปืน
- การซื้อขายยาเสพติด
- การนำเสนอสื่อลามกทุกประเภท
- การบุกรุกคอมพิวเตอร์หรือเครือข่าย
- การพัฒนา และแพร่ไวรัสคอมพิวเตอร์
- การทำให้เครือข่ายหรือเครื่องคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานหรือให้บริการได้
- การสวมรอยบุคคลเพื่อทำการฉ้อฉล

คำแนะนำ

- ไม่เข้าไปยุ่งเกี่ยวกับกิจกรรมที่ถือเป็นความผิดทางกฎหมายดังกล่าว
- ให้ปฏิบัติตามกฎหมายของประเทศทั้งในเรื่องทั่วๆ ไปและที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต รวมทั้งกฎหมายในระดับนานาชาติด้วย
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

www.eclip.org	www.bmck.com/ecommerce/
www.ilpf.org	www.gipiproject.org/
www.uncitral.org	www.cybercrime.gov

การเฝ้าดูการใช้งานอินเทอร์เน็ต (Monitoring Internet Usage)

อินเทอร์เน็ตนอกจากจะเป็นสิ่งที่มีประโยชน์ต่อสำนักงานหรือองค์กรแล้ว ยังเป็นแหล่งบันเทิงใจสำหรับพนักงานในองค์กรด้วย แต่การที่พนักงานใช้เวลาไปกับการบันเทิงมากจนเกินไปจนกลายเป็นผลเสียต่อการทำงาน หรือการที่พนักงานอาจเข้าไปยุ่งเกี่ยวกับกิจกรรมที่ส่อไปในทางผิดกฎหมาย จะเกิดเป็นผลในทางลบต่อองค์กรได้ จึงมีความจำเป็นอย่างยิ่งที่จะต้องคอยเฝ้าดูและสอดส่องกิจกรรมการใช้งานอินเทอร์เน็ตของพนักงาน

สำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน แม้อินเทอร์เน็ตจะมีประโยชน์ต่อการเรียนรู้ เป็นสิ่งบันเทิงเชิงสร้างสรรค์ และส่งเสริมการเจริญเติบโตทางด้านวัยวุฒิของบุตรหลานในครอบครัว แต่พ่อแม่ก็ควรหมั่นสอดส่องและดูแลการเข้าไปในเว็บไซต์ที่ไม่เหมาะสมของบุตรหลาน ทั้งนี้เนื่องจากมีเว็บไซต์เป็นจำนวนมากที่ส่อไปในทางที่ไม่เหมาะสมต่อบุตรหลานของเรานั่นเอง

คำแนะนำสำหรับการใช้งานอินเทอร์เน็ตภายในองค์กร

- ให้ความรู้แก่พนักงานเกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างสม่ำเสมอ
- ให้จัดทำนโยบายการใช้งานอินเทอร์เน็ตขององค์กรอย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องมีเนื้อหาดังนี้ปรากฏอยู่ในนโยบายด้วย
  - การใช้งานอินเทอร์เน็ตมีจุดประสงค์เพื่อผลประโยชน์ขององค์กร ไม่ใช่ใช้เพื่อผลประโยชน์ส่วนตัว
  - การใช้งานอินเทอร์เน็ตจะได้รับการเฝ้าดูแลอย่างใกล้ชิด เช่น โดยผู้ดูแลระบบ
  - มีแนวทางการใช้งานอีเมล์อย่างเหมาะสม
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

คำแนะนำสำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน

- พ่อแม่จะต้องให้ความรู้แก่บุตรหลานเกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างเหมาะสม
- ให้ใช้ซอฟต์แวร์เพื่อคอยตรวจสอบการเข้าเว็บไซต์ของบุตรหลาน รวมทั้งกรองการเข้าเว็บไซต์บางเว็บไม่ให้สามารถทำได้
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

สำหรับการใช้งานอินเทอร์เน็ตภายในองค์กร ให้ดูข้อมูลเพิ่มเติมที่

www.email-policy.com

www.epolicyinstitute.com

www.fatline.com

สำหรับการใช้งานอินเทอร์เน็ตจากที่บ้าน ให้ดูข้อมูลเพิ่มเติมที่

www.getnetwise.org/

www.wiredpatrol.org/

www.childnet-int.org/

การหมิ่นประมาทหรือการทำให้ผู้อื่นเสียชื่อเสียง

(Online Defamation)

ข้อความทุกรูปแบบที่ใช้งานบนอินเทอร์เน็ตไม่ว่าจะเป็นในอีเมล์ เว็บบอร์ด ห้องสนทนาบนเว็บไซต์ ต้องระมัดระวังไม่ให้เป็นข้อความเท็จหรือก่อให้เกิดความเสียหายต่อตัวบุคคลหรือองค์กรที่ถูกพาดพิง กล่าวถึง หรืออ้างอิง

คำแนะนำ

- ให้กล่าวเฉพาะสิ่งที่มีหลักฐานความจริงสนับสนุนเท่านั้น ห้ามใช้อารมณ์หรือความรู้สึกมากล่าวลงไป

- อีเมล์เมื่อส่งไปยังผู้รับแล้วจะไม่มีทางเรียกกลับคืนมาได้ ฉะนั้นให้ระมัดระวังทุกถ้อยคำในอีเมล์ที่ส่งถึงผู้รับ
- ให้ระมัดระวังการกล่าวคำในเว็บบอร์ด ห้องสนทนา ข้อความฉับพลันที่จะไม่ละเมิดผู้อื่น
- ให้ความรู้แก่พนักงานหรือบุตรหลานเกี่ยวกับการระมัดระวังการใช้ถ้อยคำของตนบนอินเทอร์เน็ต
- ก่อนที่จะกล่าวถึงผู้อื่นในเชิงลบ ให้พิจารณาถึงสาเหตุที่ต้องทำ รวมทั้งประเมินผลที่จะเกิดขึ้นด้วย
- ให้หมั่นคอยติดตามดูเว็บไซต์ในแหล่งข้อมูลเพิ่มเติม

แหล่งข้อมูลเพิ่มเติม

www.onlinepolicy.org/defamation.shtml

www.wiredpatrol.org/law/freespeech/defamation.html

www.spawn.org/marketing/slander.html

www.cyberlaw.com

การไกล่เกลี่ยความขัดแย้งบนเครือข่าย

(Online Dispute Resolution)

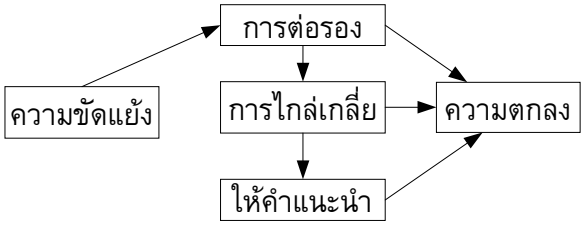
ในสังคมที่เราอยู่อาศัยกันย่อมจะมีความขัดแย้งอยู่ไม่ว่ากรณีใดกรณีหนึ่ง บนเครือข่ายอินเทอร์เน็ตก็มีความขัดแย้งอยู่เช่นเดียวกัน แต่นับว่าเป็นเรื่องยากที่จะไกล่เกลี่ยความขัดแย้งบนอินเทอร์เน็ตเนื่องจากคู่กรณีไม่เคยพบปะเห็นหน้ากันมาก่อน สหภาพยุโรป จึงได้จัดให้มีโครงการนำร่องที่มีชื่อว่า ECODIR หรือ Electronic Consumer Dispute Resolution ซึ่งแปลว่าการไกล่เกลี่ยความขัดแย้งทางอิเล็กทรอนิกส์สำหรับผู้บริโภค ECODIR นี้ได้รับการจัดตั้งขึ้นเพื่อให้ผู้บริโภคและบริษัทธุรกิจบนเครือข่ายสามารถไกล่เกลี่ยความขัดแย้งที่เกิดจากการค้าผ่านทางเครือข่ายอินเทอร์เน็ต

หากคู่กรณีต่อรองกันแล้วไม่สามารถตกลงกันได้จะมีบุคคลที่สามที่เป็นกลางมาให้ความช่วยเหลือ โดยบุคคลที่สามดังกล่าวนี้จะต้องลงนามในเอกสารรับรองความเป็นกลางของตน และกระบวนการไกล่เกลี่ยนี้จะถูกเก็บไว้เป็นความลับและกระทำโดยความสมัครใจของคู่กรณี โดยที่คู่กรณีสามารถถอนตัวจากกระบวนการนี้ได้ทุกเมื่อเพื่อนำความเข้าสู่ศาล

แนวคิดของการไกล่เกลี่ยความขัดแย้งบนเครือข่ายนี้คือในเมื่อความขัดแย้งเกิดขึ้นบนเครือข่ายอินเทอร์เน็ตก็สมควรให้มีการไกล่เกลี่ยผ่านทางเครือข่ายอินเทอร์เน็ต และเมื่อผู้ประกอบการค้าจัดตั้งร้านค้าของตนบนเครือข่ายอินเทอร์เน็ตเพิ่มมากขึ้น การไกล่เกลี่ยความขัดแย้งบนเครือข่ายนี้จะยิ่งมีความจำเป็นมากขึ้นในอนาคต วิธีการไกล่เกลี่ยนี้เป็นวิธีที่มีประสิทธิภาพและไม่สิ้นเปลืองค่าใช้จ่ายที่จะสามารถนำมาช่วยแก้ปัญหาความขัดแย้งที่เกิดจากการค้าบนเครือข่ายอินเทอร์เน็ตที่มีมูลค่าไม่สูงนัก

ผู้เข้าร่วมโครงการ ECODIR นี้ได้แก่ ภาครัฐ ภาคเอกชน ภาคการศึกษา และจากประเทศต่างๆ ในทวีปยุโรปและอเมริกาเหนือ ข้อมูลเพิ่มเติมของโครงการนี้สามารถหาดูได้จากจากเว็บไซต์ที่ระบุไว้ด้านล่าง

ECODIR เป็นกระบวนการบนเครือข่ายผ่านทางเว็บที่ได้รับการเสริมความปลอดภัย (secure web) โดยจะแบ่งออกเป็น 3 ขั้นตอนดังแสดงในแผนผังด้านล่าง



แหล่งข้อมูลเพิ่มเติม

www.ecodir.org

www.adr.org

การถูกติดตามบนเครือข่าย (Online Stalking)

การถูกติดตาม (Stalking) แม้คำนี้จะได้รับคำจำกัดความอยู่หลากหลาย แต่จะมีอยู่สองความหมาย ที่คล้ายคลึงกันดังนี้

1. การที่บุคคลหนึ่งพยายามติดต่ออีกบุคคลหนึ่งโดยซ้ำซากและโดยที่อีกบุคคลหนึ่งนั้นไม่พึงประสงค์
2. พฤติกรรมใดๆ ที่ทำให้ผู้ถูกติดตามรู้สึกว่าตนเองถูกคุกคาม มีความกังวล หรือหวาดกลัว

ดังนั้น “การถูกติดตามบนเครือข่าย” จึงเกิดขึ้นเมื่อบุคคลหนึ่งกระทำการตามความหมายด้านบนโดยการใช้อีเมล์ ห้องสนทนาบนเครือข่ายอินเทอร์เน็ต และโปรแกรมส่งข้อความฉับพลัน (instant messaging) ซึ่งสามารถก่อให้เกิดความเดือดร้อนแก่บุคคลที่ถูกติดตาม รัฐบาลบางประเทศได้กำหนดไว้ในกฎหมายใหม่หรือแก้ไขกฎหมายเก่าให้ครอบคลุมกรณีการถูกติดตามบนเครือข่ายไว้ด้วยและในบางกรณีสามารถสั่งการให้ควบคุมตัวผู้ติดตามได้

การถูกติดตามนี้สามารถทวีความรุนแรงจนกระทั่งถึงการทำลายระบบคอมพิวเตอร์ให้เกิดความเสียหายได้

คำแนะนำ

หากถูกติดตามบนเครือข่ายอยู่ ให้ปฏิบัติดังนี้

- ลบชื่อหรือสิ่งที่ใช้แทนตัวที่ใช้ในห้องสนทนาหรือโปรแกรมส่งข้อความฉับพลันออกทั้งหมด
- เปลี่ยนอีเมล์แอดเดรสโดยทันทีโดยให้ใช้อีเมล์แอดเดรสใหม่ที่ผู้พบเห็นไม่สามารถระบุเพศได้
- พิจารณาใช้ระบบอีเมล์ที่ไม่บอกชื่อผู้ส่ง

- ติดต่อผู้ให้บริการอินเทอร์เน็ตหรือผู้ดูแลห้องสนทนาโดยระบุหลักฐานที่แสดงว่าท่านกำลังถูกติดตามอยู่เพื่อลดความเสี่ยงที่จะถูกติดตามบนเครือข่าย ให้ปฏิบัติดังนี้
- ใช้ชื่อบัญชีผู้ใช้ที่ผู้พบเห็นไม่สามารถระบุเพศได้
- ไม่แสดงหรือทิ้งข้อมูลส่วนตัวไว้ ณ ที่ใดก็ตามบนอินเทอร์เน็ต ซึ่งรวมถึงประวัติส่วนตัวด้วย
- ใช้รหัสผ่านที่ยากต่อการเดา โดยใช้วิธีตามที่แนะนำในหัวข้อรหัสผ่านในคู่มือนี้
- ไม่ใช้ภาษาที่ไม่สุภาพในห้องสนทนาหรือโปรแกรมส่งข้อความฉับพลัน

แหล่งข้อมูลเพิ่มเติม

www.cyber-stalking.net

www.wiredpatrol.org/stalking/

www.privacy.net

รหัสผ่าน (Passwords)

อาจมีวันหนึ่งที่เมื่อออกจากบ้านไปแล้ว ลืมล็อกประตูบ้าน คนแปลกหน้าอาจเดินเข้ามาในบ้านและเดินสำรวจดูรอบๆ บ้าน แม้จะไม่ได้ขโมยสิ่งของใดๆ ไปก็ตาม แต่เจ้าของบ้านก็คงจะรู้สึกไม่สบายใจนักที่ได้ทราบว่ามีคนแปลกหน้าเข้ามาเยือนภายในบ้าน เหตุการณ์เช่นนี้สามารถเกิดขึ้นกับเครื่องคอมพิวเตอร์ได้เช่นกัน โดยที่ผู้บุกรุกสามารถเข้ามาแอบดูข้อมูลในเครื่องของเราได้หากไม่ได้ป้องกันไว้อย่างดีพอ รหัสผ่านถือเป็นด่านป้องกันด่านแรกสำหรับเครื่องคอมพิวเตอร์ จึงจำเป็นต้องใช้รหัสผ่านที่ยากต่อการเดา รหัสผ่านมีความสำคัญเทียบเท่ากับกุญแจไขประตูเข้าบ้าน ดังนั้นจึงควรมีคุณภาพสูงที่สุด (เช่นเดียวกับการใช้กุญแจล็อกคุณภาพสูง)

ผู้บุกรุกระบบสามารถใช้โปรแกรมแกะรหัสผ่านที่สามารถเข้าถึงรหัสผ่านที่กำหนดไว้อย่างง่ายๆ ได้ภายในระยะเวลาประมาณหนึ่งชั่วโมงเท่านั้น ในทางกลับกันการจะเดารหัสผ่านที่ยากนั้นจะต้องใช้เวลาถึง 10 ถึง 20 ปี

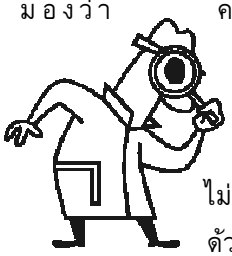
คำแนะนำ

- ไม่ใช้คำใดๆ ที่มีอยู่ในพจนานุกรมไม่ว่าจะเป็นพจนานุกรมภาษาใดๆ ก็ตาม รวมทั้งคำศัพท์ทางวิทยาศาสตร์ด้วย
- ไม่ใช้คำใดๆ ที่สะกดกลับทางซึ่งเป็นคำที่มาจากพจนานุกรม เช่น flower สะกดกลับเป็น rewolf
- ไม่ใช้คำใดๆ ที่เกี่ยวข้องกับตัวเรา เช่น ที่อยู่ หมายเลขโทรศัพท์ วันเกิด ชื่อสัตว์เลี้ยง ชื่อเล่น งานอดิเรก หรือกีฬาที่ชอบ
- ไม่ใช้ตัวอักษรหรือตัวเลขที่เรียงกัน เช่น “abcdefg” หรือ “234567”
- ไม่ใช้ตัวอักษรที่เรียงกันตามแป้นพิมพ์ เช่น “qwerty”
- ให้ใช้ตัวอักษร ตัวเลข และตัวอักษรพิเศษ ร่วมกันแบบสุ่ม

- ให้ใช้ตัวอักษรทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ในภาษาอังกฤษและใช้ตัวอักษรพิเศษร่วมด้วย เช่น * @ #
- ให้ใช้รหัสผ่านที่มีความยาวอย่างน้อย 6 ตัว ยิ่งรหัสผ่านมีความยาวมากเท่าใดก็ยิ่งมีความยากต่อการเดามากเท่านั้น
- ไม่จดรหัสผ่านเก็บไว้ไม่ว่าจะในที่ใดๆ ก็ตาม
- ไม่บอกรหัสผ่านกับผู้อื่นไม่ว่าจะด้วยเหตุผลใดๆ ก็ตาม
- ไม่ใช้ตัวเลือกให้จำรหัสผ่านที่มีอยู่ในเว็บไซต์บางเว็บหรือโปรแกรมที่ใช้งานบางโปรแกรม และให้ปิดความสามารถนี้ในโปรแกรมบราวเซอร์ที่ใช้งาน
- ไม่ใช้รหัสผ่านเดียวกันเพื่อเข้าโปรแกรมต่างๆ ที่ใช้งาน

ความลับของข้อมูลส่วนตัว (Privacy of Personal Information)

ในชีวิตประจำวันผู้ใช้งานอินเทอร์เน็ตอาจมีความจำเป็นต้องบอกข้อมูลส่วนตัวให้ผู้อื่นได้รับทราบจนเป็นเรื่องปกติ เช่น ข้อมูลส่วนตัวที่ให้ในระหว่างการจ่ายเงินค้างชำระ การเตรียมการเดินทาง การใช้บัตรเครดิตในการจับจ่ายใช้สอย เป็นต้น ข้อมูลที่ให้ไปนี้อาจถูกส่งต่อไปให้กับผู้อื่นต่อไปซึ่งทำให้ผู้ให้ข้อมูลขาดความมั่นใจว่าผู้รับจะนำข้อมูลของตนไปเผยแพร่ต่อหรือไม่ และมีบางกลุ่มที่ถึงขนาดมองว่า ความเสี่ยงของข้อมูลส่วนตัวในเครือข่ายอินเทอร์เน็ตนั้นมีมากกว่าในโลกแห่งความเป็นจริงทางกายภาพ และทำให้คนเหล่านี้ไม่ยอมเข้ามาเกี่ยวข้องกับเครือข่ายอินเทอร์เน็ตเลย



การให้ข้อมูลส่วนตัวเป็นสิ่งที่สามารถทำได้ตามปกติ ไม่ว่าจะอยู่บนโลกแห่งอินเทอร์เน็ตหรือไม่ก็ตาม แต่ต้องกระทำด้วยความระมัดระวัง หลักการให้ที่สำคัญคือให้โดยให้น้อยที่สุดเท่าที่จะทำได้

คำแนะนำ

ก่อนที่จะให้ข้อมูลส่วนตัวกับเว็บไซต์หนึ่งที่ต้องการประกอบธุรกรรมด้วย ให้ทำการตรวจสอบนโยบายการใช้ข้อมูลส่วนตัวของลูกค้า ได้แก่

- การนำอีเมล์แอดเดรสของลูกค้าไปใช้งาน เช่น ขายหรือแลกเปลี่ยนกับผู้อื่นหรือไม่
- การนำข้อมูลส่วนตัวไปใช้โดยผ่านการยินยอมจากลูกค้าแล้วหรือไม่

แหล่งข้อมูลเพิ่มเติม

www.privacyfoundation.org

www.oecd.org

www.epic.org

www.privacy.net

การใช้งานอินเทอร์เน็ตในที่สาธารณะ (Public Access Points)

ผู้คนจำนวนมากมายที่ไม่มีเครื่องคอมพิวเตอร์เป็นของตัวเองแต่ก็ต้องการที่จะเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ผู้คนที่เดินทางไปในวันหยุดพักผ่อนและไม่ได้นำเครื่องแลปทอปไปด้วยแต่ก็ต้องการที่จะใช้อินเทอร์เน็ตเพื่อติดต่อกับเพื่อนฝูง ครอบครัว และผู้ร่วมงาน นักธุรกิจที่เดินทางไปโดยไม่ต้องการนำเครื่องแลปทอปไปด้วยก็ยังต้องการที่จะใช้อีเมล์และแลกเปลี่ยนเอกสารทางธุรกิจที่สำคัญ ที่กล่าวมาทั้งหมดนี้คือเหตุผลสำหรับการใช้งานอินเทอร์เน็ตผ่านทางจุดเชื่อมต่อในที่สาธารณะ เช่น อินเทอร์เน็ตคาเฟ่ สถานที่ใช้งานอินเทอร์เน็ตตามสนามบิน เครื่องคอมพิวเตอร์สาธารณะในโรงแรมห้องสมุด หรือสถานที่อื่นๆ

วิธีการเข้าถึงเครือข่ายอินเทอร์เน็ตนี้แม้จะสามารถทำได้อย่างสะดวกสบาย แต่ก็เป็นวิธีที่ต้องให้ความระมัดระวังด้วยเช่นกัน ให้พึงรำลึกไว้เสมอว่าเครื่องคอมพิวเตอร์ในที่สาธารณะเหล่านี้เป็นเครื่องที่มีความเปิดเผยสูงและให้ปฏิบัติตามคำแนะนำถัดไปด้วยความระมัดระวัง

คำแนะนำ

- ให้ระวังคนที่นั่งหรือยืนอยู่ใกล้ๆ ซึ่งอาจแอบมองจากด้านหลังเพื่อขโมยบัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนตัวอื่นๆ ในขณะที่ผู้ใช้กำลังป้อนข้อมูลเหล่านั้นเข้าเครื่อง
- เปลี่ยนรหัสผ่านเข้าสู่ระบบบ่อยๆ
- ให้ล้างหน่วยความจำคอมพิวเตอร์ (cache) ในเว็บบราวเซอร์หลังจากที่ใช้งานเสร็จแล้ว ซึ่งจะช่วยลดโอกาสที่ผู้อื่นจะสามารถเขาถึงข้อมูลส่วนตัวของท่านได้
- ให้ล้างบันทึกประวัติการใช้งาน (history settings) ในเว็บบราวเซอร์หลังจากที่ใช้งานเสร็จแล้ว
- ให้ปิดเว็บบราวเซอร์ทั้งหมดที่เปิดใช้งานหลังจากที่ใช้งานเสร็จแล้ว
- ไม่อนุญาตให้เครื่องคอมพิวเตอร์จำรหัสผ่านให้ เช่น จะต้องคลิกตัวเลือกการจำรหัสผ่านออก
- ไม่ป้อนข้อมูลลับหรือส่วนตัวที่เป็นความลับใดๆ โดยผ่านทางเครื่องคอมพิวเตอร์สาธารณะ

เว็บเพจที่มีการเสริมความปลอดภัย (Secure Web Pages)

ในการสั่งซื้อสินค้าผ่านทางอินเทอร์เน็ต ผู้ซื้อควรทำทุกอย่างที่สามารถทำได้เพื่อที่จะสามารถตัดสินใจได้ว่าเว็บไซต์นั้นเป็นเว็บไซต์ของร้านค้าหรือธุรกิจที่ถูกกฎหมายหรือไม่ และมีนโยบายการทำธุรกรรมผ่านทางเครือข่ายที่ดีและเป็นไปตามที่แนะนำไว้ในคู่มือนี้หรือไม่

ในขั้นตอนของการสั่งซื้อ ผู้ซื้ออาจจำเป็นต้องให้ข้อมูลส่วนตัวและหมายเลขบัตรเครดิตกับร้านนั้นโดยผ่านทางอินเทอร์เน็ต ก่อนที่จะให้ข้อมูลส่วนตัวไปผู้ซื้อจะต้องตรวจสอบว่าข้อมูลที่ส่งมอบให้ทางอินเทอร์เน็ตนั้นจะเป็นไปอย่างปลอดภัย กล่าวคืออย่างน้อยไม่มีผู้อื่นแอบดักดู

ข้อมูลของเราได้ คำแนะนำด้านล่างจะได้กล่าวถึงการตรวจสอบต่างๆ ที่จำเป็นก่อนที่จะส่งมอบข้อมูลส่วนตัวใดๆ ให้กับร้านค้า

คำแนะนำ

- มีวิธีการตรวจสอบอย่างง่ายๆ เพื่อตรวจสอบดูว่าเว็บเพจหนึ่งๆ ได้รับการเสริมความปลอดภัยหรือไม่ วิธีแรกคือสำหรับระบบที่ใช้ไมโครซอฟท์วินโดว์ส คลิกปุ่มขวาของเมาส์ในขณะที่เมาส์พอยเตอร์อยู่ตรงที่ว่างบนเว็บเพจแล้วเลือก “Properties” จะทำให้มีหน้าต่างแสดงข้อมูลของหน้านั้นปรากฏขึ้น จากนั้นคลิกที่ “Certificates” (ใบรับรองอิเล็กทรอนิกส์) หากเว็บเพจนั้นไม่ได้รับการเสริมความปลอดภัยก็จะมีข้อความบอกว่าหน้านั้นไม่มีใบรับรองอิเล็กทรอนิกส์อยู่ แต่ถ้าเว็บเพจนั้นมีการเสริมความปลอดภัยก็จะมีข้อความระบุขนาดของกุญแจ (Key) สำหรับเว็บเพจนั้น ซึ่งขนาดที่เหมาะสมของกุญแจควรจะเป็น 128 บิตเป็นอย่างน้อย การปฏิบัติตามคำแนะนำง่ายๆ นี้ ก็จะสามารถทราบได้ว่าข้อมูลส่วนตัวที่ส่งผ่านไปทางอินเทอร์เน็ตจะได้รับการส่งไปอย่างปลอดภัยหรือไม่
- วิธีที่สองและสามจะเป็นวิธีที่ใช้ไม่ได้เสมอไป วิธีการคือให้ดูที่ช่อง “Address” ในบราวเซอร์ว่าที่อยู่ของเว็บนั้นขึ้นต้นด้วยคำ “https” หรือ “http” หากเว็บนั้นได้รับการเสริมความปลอดภัย ที่อยู่ของเว็บนั้นจะขึ้นต้นด้วยคำ “https” วิธีนี้จะสามารถทราบได้ว่าเว็บหนึ่งๆ ได้รับการเสริมความปลอดภัยหรือไม่ แต่จะไม่ทราบว่าเว็บนั้นมีความปลอดภัยในระดับใดเนื่องจากจะไม่ทราบขนาดของกุญแจที่ใช้งาน
- วิธีที่สามคือให้ตรวจสอบที่ด้านล่างของหน้าต่างบราวเซอร์ว่ามีการแสดงเครื่องหมายใดๆ ที่แสดงถึงการเสริมความปลอดภัยหรือไม่ โดยปกติจะปรากฏเป็นรูปกุญแจสายยูที่ล็อกแล้ว หรือรูปลูกกุญแจที่ไม่หัก เช่นเดียวกันกับวิธีที่สอง วิธีนี้ไม่สามารถบอกได้ว่าเว็บนั้นมีความปลอดภัยในระดับใด นอกจากนั้นแล้วในเว็บเพจบางประเภท (เช่น เว็บเพจที่ใช้เฟรม) อาจจะไม่มีการแสดงเครื่องหมายนี้ปรากฏให้เห็น

แหล่งข้อมูลเพิ่มเติม

ให้ดูในส่วน “Help” ของบราวเซอร์สำหรับข้อมูลเพิ่มเติมในเรื่องใบรับรองอิเล็กทรอนิกส์ เว็บไซต์ที่ได้รับการเสริมความปลอดภัย และการใช้งานเว็บไซต์ที่ได้รับการเสริมความปลอดภัย

การปรับปรุงซอฟต์แวร์ (Software Updates)

การไม่ปรับปรุงซอฟต์แวร์บนเครื่องคอมพิวเตอร์ที่ใช้งานให้ทันสมัยอยู่เสมอ อาจกลายเป็นต้นตอของปัญหาด้านความปลอดภัยได้ หลังจากที่ได้มีการใช้งานโปรแกรมผ่านไปเป็นระยะเวลาหนึ่งแล้ว จะมีปัญหาเล็กๆ น้อยๆ ซึ่งรวมถึงปัญหาด้านความปลอดภัยเกิดขึ้นเสมอ ผู้ผลิตจึงได้ทำการพัฒนาโปรแกรมสำหรับอุดช่องโหว่ (Patch) เพื่อแก้ปัญหาเหล่านั้น นอกจากนั้นการปรับปรุงซอฟต์แวร์ยังอาจหมายถึง เป็นการเพิ่มขีดความสามารถทางด้านการรักษาความปลอดภัยให้สูงขึ้น ทั้งนี้เนื่องจากผู้ผลิตซอฟต์แวร์ที่มีชื่อเสียงต่างก็พยายามที่จะทำให้สภาพแวดล้อมในการใช้งานมีความปลอดภัยมากขึ้น โดยเฉพาะอย่างยิ่งสำหรับซอฟต์แวร์ระบบปฏิบัติการ ได้แก่ วินโดว์ส แม็ค หรือลินุกซ์

คำแนะนำ

- หากใช้งานวินโดว์สเอ็กซ์พีหรือวินโดว์ส 2000 ให้เลือกใช้ระบบไฟล์แบบ “NTFS” แทนที่จะเป็นแบบ “FAT32” ซึ่งจะทำให้ระบบมีความปลอดภัยสูงมากขึ้นและยังมีขีดความสามารถในการเข้ารหัสข้อมูลเพื่อให้ข้อมูลที่เก็บเป็นความลับด้วย
- ใช้ระบบปฏิบัติการรุ่นล่าสุด
- ใช้เว็บบราวเซอร์รุ่นล่าสุด
- ตรวจสอบและติดตั้งโปรแกรมอุดช่องโหว่ของโปรแกรมสำนักงานอย่างสม่ำเสมอ โปรแกรมสำนักงาน เป็นโปรแกรมที่มีความสำคัญเนื่องจากเป็นโปรแกรมที่ใช้ในการสร้างไฟล์ที่มีการใช้งานร่วมกัน หรือที่รับส่งกันผ่าน

ทางอีเมล์ ฟล็อปปี้ดิสก์ และระบบการแชร์ไฟล์ (เช่น โปรแกรมเวิร์ด ตารางคำนวณ ฐานข้อมูล และปฏิทิน)

- ใช้โปรแกรมอีเมล์ที่มีขีดความสามารถในการรักษาความปลอดภัยสูง โปรแกรมอีเมล์นับได้ว่าเป็นโปรแกรมที่มีความสำคัญยิ่งเนื่องจากเป็นโปรแกรมที่ใช้งานอยู่เป็นประจำในการสื่อสารกับทั้งคนที่รู้จักและคนแปลกหน้า
- ติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดและต้องปรับปรุงไฟล์รูปแบบไวรัสใหม่ๆ ให้ทันสมัยอยู่เสมอ
- ปรับปรุงโปรแกรมไฟร์วอลล์ให้ทันสมัยอยู่เสมอ
- หากเป็นไปได้ ให้ตั้งค่าให้โปรแกรมที่ใช้งานทำการปรับปรุงตัวเองโดยอัตโนมัติ (Automatic Update) ซึ่งเป็นวิธีที่มีประสิทธิภาพมากที่จะทำโปรแกรมที่ใช้งานได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ

สแปม (Spam)

ในปัจจุบันเราทุกคนส่วนใหญ่ล้วนได้รับจดหมายขยะ ตู้จดหมายของเราจะเต็มไปด้วยจดหมายโฆษณาที่เราไม่ได้ขอให้ส่งมาให้ และเราก็ทิ้งจดหมายเหล่านั้นไปโดยไม่ได้แม้แต่จะเปิดอ่าน สิ่งที่เทียบเท่ากันนี้กำลังเกิดขึ้นกับระบบอีเมล์ที่เราใช้งานกันอยู่ กล่าวคือข้อความอีเมล์ที่เราไม่ได้ขอให้ส่งมาให้จะมาอยู่ในตู้จดหมายอิเล็กทรอนิกส์ของเราเกือบทุกวันและกลายเป็นสิ่งที่ค่อนข้างจะน่ารำคาญ เราเรียกข้อความอีเมล์ที่เป็นขยะดังกล่าวว่าสแปมเมล์ หรือเรียกสั้นๆ ว่าสแปม

สแปมเป็นปัญหาที่หนักกว่าจดหมายขยะในตู้จดหมาย เนื่องจากสแปมก่อให้เกิดค่าใช้จ่ายต่อผู้รับตามสาเหตุที่จะได้กล่าวถึงด้านล่าง ในขณะที่จดหมายขยะจะก่อให้เกิดค่าใช้จ่ายต่อผู้ส่งซึ่งต้องใช้เงินในการตีพิมพ์โฆษณาเพื่อส่งมายังผู้รับ นอกจากนั้นแล้วผู้ส่งสแปมจะเสียค่าใช้จ่ายเท่าเดิมไม่ว่าสแปมเมล์นั้นจะถูกส่งไปยังผู้รับเพียงคนเดียวหรือล้านคนก็ตาม ส่วนจดหมายขยะผู้ส่งจะต้องเสียค่าใช้จ่ายเท่ากับจำนวนผู้รับ

สแปมทำให้บุคคลและองค์กรสิ้นเปลืองทั้งเวลาและเงินตามที่จะได้กล่าวถึงดังนี้

- ผู้รับสแปมส่วนใหญ่จะต้องเสียค่าใช้จ่ายในการเชื่อมต่อกับอินเทอร์-เน็ตเป็นรายชั่วโมง หากต้องรับสแปมเป็นจำนวนมาก ก็เป็นที่แน่นอนว่าผู้รับจะต้องเสียค่าใช้จ่ายในการนี้สูงมากขึ้น
- ผู้รับอาจต้องใช้เวลาในการจัดการกับสแปมเป็นจำนวนมากในแต่ละวัน (ทั้งนี้เนื่องจากผู้ส่งสามารถส่งได้ง่ายโดยมีค่าใช้จ่ายเท่าเดิม)
- สแปมกีดขวางการทำงานของเมล์เซิร์ฟเวอร์ทั่วโลกซึ่งทำให้ทุกคนประสบกับการเชื่อมต่อที่ช้าลงและเสียค่าใช้จ่ายในการเชื่อมต่อที่สูงขึ้น

ถึงแม้ว่าจะไม่สามารถกำจัดสแปมได้อย่างเด็ดขาดแต่เราอาจลดระดับความรุนแรงลงได้โดยให้ปฏิบัติตามคำแนะนำด้านล่างนี้

คำแนะนำ

- ไม่ส่งอีเมล์เพื่อตอบกลับสแปมที่ส่งมา การตอบสแปมนั้นเท่ากับเป็นการยืนยันอีเมล์แอดเดรสของผู้รับว่าเป็นแอดเดรสที่มีอยู่จริงและจะทำให้ผู้รับนั้นตกเป็นเป้าหมายที่ชัดเจนมากยิ่งขึ้น
- ให้ใช้อีเมล์แอดเดรสที่ใช้ในงานประจำวันเพื่อติดต่อกับผู้ที่ติดต่ออยู่ด้วยเป็นประจำ เช่น ผู้ร่วมงาน เพื่อน และครอบครัว สำหรับการส่งอีเมล์เพื่อจุดประสงค์อื่นๆ ให้ใช้อีเมล์แอดเดรสต่างหากอีกอันหนึ่ง
- ไม่ใช้อีเมล์แอดเดรสที่ใช้ในงานประจำวันเพื่อสมัครสมาชิกอีเมล์เพื่อขอรับข้อมูลข่าวสารหรือเข้าเป็นสมาชิกในเมล์ลิ่งลิสต์ต่างๆ
- ไม่ซื้อสินค้าใดๆ ที่โฆษณาในสแปม เนื่องจากจะยิ่งทำให้ผู้ส่งสแปมได้รับผลตอบแทนและจะใช้วิธีนี้ต่อไปเรื่อยๆ
- ใช้ตัวกรองสแปม (สแปมฟิลเตอร์) ซึ่งมีให้เลือกหลากหลายและเลือกชนิดที่เหมาะสมกับโปรแกรมอีเมล์ที่ใช้งานอยู่ให้มากที่สุด
- ให้รายงานร้องเรียนปัญหาสแปมกลับไปยังผู้ให้บริการเครือข่ายอินเทอร์-เน็ต เว็บไซต์ต่อต้านสแปม หรือองค์กรคุ้มครองผู้บริโภค

- ตรวจสอบนโยบายการใช้ข้อมูลส่วนตัวของลูกค้าของเว็บไซต์ที่เข้าไปใช้บริการ เพื่อดูว่าเว็บนั้นจะนำอีเมล์แอดเดรสของลูกค้าไปทำอะไรบ้าง

แหล่งข้อมูลเพิ่มเติม

spam.abuse.net

www.cauce.org

การปลอมแปลงอีเมล์ (Spoofing)

การปลอมแปลงบนระบบคอมพิวเตอร์ที่สำคัญมีด้วยกันสองประเภท ประเภทแรกคือการปลอมแปลงหมายเลข IP Address (IP Address Spoofing) ผู้ให้บริการอินเทอร์เน็ต (ISP) ในปัจจุบันจะสามารถป้องกันลูกค้าของตนจากการปลอมแปลงประเภทนี้ได้แล้ว ดังนั้นผู้ใช้ที่บ้านและธุรกิจจึงไม่จำเป็นจะต้องกังวลกับปัญหานี้ อย่างไรก็ตามองค์กรหรือธุรกิจที่ต้องดูแลระบบเครือข่ายเองอาจมีความจำเป็นต้องปรึกษากับผู้ขายอุปกรณ์เครือข่ายที่องค์กรจัดซื้อมาใช้งานเพื่อปกป้องตนเองจากปัญหานี้

การปลอมแปลงอีกประเภทหนึ่งคือการปลอมแปลงอีเมล์ (Email Spoofing) ผลที่เกิดขึ้นคือผู้ใช้จะได้รับอีเมล์ที่ระบุว่ามาจากผู้ส่งคนหนึ่งแต่แท้จริงแล้วเป็นอีเมล์ที่มาจากผู้ส่งอีกคนหนึ่ง การปลอมแปลงอีเมล์นี้โดยทั่วไปแล้วจะมีวัตถุประสงค์ที่จะหลอกให้เหยื่อกระทำการที่อาจก่อให้เกิดความเสียหายหรือบอกข้อมูลที่มีความสำคัญออกมา (เช่น รหัสผ่าน หรือข้อมูลส่วนตัว)

คำแนะนำ

- เมื่อได้รับแจ้งเตือนถึงการปลอมแปลงอีเมล์ที่กล่าวว่าผู้ส่งคือท่าน หรือได้รับทราบถึงการปลอมแปลงจากการตีกลับของอีเมล์ของท่านทั้งๆ ที่ท่านไม่ได้เป็นผู้ส่งไป ให้เก็บรวบรวมหลักฐานทั้งหมดที่เกี่ยวกับการปลอมแปลงนั้นและส่งไปให้กับผู้ให้บริการอินเทอร์เน็ตของท่านเพื่อใช้ในการสืบสวนต่อไป

- ให้ใช้ลายมือชื่ออิเล็กทรอนิกส์กับผู้ที่ติดต่อด้วย หากไม่มั่นใจว่าอีเมล์ที่ได้รับมาจากแหล่งที่เชื่อถือได้หรือไม่ สำหรับข้อมูลเพิ่มเติมในเรื่องนี้โปรดดูที่หัวข้อลายมือชื่ออิเล็กทรอนิกส์
- ให้ระมัดระวังอีเมล์ที่ระบุว่าส่งมาจากเพื่อนหรือผู้ร่วมงานและใช้ subject ของอีเมล์ที่แปลกๆ อีเมล์ดังกล่าวนี้อาจส่งมาโดยอัตโนมัติจากซอฟต์แวร์ที่ไม่ประสงค์ดีต่างๆ เช่น หนอนเครือข่าย เป็นต้น
- ให้ดูวิธีการหลอกลวงต่างๆ จากเว็บไซต์ด้านล่างซึ่งเป็นเว็บของเซิร์ต (CERT-Computer Emergency Response Team) ซึ่งเป็นหน่วยงานที่ได้รับรายงานจากทั่วโลกเกี่ยวกับการหลอกหลวงในรูปแบบต่างๆ ที่เกิดขึ้น

มีวิธีการหลอกลวงหลากหลายวิธีที่นำมาใช้หลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน การหลอกลวงดังกล่าวอาจจะมาในรูปของการปลอมแปลงอีเมล์ การหลอกให้เข้าไปดูเว็บไซต์ การโทรศัพท์ถาม หรือแม้แต่การส่งจดหมายมาถามทางไปรษณีย์ ทั้งนี้ก่อนที่จะให้ข้อมูลใดๆ เกี่ยวกับรหัสผ่านหรือข้อมูลส่วนตัวของตน ให้ตรวจสอบให้มั่นใจก่อนว่าผู้สอบถามเป็นผู้ที่รู้จักหรือสามารถพิสูจน์ตัวตนได้

แหล่งข้อมูลเพิ่มเติม

www.cert.org/tech_tips/email_spoofing.html

สปายแวร์ (Spyware)

สปายแวร์คือซอฟต์แวร์ใดๆ ที่ใช้ช่องทางการเชื่อมต่อกับอินเทอร์เน็ตในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อแอบส่งข้อมูลส่วนตัวของผู้ใช้นั้นไปให้กับบุคคลหรือองค์กรหนึ่งโดยที่ผู้ใช้เองไม่ทราบ หรือไม่ได้รับอนุญาตจากผู้ใช้ก่อน สปายแวร์สามารถเข้าสู่เครื่องคอมพิวเตอร์ที่ใช้งานได้โดยผ่านทางไวรัสคอมพิวเตอร์ เว็บเพจที่เข้าไปดู หรืออีเมล์ที่เปิดอ่าน

สปายแวร์นั้นมีหลายประเภทนับตั้งแต่ประเภทที่เป็นคุกกี้จากการเข้าดูเว็บ (ดูรายละเอียดในหัวข้อ**คุกกี้**) จนกระทั่งถึงประเภทที่เป็นโปรแกรมที่ล่วงล้ำเข้ามาในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อรายงานข้อมูลกลับไปยังผู้ผลิตว่าผู้ใช้ใช้งาน

โปรแกรมที่ติดตั้งนั้นอย่างไร โปรแกรมที่ล่วงล้ำนี้โดยทั่วไปจะเป็นซอฟต์แวร์ที่ผู้ใช้ดาวน์โหลดมาจากอินเทอร์เน็ตและติดตั้งเพื่อใช้งานในจุดประสงค์หนึ่ง และผู้ผลิตซอฟต์แวร์นั้นก็ย่อมจะต้องการทราบลักษณะการใช้งานของผู้ใช้เพื่อใช้เป็นข้อมูลในการปรับปรุงซอฟต์แวร์ของตนต่อไป จึงล่วงละเมิดผู้ใช้โดยแอบติดตั้งโปรแกรมในส่วนของการรายงานผล กลับไปยังผู้ผลิตด้วย ผู้ใช้โดยส่วนใหญ่จะไม่เห็นด้วยกับการละเมิดนี้เนื่องจากเห็นว่าเป็นการละเมิดสิทธิและความเป็นส่วนตัว และก็ได้มีการฟ้องร้องบริษัทผู้ผลิตที่กระทำเช่นนี้มาหลายกรณีแล้วและส่งผลให้มีการแก้ไขซอฟต์แวร์เพื่อมิให้กระทำการล่วงละเมิดผู้ใช้อีกต่อไป

อย่างไรก็ตามก็ยังคงมีบริษัทผู้ผลิตซอฟต์แวร์อีกหลายบริษัทที่ยังคงรวบรวมข้อมูลส่วนตัวของผู้ใช้อยู่อย่างลับๆ ผู้ใช้จึงต้องระมัดระวังและอ่านข้อมูลและเงื่อนไขการติดตั้งของโปรแกรมใดๆ ที่ต้องการติดตั้ง โดยส่วนใหญ่แล้วในระหว่างการติดตั้งผู้ใช้สามารถเลือกที่จะไม่ให้ทำการรายงานข้อมูลกลับไปยังบริษัทได้ แต่จะต้องใช้ความระมัดระวังว่ามีขั้นตอนใดที่จะเป็นตัวเลือกดังกล่าว เนื่องจากบางบริษัทมีความต้องการที่จะได้รับทราบข้อมูลของผู้ใช้งานเป็นอย่างมาก จึงใช้วิธีการต่างๆ ที่จะปกปิดการติดตั้งสปายแวร์ลงไปยังเครื่องคอมพิวเตอร์ของผู้ใช้

เว็บบัก (Web Bug) ก็เป็นอีกรูปแบบหนึ่งของสปายแวร์ เว็บบักเป็นโปรแกรมเล็กๆ ที่มองเห็นเป็นไฟล์รูปภาพเล็กๆ อยู่บนเว็บเพจหรือในข้อความอีเมล์ที่ส่งมาเป็นแบบ HTML ซึ่งโดยส่วนใหญ่แล้วผู้ใช้จะไม่สามารถสังเกตเห็นได้อย่างชัดเจน เว็บบักจะทำงานร่วมกับคุกกี้เพื่อเก็บรวบรวมข้อมูลลักษณะนิสัยการท่องเว็บของผู้ใช้ การป้องกันเว็บบักที่ดีที่สุดคือการตั้งค่าการรับคุกกี้ในบราวเซอร์ที่ใช้งานให้มีค่าความปลอดภัยสูงที่สุดเท่าที่จะยอมรับได้

คำแนะนำ

- ตรวจสอบและปรับแต่งการตั้งค่าสำหรับคุกกี้ในเว็บบราวเซอร์ที่ใช้งานให้มีความเหมาะสม
- ดาวน์โหลดโปรแกรมตรวจสอบสปายแวร์มาใช้งาน เช่นโปรแกรม “Ad-aware” (www.lavasoft.de)
- อ่านนโยบายของเว็บไซต์ที่เข้าไปชมว่าเว็บนั้นจะนำข้อมูลส่วนตัวของผู้ใช้ไปใช้งานอย่างไรและเว็บนั้นใช้สปายแวร์ในการเก็บรวบรวมข้อมูลหรือไม่
- ติดตั้งโปรแกรมไฟร์วอลล์และปรับปรุงให้ทันสมัยอยู่เสมอ

แหล่งข้อมูลเพิ่มเติม

www.bugnosis.org

grc.com/optout.htm

www.spychecker.com

โปรแกรมโทรจัน (Trojan Programs)

โปรแกรมโทรจันเข้ามาสู่เครื่องที่ใช้งานโดยที่ผู้ใช้อาจจะไม่รู้ตัวและจะทำงานอยู่เบื้องหลังซึ่งทำให้เป็นการยากที่จะตรวจจับได้ โดยทั่วไปแล้วโปรแกรมโทรจันจะแฝงมากับโปรแกรมอื่น สาเหตุที่เราเรียกกันว่า “โทรจัน” นั้นเป็นการอุปมาอุปไมยซึ่งเทียบได้กับม้าโทรจันในนิยายปรัมปราของกรีก ม้าโทรจันนี้เมื่อดูจากภายนอกแล้วก็เหมือนม้าที่ทำด้วยไม้ธรรมดาๆ ที่ถูกส่งเข้าไปในตัวเมือง แต่ข้างในตัวม้าจะแฝงไว้ด้วยข้าศึกติดเข้ามาด้วย ซึ่งเมื่อเข้าไปในตัวเมืองแล้ว ก็จะสามารถเข้าไปเปิดประตูเมืองให้กับฝ่ายศัตรูเข้ามาได้ โปรแกรมโทรจันจึงทำงานเป็น “ไส้ศึก” ในลักษณะเดียวกับม้าโทรจันนั่นเอง โปรแกรมโทรจันอาจจะติดมากับไฟล์ที่ส่งมาทางอีเมล์ มาจากการแลกเปลี่ยนโปรแกรมกันในห้องสนทนา มาจากไฟล์ที่อยู่ในฟล็อปปี้ดิสก์หรือโปรแกรมที่ก็อปปี้กันมา และวิธีอื่นๆ อีกมากมาย

โปรแกรมโทรจันแบ่งออกเป็น 3 ชนิดหลักๆ ดังนี้

- โปรแกรมเข้าถึงเครื่องคอมพิวเตอร์จากทางไกล (Remote Access Tools – RATs) โปรแกรมประเภทนี้จะทำให้ผู้บุกรุกระบบจากทางไกล เช่น โดยผ่านทางเครือข่ายเข้ามา สามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ถูกติดตั้งโทรจันลงไป
- ตัวจับการพิมพ์แป้นคีย์บอร์ด (Key Loggers) โปรแกรมประเภทนี้จะบันทึกการพิมพ์จากแป้นคีย์บอร์ดทั้งหมดที่ป้อนเข้าเครื่อง แล้วรวบรวมส่งเป็นไฟล์ให้ผู้บุกรุกต่อไป
- ตัวจับรหัสผ่าน (Password Retrievers) โปรแกรมประเภทนี้จะนำส่งไฟล์รหัสผ่านในเครื่องของผู้ใช้ให้แก่ผู้บุกรุก

การดาวน์โหลดไฟล์โปรแกรมโทรจันมาแต่ยังไม่ได้สั่ง “รัน” หรือ “เอ็กซีคิวต์” ไฟล์นั้น จะยังไม่ทำให้โปรแกรมโทรจันเริ่มต้นการทำงาน ผู้ใช้ต้องระมัดระวังในการทำงานกับไฟล์ประเภทเวิร์ดหรือสเปรดชีตด้วย ทั้งนี้เนื่องจากไฟล์ประเภทนี้อาจมีมาโครที่สามารถสั่งให้เครื่องทำงานได้ มีไวรัส หรือโทรจันแอบแฝงมาด้วย

โปรแกรมโทรจันกับไวรัสคอมพิวเตอร์ (ให้ดูในหัวข้อ**ไวรัส**) แม้ไม่ใช่เป็นสิ่งเดียวกัน แต่โปรแกรมป้องกันไวรัสหลายโปรแกรมจะสามารถตรวจจับหาโปรแกรมโทรจันได้

คำแนะนำ

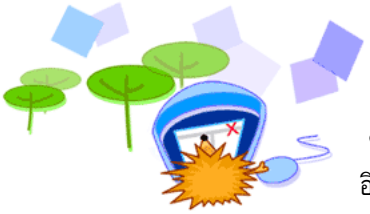
- ติดตั้งโปรแกรมไฟร์วอลล์บนเครื่องคอมพิวเตอร์ที่ใช้งาน
- หมั่นปรับปรุงไฟล์รูปแบบไวรัสของโปรแกรมป้องกันไวรัสให้มีความทันสมัยอยู่เสมอ
- ใช้โปรแกรมป้องกันไวรัสตรวจสอบโปรแกรมที่กำลังจะติดตั้งและใช้งานก่อนทุกครั้ง
- ใช้โปรแกรมป้องกันไวรัสตรวจสอบเครื่องคอมพิวเตอร์ที่ใช้งานทั้งเครื่องอย่างน้อยสัปดาห์ละหนึ่งครั้ง

แหล่งข้อมูลเพิ่มเติม

www.cert.org

ไวรัส (Viruses)

ไวรัสคอมพิวเตอร์เป็นคำอุปมาอุปไมยที่เทียบได้กับไวรัสทางชีวภาพ เนื่องจากไวรัสคอมพิวเตอร์สามารถแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งในลักษณะที่คล้ายกันกับการแพร่กระจายของเชื้อไวรัสทางชีวภาพจากคนหนึ่งไปสู่อีกคนหนึ่ง ในยุคที่ยังไม่มีการใช้เครือข่ายอินเทอร์เน็ตอย่างแพร่หลายไวรัสจะแพร่กระจายโดยผ่านทางการใช้งานแผ่นฟล็อปปี้ดิสก์ร่วมกัน แต่ในปัจจุบันไวรัสสามารถแพร่กระจายได้หลายๆ ทาง เช่น อีเมล์โปรแกรมต่างๆ เกม รวมทั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต



ไวรัสเป็นโปรแกรมชนิดหนึ่งซึ่งผลกระทบของไวรัสจะขึ้นอยู่กับว่าโปรแกรมไวรัสนั้นได้รับการออกแบบมาโดยมีจุดมุ่งหมายอะไร ไวรัสบางตัวได้รับการออกแบบมาให้ทำให้ไฟล์ในระบบเกิดความเสียหายหรือไปขัดขวางการทำงานของระบบให้ไม่สามารถทำงานได้ตามปกติ ไวรัสทุกชนิดแม้แต่ชนิดที่จัดว่ามีความรุนแรงน้อยก็มีศักยภาพในการทำลายไฟล์ให้เกิดความเสียหายได้ แต่สิ่งที่ไวรัสไม่สามารถทำได้คือการทำให้ฮาร์ดแวร์ของเครื่องคอมพิวเตอร์ได้รับความเสียหาย ดังนั้นข่าวหรือข้อมูลที่ได้รับที่ว่าไวรัสจะสามารถทำให้ซีพียูของเครื่องละลาย ทำลายฮาร์ดไดรฟ์ ทำให้จอภาพระเบิด ฯลฯ ล้วนเป็นข้อมูลเท็จหรือเป็นสิ่งที่เราเรียกกันว่าไวรัสหลอก (hoax)

ผู้ใช้งานคอมพิวเตอร์อาจเคยได้รับคำเตือนจากเพื่อนหรือผู้ร่วมงานเกี่ยวกับเรื่องไวรัสอันตราย ซึ่งในหลายเรื่องจะเป็นเรื่องของไวรัสหลอกที่ผู้ที่รู้เท่าไม่ถึงการณ์ส่งต่อๆ กันมา อย่าส่งต่ออีเมล์ไวรัสหลอกลวงเหล่านี้เนื่องจากยิ่งจะทำให้อีเมล์เพิ่มขึ้นเป็นจำนวนมากและไปกีดขวางทางเดินของข้อมูลบนเครือข่าย รวมทั้งจะทำให้บรรลุวัตถุประสงค์ของผู้ที่ส่งไวรัสหลอกนี้ออกมาเป็นคนแรก หากหมั่นปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอแล้ว ก็ไม่มีความจำเป็นต้องสนใจกับคำเตือนประเภทนี้แต่อย่างใด

คำแนะนำ

- ใช้โปรแกรมป้องกันไวรัสรุ่นล่าสุดและให้ทำการตรวจสอบไฟล์ในเครื่องอย่างสม่ำเสมอ
- ไม่เปิดไฟล์ที่มาจากแหล่งที่ไม่รู้จักหรือไม่ได้คาดหมายไว้ ให้เปิดไฟล์ได้ก็ต่อเมื่อสามารถตรวจสอบได้ว่าไฟล์นั้นเป็นไฟล์อะไร ส่งมาจากใคร และมีจุดประสงค์อะไร ให้ตรวจสอบทุกไฟล์ก่อนเปิดโดยไม่มีข้อยกเว้น แม้กระทั่งไฟล์แนบในอีเมล์ที่ระบุว่ามาจากเพื่อนสนิท เนื่องจากเป็นไปได้ว่าผู้บุกรุกอาจบุกรุกเข้าไปในเครื่องของเพื่อนสนิทนั้นและได้อีเมล์แอดเดรสของท่านมา
- ให้ตรวจสอบข้อมูลไวรัสหลอกได้จากแหล่งข้อมูลเพิ่มเติม หากไม่แน่ใจว่าอีเมล์หรือข้อมูลที่ได้รับนั้นเป็นเรื่องจริงหรือไม่

แหล่งข้อมูลเพิ่มเติม

www.symantec.com

www.mcafee.com

www.europe.f-secure.com/news/hoax.htm (ข้อมูลไวรัสหลอก)

แนวทางปฏิบัติ

แนวทางปฏิบัติสำหรับการรับส่งอีเมล์

- ให้ตระหนักอยู่เสมอว่าข้อความใดๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็น และอ่านได้โดยผู้อื่น ดังนั้นการส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป
- ไม่เปลี่ยนแปลงหรือแก้ไขข้อความอีเมล์ดั้งเดิมที่ได้รับมาและต้องการส่งต่อไป และหากอีเมล์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัว ให้ขออนุญาตผู้ส่งก่อนที่จะส่งต่ออีเมล์นั้นไป
- ไม่ส่งอีเมล์ที่เป็นลูกโซ่ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับอีเมล์ลูกโซ่และมีข้อความขอให้ส่งต่ออีเมล์นั้น ให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที
- ใช้ความระมัดระวังในการตอบอีเมล์สำหรับบางอีเมล์แอดเดรส เนื่องจากแอดเดรสบางแอดเดรสดูเหมือนเป็นแอดเดรสสำหรับผู้รับเพียงคนเดียว แต่แท้จริงแล้วอาจเป็นแอดเดรสรวมที่ส่งถึงผู้รับหลายคน
- หากอีเมล์มีความยาวกว่า 100 บรรทัด ให้แจ้งให้ผู้รับทราบโดยระบุไว้ในซับเจ็กต์ (Subject) ของอีเมล์ว่าข้อความที่ส่งมาให้มีความยาวมาก
- ในการตอบอีเมล์ที่เป็นภาษาอังกฤษ ให้ใช้ตัวอักษรทั้งตัวใหญ่และตัวเล็กตามหลักภาษาอังกฤษที่ถูกต้องและตามธรรมเนียมบนอินเทอร์เน็ตที่ใช้กัน ไม่ใช้ตัวอักษรตัวใหญ่ทั้งหมดซึ่งจะถือว่าเป็นการตะโกน
- ใช้สัญลักษณ์ เช่น :-) ซึ่งหมายถึงอารมณ์ดี :-(ซึ่งหมายถึงไม่มีความสุข หรืออื่นๆ ให้น้อยที่สุด เนื่องจากบางแห่งหรือบางวัฒนธรรมจะไม่เข้าใจความหมายของสัญลักษณ์เหล่านี้
- ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน

- อีเมล์ที่มีข้อมูลส่วนบุคคลควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)
- ใส่ชื่อหัวข้อเรื่องในซับเจ็กต์ของอีเมล์เพื่อแสดงถึงเรื่องของอีเมล์ที่ต้องการหารือหรือแจ้งให้ทราบ
- ส่งอีเมล์ตอบกลับสั้นๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับอีเมล์นั้นแล้วและจะตอบกลับอย่างสมบูรณ์ในภายหลัง
- ไม่ส่งอีเมล์ประเภทโฆษณาที่ผู้รับไม่ได้ร้องขอให้ผู้ส่งส่งมาให้ (การส่งเมล์ในลักษณะนี้ถือเป็นสิ่งที่ไม่เหมาะสมและในบางประเทศถือเป็นสิ่งที่ผิดกฎหมาย)
- ไม่ส่งไฟล์ที่มีขนาดใหญ่ซึ่งมีขนาดตั้งแต่ 150 กิโลไบต์ขึ้นไป
- ให้พิจารณาใช้ “BCC” (blind carbon copy – สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งอีเมล์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมาก

แนวทางปฏิบัติสำหรับการใช้งานเมล์ลิ่งลิสต์

- ให้ศึกษาข้อมูลในเมล์ลิ่งลิสต์ที่เข้าไปมีส่วนร่วมอย่างน้อย 1-2 เดือนก่อนที่จะเริ่มต้นส่งข้อความเข้าไปในกลุ่มนั้น
- ให้ประพฤติตนให้เหมาะสมในการตอบหรือแสดงความคิดเห็นในเมล์ลิ่งลิสต์
- ใช้ความระมัดระวังในการส่งข้อความใดๆ ที่อาจทำให้รู้สึกเสียใจในภายหลังได้
- ใช้ข้อความที่สั้นและตรงประเด็น
- ไม่ส่งข้อความประเภทโฆษณาลงไปในเมล์ลิ่งลิสต์ เว้นแต่เมล์ลิ่งลิสต์นั้นจะอนุญาตให้ทำได้
- ให้ตอบข้อความที่ผู้อื่นลงไว้ก่อนหน้าโดยลงอย่างน้อยส่วนหนึ่งของข้อความเดิมไว้ด้วยเพื่อให้ผู้อ่านในเมล์ลิ่งลิสต์สามารถเข้าใจการตอบนั้นได้
- ระมัดระวังที่จะไม่ตอบข้อความที่เป็นเรื่องส่วนตัวลงไปในเมล์ลิ่งลิสต์

- ให้รีบส่งคำขอโทษตามลงไปโดยทันที หากไม่ได้ตั้งใจส่งข้อความหนึ่งที่เป็นเรื่องส่วนตัวลงไปเมล์ลิ่งลิสต์
- ส่งอีเมล์แสดงความรู้สึกโดยส่งไปให้เฉพาะบุคคลผู้นั้นเป็นการส่วนตัว หากต้องการแสดงความรู้สึกส่วนตัวที่รุนแรงที่มีต่อข้อความของผู้นั้น
- ไม่เข้าไปเกี่ยวข้องกับสภาวะการถกเถียงที่ไม่มีข้อยุติ (flame wars) และไม่ลงข้อความหรือตอบโต้ต่อข้อความที่จะเป็นชนวนแห่งการโต้เถียงกันอย่างไม่รู้จบ
- ไม่ใช้ตัวอักษร (Font) ที่ไม่เป็นมาตรฐานกับข้อความที่ส่งไป เนื่องจากตัวอักษรเหล่านี้อาจแสดงผลออกมาไม่เหมือนกันในเครื่องที่แตกต่างกันและอาจทำให้ผู้รับอ่านตัวอักษรนั้นได้ยาก
- ส่งอีเมล์เพื่อขอสมัครเข้าเป็นสมาชิกของเมล์ลิ่งลิสต์และยกเลิกการเป็นสมาชิกไปยังอีเมล์แอดเดรสที่ระบุไว้
- ให้ยกเลิกการเป็นสมาชิกในเมล์ลิ่งลิสต์หนึ่ง หากไม่สามารถตรวจหรือรับอีเมล์จากเมล์ลิ่งลิสต์นั้นได้เป็นระยะเวลานาน
- ให้กล่าวคำขอโทษถึงผู้รับที่ไม่ได้เกี่ยวข้องโดยตรงในกรณีที่ลงข้อความหนึ่งในหลายๆ เมล์ลิ่งลิสต์ที่มีความเกี่ยวข้องกัน (ซึ่งเราเรียกกันว่า cross-posting) แต่ข้อความนั้นอาจไม่เกี่ยวข้องโดยตรงกับบางเมล์ลิ่งลิสต์
- ไม่บอกชื่อบัญชีผู้ใช้หรือรหัสผ่านที่ใช้งานกับเมล์ลิ่งลิสต์ให้ผู้อื่นทราบ
- ใช้รูปแบบวันเดือนปีในรูปแบบดังนี้ “11 Feb 2002” เพื่อหลีกเลี่ยงความเข้าใจผิดในการแสดงวันเดือนปี
- ใช้คำย่อได้ตามความจำเป็นแต่ไม่ใช้มากจนเกินไปเนื่องจากจะทำให้ผู้อ่านเกิดความสับสนและเป็นที่น่ารำคาญได้ ตัวอย่างคำย่อที่ใช้กันบ่อยๆ ในภาษาอังกฤษ เช่น

  IMHO = in my humble/honest opinion (ตามความรู้อันไม่มากนักของฉัน)

  FYI = for your information (เพื่อเป็นข้อมูลให้ทราบ)

  BTW = by the way (นอกจากนี้)

แนวทางการสร้างเว็บไซต์ที่แสดงถึงการประกอบการที่ดีต่อผู้บริโภค

ทางด้านข้อมูลทั่วไปขององค์กร

1. ให้อธิบายถึงลักษณะของธุรกิจอย่างชัดเจน
2. ให้ข้อมูลในเรื่องต่อไปนี้
    - ที่อยู่ทางกายภาพขององค์กร (ที่อยู่จริงทางไปรษณีย์)
    - อีเมล์แอดเดรสหรือหมายเลขโทรศัพท์ที่ผู้บริโภคสามารถใช้ติดต่อองค์กรได้โดยตรง

ทางด้านข้อมูลของผู้บริโภค

1. ระบุไว้อย่างชัดเจนว่าต้องการข้อมูลอะไรบ้างจากผู้บริโภค และจะนำข้อมูลดังกล่าวไปใช้งานอย่างไรและไปใช้ร่วมกับใครบ้าง
2. อธิบายมาตรการรักษาความปลอดภัยเพื่อสร้างความปลอดภัยในการทำธุรกรรมบนเว็บไซต์
3. ทำความเข้าใจกฎหมายเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของลูกค้าซึ่งมีถิ่นฐานอยู่ในประเทศอื่น

ทางด้านการโฆษณาและการตลาด

1. ให้ข้อมูลที่ถูกต้องและเป็นจริงเกี่ยวกับสินค้าและธุรกิจขององค์กร
2. ให้การรับรองต่อทุกคำพูดที่ระบุไว้เกี่ยวกับสินค้าและบริการขององค์กร
3. ให้เปิดเผยผู้ลงโฆษณาทั้งหมดซึ่งเป็นผู้ให้การสนับสนุนเว็บไซต์ขององค์กร
4. ให้เคารพในการตัดสินใจของผู้บริโภคที่เลือกที่จะไม่รับโฆษณาทางอีเมล์จากองค์กร
5. ให้ใช้ความระมัดระวังเป็นพิเศษเมื่อทำการโฆษณาที่เกี่ยวข้องกับเด็กและเยาวชน

ทางด้านการขาย

1. ระบุไว้อย่างชัดเจนเกี่ยวกับสินค้าที่ขาย และมีข้อมูลรายละเอียดอย่างเพียงพอต่อผู้บริโภค รวมทั้งเงื่อนไขต่างๆ ในการซื้อขาย
2. ระบุค่าใช้จ่ายทั้งหมดที่เกี่ยวข้องในการซื้อสินค้าซึ่งรวมถึงค่าส่ง ค่าบรรจุหีบห่อ และค่าใช้จ่ายเพิ่มเติมอื่นๆ ด้วย และระบุสกุลเงินตราที่ใช้ด้วย
3. ระบุข้อจำกัดหรือข้อห้ามใดๆ ที่อาจมีในการซื้อสินค้า
4. ระบุข้อมูลเรื่องการประกันสินค้า
5. ระบุวันเวลาโดยประมาณที่ผู้ซื้อจะได้รับสินค้า ระบุหมายเลขสำหรับติดตามสินค้าและเว็บไซต์ของบริษัทขนส่งเพื่อให้ผู้ซื้อสามารถติดตามสินค้าได้
6. อธิบายวิธีการชำระเงินแบบต่างๆ ไว้อย่างชัดเจน

ทางด้านการคุ้มครองผู้บริโภค

1. อธิบายนโยบายการคืนสินค้า วิธีการส่งสินค้ากลับ การขอยกเลิกการใช้เครดิตที่ใช้ไปแล้วนั้น รวมทั้งการแลกเปลี่ยนสินค้าใหม่
2. ระบุเงื่อนไขทั้งหมดในการคืนสินค้า
3. ให้ข้อมูลที่อยู่ติดต่อขององค์กรในกรณีที่ผู้บริโภคต้องการจะติดต่อเมื่อมีปัญหาหรือต้องการร้องเรียน
4. จัดทำหลักฐานการทำธุรกรรมระหว่างองค์กรกับผู้บริโภค ซึ่งอาจเป็นข้อมูลบนเว็บไซต์ให้ผู้บริโภคบันทึกเก็บไว้ได้ หรืออาจเป็นข้อมูลยืนยันการทำธุรกรรมซึ่งส่งไปทางอีเมล์
5. มีนโยบายกล่าวไว้บนเว็บอย่างชัดเจนเกี่ยวกับการเก็บรักษาความลับของข้อมูลส่วนตัวของผู้บริโภค
6. เคารพสิทธิของผู้บริโภคในการที่จะเลือกหรือไม่เลือกที่จะมีส่วนร่วมในกิจกรรมต่างๆ เช่น การรับอีเมล์ข่าวสาร หรือการรับอีเมล์โฆษณาจากผู้ค้ารายอื่น
7. ให้ข้อมูลเกี่ยวกับวิธีการไกล่เกลี่ยข้อขัดแย้งที่อาจเกิดขึ้นจากการซื้อขาย

แนวทางปฏิบัติในการสั่งซื้อสินค้าบนเครือข่ายอย่างปลอดภัย

การซื้อสินค้าบนอินเทอร์เน็ตเป็นสิ่งที่กระทำได้ง่ายและสะดวกสบาย แต่ผู้บริโภคควรมั่นใจว่าสามารถทำได้อย่างปลอดภัยและเชื่อถือได้ ให้ปฏิบัติตามแนวทาง ดังต่อไปนี้เมื่อมีความจำเป็นต้องซื้อสินค้าบนอินเทอร์เน็ต

- ติดต่อกับบริษัทที่มีความเชื่อถือได้สูง เช่น อาจเป็นบริษัทที่เพื่อนแนะนำจากประสบการณ์ที่เคยซื้อกับบริษัทนี้
- ตรวจสอบรายละเอียดของบริษัท เช่น ที่อยู่จริงและหมายเลขโทรศัพท์ เพื่อให้มั่นใจได้ว่าสามารถติดต่อกับบริษัทได้เมื่อเกิดปัญหาหรือเมื่อต้องการร้องเรียน
- อ่านและทำความเข้าใจนโยบายการเก็บรักษาความลับของลูกค้าของเว็บนั้นและการนำข้อมูลส่วนตัวของลูกค้าไปใช้งาน นโยบายนี้ต้องระบุว่าจะมีการเก็บรวบรวมข้อมูลอะไรบ้าง หากไม่พบนโยบายนี้บนเว็บ ให้ส่งอีเมล์หรือจดหมายเพื่อสอบถามหรือขอให้ทางบริษัทลงนโยบายนี้บนเว็บไซต์ หลายๆ บริษัทจะเคารพสิทธิของลูกค้าว่าจะยอมให้ใช้ข้อมูลส่วนตัวหรือไม่ เช่น การนำอีเมล์แอดเดรสของลูกค้าไปใช้เพื่อการตลาดหรือให้กับผู้ค้ารายอื่น เป็นต้น
- ตรวจสอบว่าสามารถยอมรับในนโยบายการคืนสินค้าและคืนเงินของบริษัทหรือไม่ เนื่องจากไม่ใช่ทุกบริษัทที่จะยอมให้มีการคืนสินค้าหรือคืนเงิน บางบริษัทจะยอมให้เป็นเครดิตเพื่อการซื้อสินค้าอื่นๆ แทน บางบริษัทจะคิดค่าธรรมเนียมการคืน ส่วนใหญ่จะไม่คืนค่าขนส่งและค่าประกันการส่งสินค้า
- อ่านและทำความเข้าใจอย่างชัดเจนเกี่ยวกับเงื่อนไขการรับประกันสินค้าบางประเภท เช่น เครื่องใช้อิเล็กทรอนิกส์ หรือคอมพิวเตอร์มือสอง
- เข้าสู่ระบบการขายสินค้าโดยใช้รหัสผ่านที่ยากต่อการเดา (ดูหัวข้อ **รหัสผ่าน**) ไม่บอกรหัสผ่านของตนแก่ผู้อื่น และไม่เลือกให้มีการจำรหัสผ่านสำหรับเข้าเว็บนั้น
- ตรวจสอบรายละเอียดทั้งหมดของการสั่งซื้อ เช่น ชนิดของสินค้า ขนาด จำนวน รูปร่าง สี ที่อยู่ที่จะใช้รับสินค้า และการคิดเงิน รวมถึงราคาสินค้า

ค่าบรรจุหีบห่อ ค่าขนส่ง และภาษีด้วย ทั้งหมดนี้ต้องถูกต้องก่อนที่จะยืนยันการสั่งซื้อสินค้านั้น

- ตรวจสอบว่าการทำธุรกรรมโดยผ่านทางเว็บเพจขององค์กรได้รับการเสริมความปลอดภัยแล้ว (ดูหัวข้อ**เว็บเพจ**ที่ได้รับการเสริมความปลอดภัย)
- เก็บใบเสร็จรับเงินไว้ เช่น สั่งพิมพ์หน้าเว็บที่มีรายละเอียดของการสั่งซื้อสินค้านั้น (เว็บบางเว็บจะแนะนำให้ลูกค้าสั่งพิมพ์หน้าเว็บนั้นและเก็บไว้ ส่วนบางเว็บจะส่งใบเสร็จให้โดยผ่านทางอีเมล์)
- ให้สั่งพิมพ์สัญญาการเป็นสมาชิกและทำความเข้าใจกับวิธีการยกเลิกการเป็นสมาชิก ในกรณีที่สั่งซื้อโดยการสมัครเข้าเป็นสมาชิกทางเว็บของนิตยสารหรือ สิ่งตีพิมพ์อื่นๆ
- ตรวจสอบว่ามีวิธีการติดตามว่าสถานะของการส่งมอบสินค้าที่สั่งซื้อได้ดำเนินการไปถึงไหนแล้ว

แนวทางปฏิบัติในการประมูลสินค้าบนเครือข่าย

ก่อนที่จะเข้าประมูลหรือซื้อสินค้าบนอินเทอร์เน็ต ให้ปฏิบัติดังนี้

- อ่านให้แน่ใจในรายละเอียดของสินค้าที่จะทำการประมูล ซึ่งรวมถึงวิธีการชำระเงิน ค่าบรรจุหีบห่อ ค่าขนส่ง การรับประกัน และนโยบายการคืนสินค้า หากยังไม่เข้าใจหรือไม่แน่ใจในสิ่งใด ให้ติดต่อกับผู้ขายโดยใช้อีเมล์ ให้ระมัดระวังผู้ขายที่ไม่ตอบอีเมล์หรือให้คำตอบที่ไม่เป็นที่พอใจ
- หาข้อมูลเกี่ยวกับสินค้านั้นทั้งจากแหล่งข้อมูลบนอินเทอร์เน็ตและนอกอินเทอร์เน็ต รวมทั้งพยายามหาราคาจริงในตลาดให้ได้ก่อนเข้าประมูล
- ตรวจสอบรูปของสินค้าที่ให้ไว้บนเว็บอย่างละเอียดเพื่อดูสภาพของสินค้านั้น

- ตรวจสอบประวัติของผู้ขายในเว็บประมูลนั้น ซึ่งเว็บประมูลส่วนใหญ่จะมีข้อมูลนี้อยู่ ให้ดูว่าผู้ขายนั้นมีความเกี่ยวข้องกับเว็บประมูลนั้นมาเป็นระยะเวลานานเท่าใด (ยิ่งนานจะยิ่งดี) หากผู้ขายนั้นเป็นรายใหม่ ให้ติดต่อกับผู้ขายนั้นโดยตรงทางอีเมล์หรือทางโทรศัพท์ก่อนเพื่อขอทราบข้อมูลเกี่ยวกับผู้ขาย
- ตรวจสอบนโยบายการทำธุรกิจและเงื่อนไขการขายของผู้ขาย
- ตรวจสอบวันและเวลาในการส่งมอบสินค้าที่แน่นอน
- ตรวจสอบว่าสินค้าที่จะประมูลไม่เป็นสิ่งอันตรายหรือสิ่งผิดกฎหมาย
- กำหนดราคาประมูลสูงสุดที่สามารถจ่ายได้ไว้ก่อน พึงระลึกว่าการเข้าร่วมการประมูลเท่ากับถูกบังคับโดยทางสัญญาหรือข้อกำหนดให้จ่ายเงินชำระสินค้าที่ประมูลได้นั้น
- เมื่อต้องการประมูลสินค้าที่มีราคาสูงหรือไม่มั่นใจในการประมูลหนึ่ง ให้ใช้บริการให้คำปรึกษาจากเว็บประมูลนั้น หรือสอบถามจากผู้ที่คุ้นเคยหรือรู้จักสินค้านั้น
- ให้บันทึกเว็บเพจทั้งหมดที่เกี่ยวข้องกับกระบวนการประมูลนั้น รวมทั้งอีเมล์สำหรับติดต่อกับผู้ขายด้วย เพื่อประโยชน์ในกรณีที่จำเป็นต้องติดต่อกับผู้ขายอีกในภายหลัง
- ระมัดระวังไม่เปิดเผยข้อมูลส่วนตัวมากเกินไปในระหว่างที่ติดต่อกับผู้ขาย

ออกแบบรูปเล่มโดย

งานประชาสัมพันธ์และผลิตสื่อ