บทที่ 2

ความสำคัญของปัญหาจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์

2.1 คำนิยามและความหมายของสแปมเมล (Spam Mail)

การให้คำนิยาม หรือคำจำกัดความของ "สแปมเมล" (Spam Mail) ซึ่งเป็นเพียงคำแสลงในภาษาอังกฤษอย่างตรงตัวนั้น เป็นการยากและยังมีความเห็นที่หลากหลาย อย่างไรก็ดี จากการศึกษาพบว่า ถ้อยคำที่นำมาใช้แทนคำเรียกสแปมเมลที่เป็นทางการมากที่สุดในต่างประเทศนั้น มักจะใช้คำว่า "Unsolicited Commercial Email (UCE)" ซึ่งพบได้ในกฎหมาย Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN SPAM Act of 2003) ของสหรัฐฯ หรือคำว่า "Unsolicited Bulk Email (UBE)" ที่ใช้กล่าวอ้างถึงสแปมเมลในบทความหลายๆ ฉบับ ซึ่งความหมายถึง จดหมายอิเล็กทรอนิกส์เชิงพาณิชย์ที่ถูกส่งมาโดยผู้รับไม่ได้ให้ความยินยอม กับจดหมายอิเล็กทรอนิกส์จำนวนมหาศาลที่ถูกส่งมาโดยผู้รับไม่ได้ให้ความยินยอม ในขณะที่ E-Privacy Directive 2002/58/EC ของกลุ่มประเทศสหภาพยุโรปนั้น ใช้คำว่า "Unsolicited Communication"* ในการสื่อความหมายถึง "วิธีการสื่อสารโดยระบบอัตโนมัติที่ไม่ได้รับความยินยอมจากผู้รับก่อน" ซึ่งกินความรวมถึงวิธีการสื่อสารโดยผ่านทางอีเมลด้วย อย่างไรก็ดี การให้ความหมายในกรณีนี้ อาจจะกว้างเกินไป เพราะปกติเรามักจะได้รับอีเมลทุกวัน โดยที่ผู้ส่งก็มิเคยได้รับอนุญาตให้ส่งเป็นการล่วงหน้าแต่อย่างใด ดังนั้นจึงเป็นการยากที่จะให้คำจำกัดความสแปมเมลโดยใช้ถ้อยคำเพียงคำเดียวได้ ซึ่งนอกจากจะไม่ชัดเจนแล้ว ก็ยังก่อให้เกิดความสับสนจากการพยายามให้ความหมายของคำว่า "สแปมเมล" ด้วย

ในประเทศไทยเอง ก็ยังไม่มีการบัญญัติศัพท์ที่จะนำมาใช้เรียกสแปมเมลโดยเฉพาะ แต่ก็มีผู้พยายามคิดค้นถ้อยคำเพื่อใช้เรียกสแปมเมลเอาไว้หลากหลาย เช่น จดหมายอิเล็กทรอนิกส์ที่ผู้รับ

---

* "Article 13 - Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent..."

ไม่พึงปรารถนา หรือจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงประสงค์ หรือจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่ต้องการ ทั้งนี้ก็โดยการพยายามเทียบเคียงความหมายกับคำว่า "Unsolicited Email" นั้นเอง อย่างไรก็ดี ฝ่ายวิจัยและพัฒนาสาขาสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติได้ให้ความหมายของคำว่า "สแปม" เอาไว้ในพจนานุกรมออนไลน์ LEXiTRON[1] ว่า "สแปม" หมายถึง "ขยะไปรษณีย์อิเล็กทรอนิกส์" ซึ่งก็อาจทำให้เกิดความสับสนกับคำว่า "Junk Mail" ได้ ส่วนศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย (ThaiCERT)[2] ก็ได้ให้ความหมายของคำว่า "สแปม" เอาไว้ว่า "การทำให้ผู้หนึ่งหรือ newsgroup หนึ่งเต็มไปด้วยข้อความที่ไม่เกี่ยวข้องและไม่เหมาะสม" ซึ่งเป็นการให้ความหมายในเชิงอธิบายลักษณะของสแปมมากกว่า

การพยายามที่จะหาคำจำกัดความของคำว่า "สแปมเมล" ซึ่งเป็นคำแสลงให้มีความหมายครบถ้วนตรงตัวนั้น เป็นการยากแม้แต่การให้คำนิยามในภาษาอังกฤษเอง อย่างไรก็ดี จากการศึกษา พบว่า "สแปมเมล" ก็คือ จดหมายขยะ (Junk Mail) รูปแบบหนึ่ง คือเป็นจดหมายหรือข้อความที่ผู้รับไม่ต้องการ แต่ลักษณะสำคัญของสแปมเมลนั้น คือจดหมายหรือข้อความถูกส่งมาจากที่ต่างๆ โดยผู้ส่งซึ่งอาจจะเป็นบุคคลธรรมดา หรือบริษัท ห้างร้านต่างๆ ได้ส่งไปยังอีเมล ของผู้รับอย่างต่อเนื่อง โดยส่งถึงผู้รับคราวละหลายๆ คน หรือหลายๆ ที่อยู่อีเมล โดยมิได้รับความยินยอมจากผู้รับหรือผู้รับไม่ได้ร้องขอ หรือคาดว่าจะได้รับ เพราะไม่เคยรู้จักกับผู้ส่งมาก่อน เพียงแต่ผู้ส่งใช้โปรแกรมในการส่งอีเมลแบบกระจายไปตามแหล่งต่างๆ ให้ทั่วเท่าที่จะสามารถส่งไปได้ สแปมเมลส่วนใหญ่จึงมักจะไม่ปรากฏชื่อและที่อยู่ของผู้ส่ง หรือหากปรากฏก็มักจะไม่ใช่ชื่อหรือที่อยู่ที่เป็นจริง ทำให้ผู้รับไม่สามารถที่จะหยุดยั้งสแปมเมลเหล่านั้นโดยการขอให้ผู้ส่งหยุดการส่งเมลเหล่านั้นได้ เพราะไม่สามารถติดต่อไปยังที่อยู่ของผู้ส่งที่แท้จริงได้ สแปมเมลเหล่านี้ก่อให้เกิดความรำคาญ และด้นทุนแก่ผู้รับ โดยที่ผู้รับต้องคอยลบสแปมเมลต่างๆ ที่ได้รับวันละหลายๆ ฉบับโดยแทบจะไม่เปิดอ่านเลย

จุดมุ่งหมายหลักของสแปมเมลส่วนใหญ่ก็คือ การเชิญชวนให้ซื้อสินค้า หรือแนะนำเว็บไซท์ทางการค้าที่เจ้าของเว็บไซต์จ่ายเงินจ้างแฮกเกอร์ให้สร้างสแปมเมลให้กับเว็บไซต์ของตน แต่สแปมเมลจะมีวัตถุประสงค์อื่นๆ อีกที่ไม่ใช่ในเชิงพาณิชย์ (หรือที่เรียกว่า Direct Marketing) ก็ได้ เช่น การโจมตีระบบ การส่งข้อความหมิ่นประมาท ใส่ร้ายป้ายสีคนอื่น หรือจุดประสงค์ทางการเมือง ฯลฯ

---

[1] http://lexitron.nectec.or.th/

[2] พ.ต. ปนิวัธน์ ทรัพย์รุ่งเรือง, "คำศัพท์ที่เกี่ยวข้องกับ computer security และ intrusion detection ฉบับปรับปรุงเวอร์ชัน 2.0," ที่ http://thaicert.org/paper/basic/paniwat2.0_r1.pdf (กุมภาพันธ์ 2549) : 54.

ซึ่งในปัจจุบันรูปแบบการส่งสแปมเมลนั้น มิได้จำกัดอยู่เพียงการส่งทางไปรษณีย์อิเลคทรอนิกส์ (E-mail) หรือที่เรียกว่า สแปมอีเมล หรือสแปมเมล เท่านั้น แต่ยังสามารถใช้รูปแบบการส่งสแปมไปทางโทรศัพท์มือถือเป็นข้อความสั้นๆ (SMS) หรือส่งเป็นภาพเคลื่อนไหว (MMS) หรือส่งทางเครื่องโทรสาร (Fax) ก็ได้ ดังนั้น คำว่า "สแปม" จึงนำมาใช้เพื่ออธิบายถึงวิธีการส่งข้อความโดยอัตโนมัติประเภทนี้โดยใช้รูปแบบอื่นๆ ด้วย (แต่ในการวิจัยครั้งนี้ จะเน้นเฉพาะการส่งสแปมทางอีเมลเท่านั้น) เหตุผลสำคัญที่ทำให้การตลาดออนไลน์ โดยวิธีการส่งสแปมเมลเป็นที่นิยมอย่างมากนั้น ก็เนื่องมาจากต้นทุนที่ต่ำมาก เมื่อเทียบกับการทำการตลาดโดยวิธีอื่น เช่น การแจกใบปลิวโฆษณา นั่นเอง

อย่างไรก็ดี ก็มีผู้ให้ความเห็นว่า[3] การจะมองว่าอะไรคือสแปมเมลนั้น ขึ้นอยู่กับตัวผู้รับเองเป็นสำคัญ เพราะสแปมเมลสำหรับบุคคลหนึ่ง ก็มิได้หมายความว่า จะถือเป็นสแปมเมลสำหรับอีกบุคคลหนึ่งเสมอไป นอกจากนี้ การส่งสแปมเมลถึงกลุ่มคนจำนวนมากๆ ก็มิได้จัดว่าจะเป็นการสแปมเสมอไป เช่นบริษัทฯ หรือกลุ่มอุตสาหกรรม ที่ต้องการจะส่งอีเมล ถึงกลุ่มคนจำนวนมาก ที่เป็นลูกค้า ดังนั้นองค์ประกอบสำคัญจึงน่าจะอยู่ที่ การส่งอีเมลเหล่านั้นได้รับอนุญาตจากผู้รับหรือไม่ ที่พอจะทำให้แยกแยะได้ว่าการกระทำอย่างไรจัดว่าเป็นการสแปม

2.2 ต้นกำเนิดและที่มาของคำว่า "สแปมเมล"

2.2.1 ต้นกำเนิดของสแปมเมล[4]

2.2.1.1 **ข้อสันนิษฐานเรื่อง** "Green Card Lottery"

รูปแบบการส่งข้อความที่เรียกว่า "สแปม" เกิดขึ้นตั้งแต่เมื่อไร และอย่างไรนั้น ต่างก็มีความคิดเห็นและข้อสันนิษฐานที่แตกต่างกันมากมาย อย่างไรก็ดี ข้อสันนิษฐานที่ถูกนำมากล่าวอ้างถึงมากที่สุดในการส่งสแปมเมลเป็นครั้งแรกนั้น เกิดขึ้นในเดือนเมษายน ปี 1994 โดยทนายความสองสามีภรรยาจากฟีนิก (Phoenix) ในรัฐอริโซนา ที่ชื่อว่า Canter และ Siegel ซึ่งเป็นผู้ที่ทำให้รูปแบบการส่งสแปมเมลกลายเป็นสิ่งที่ได้รับความนิยมในเวลาต่อมา ก่อนหน้านี้แม้ว่าพวกเขาจะทำการส่งข้อความในลักษณะดังกล่าวออกไปบ้าง แต่ก็เป็นการส่งไปยังกลุ่มคนจำนวนน้อย จนกระทั่งพวกเขา

---

[3] Steven Brightbill, "Spam vs. Legitimate Mass E-mail," at http://www.soundingline.com/magazine/2003/2003_May/spam_vs_legitimate_mass_email.htm (last visited March 2006).

[4] Brad Templeton, "Origin of the term "Spam" to mean net abuse," at http://www.templetons.com/brad/spamterm.html (last visited February 2006).

ได้ว่าจ้างนักโปรแกรมเมอร์ให้เขียนต้นฉบับโปรแกรมอย่างง่ายๆ เพื่อใช้ในการโพสท์ข้อความโฆษณาบริการที่เรียกว่า "Green Card Lottery"[5] ซึ่งเป็นรูปแบบที่ได้รับอนุมัติจากสภาคองเกรซของสหรัฐฯ ในช่วงต้นยุค 90 เพื่อเปิดโอกาสในการขอสัญชาติแก่ผู้ที่เข้ามาอยู่อาศัยในสหรัฐฯ แต่ในขณะเดียวกันก็เปิดโอกาสให้กับนักฉกฉวยในการทำเงินจากการคิดค่าธรรมเนียมที่สูง จากการเสนอบริการยื่นเอกสารที่จำเป็นต้องใช้ในการนี้ด้วย ทั้งนี้ ข้อความโฆษณาบริการของพวกเขาถูกโพสท์ลงบนกระดานข้อความของกลุ่มข่าว (newsgroups) ทุกแห่งบนยูสเนต (USENET) ซึ่งเป็นระบบการชุมนุมออนไลน์ที่ใหญ่ที่สุดในโลก ผลจากการนี้ทำให้กลุ่มข่าวที่มีมากกว่า 1,000 แห่งนั้น ต่างก็ได้รับข้อความโฆษณาของพวกเขากันโดยทั่ว

อย่างไรก็ดี แม้ว่าการกระทำดังกล่าวจะมิใช่ครั้งแรกที่การส่งข้อความถูกนำไปใช้ในทางที่ผิด และไม่ใช่ครั้งแรกที่มีการส่งข้อความจำนวนมากออกไป จนถูกเรียกว่า "สแปม" แต่การกระทำดังกล่าว นับเป็นการส่งข้อความออกไปโดยจงใจครั้งแรก ที่ได้รับการเรียกขานว่า "สแปม" โดยพร้อมเพรียงกันในเวลาต่อมา ซึ่งเมื่อมีการคิดค้นโปรแกรมเพื่อใช้ในการรวบรวมที่อยู่อีเมลจำนวนมากได้ และนำมาใช้เพื่อส่งอีเมลไปยังผู้รับจำนวนมากที่ไม่ได้ร้องขอ ถ้อยคำดังกล่าวก็ถูกนำมาใช้อย่างรวดเร็วเพื่ออธิบายถึงอีเมลขยะที่พวกเขาไม่ต้องการเหล่านี้ และได้กลายมาเป็นคำสามัญที่ใช้เรียกขานการกระทำเช่นนี้จนปัจจุบัน

2.2.1.2 ข้อสันนิษฐานเรื่อง "The MUDers"

ข้อสันนิษฐานนี้ เกิดจากการค้นคว้าวิจัยของ Brad Templeton[6] ซึ่งเป็นผู้ที่สนใจศึกษาและค้นคว้าเกี่ยวกับที่มาของ "สแปม" โดยเขาเห็นว่า "Green Card Lottery" นั้นไม่ได้สร้างคำว่า "สแปม" และก็มิใช่เป็นการส่งสแปมครั้งแรกด้วย แม้ว่าจะเป็นการส่งสแปมเชิงพาณิชย์ครั้งแรกที่ใหญ่ที่สุดก็ตาม

โดยจากการวิจัยของเขาพบว่า คำว่า "สแปม" นั้น เกิดขึ้นในช่วงปลายยุค 80 ในชุมชนที่เรียกว่า "MUD" (Multi-User-Dungeon) ซึ่งเป็นคำโบราณที่ใช้เรียกการสนทนาแบบเรียลไทม์ ระหว่างผู้ใช้หลายๆ คนภายใต้สภาวะการณ์อย่างเดียวกัน โดยผู้ใช้สามารถพูดคุย แลกเปลี่ยน

---

[5] Hitchcock, J.A, "Net crimes & misdemeanors : outmaneuvering the spammers, swindlers, and stalkers who are targeting you online : Spam Not In a Can," (2002) : 31.

[6] Brad Templeton, "Origin of the term "Spam" to mean net abuse," at http://www.templetons.com/brad/spamterm.html (last visited February 2006).

และโต้ตอบซึ่งกันและกันได้ ภายใต้สมมติฐานและหัวข้อสนทนาในสภาวการณ์นั้น การใช้คำว่า "MUD" ก็เพื่อเตือนให้คนนึกถึงเกมการผจญภัยครั้งแรกที่เรียกว่า "Dungeons and Dragons" ซึ่งเกี่ยวกับการร่วมกันสำรวจถ้ำ หรือกรุนักโทษ อันเป็นต้นแบบของเกม "EverQuest" และ "The Sims Online" ในเวลาต่อมา

ผู้คนใช้ "MUD" เพื่อการสนทนา พูดคุย และสร้างความประทับใจแก่ผู้อื่นด้วยวัตถุประสงค์ที่พวกเขาสร้างขึ้นมา ซึ่งนับเป็นครั้งแรกที่มีการพัฒนารูปแบบอย่างมากจากระบบห้องสนทนาโดยทั่วไป โดยคำว่า "สแปม" ถูกนำมาใช้กับพฤติกรรมที่แปลกแยกสองสามประการ คือ หนึ่ง พฤติกรรมในการโจมตีคอมพิวเตอร์ด้วยข้อมูลจำนวนมากเพื่อขัดขวางระบบการทำงาน หรือ สอง พฤติกรรมที่เรียกว่า "การสแปมฐานข้อมูล" (spam the database) ซึ่งเป็นการใช้โปรแกรมในการสร้างหัวข้อออกมาเป็นจำนวนมาก ซึ่งมากกว่าการสร้างสรรค์โดยตัวผู้เล่นเอง และบางครั้งก็นำมาใช้เพื่ออธิบายถึงการโจมตีการสนทนาด้วยกลุ่มข้อความที่แทรกเข้ามาโดยการใช้โปรแกรม (ซึ่งเรียกว่า "bot" ในปัจจุบันนี้) หรือการแทรกไฟล์ข้อมูลแทนการพิมพ์แบบเรียลไทม์จริงๆ

อย่างไรก็ดี ไม่มีการยืนยันว่าถ้อยคำดังกล่าวถูกนำมาใช้ใน "MUDs" ได้อย่างไรนับจากยุคแรกเริ่มของการมีระบบสนทนา โดย Rich Frueh[7] เชื่อว่า ถ้อยคำดังกล่าวน่าจะมีต้นกำเนิดมาจากการเปิดถ่ายทอดสัญญาณของบิทเนต (Bitnet's Relay) (ระบบสนทนาที่เรียกว่า IRC ในปัจจุบัน) ซึ่งเมื่อความสามารถในการป้อนไฟล์ไปยังระบบสนทนาถูกสร้างขึ้น ผู้คนก็สร้างความรำคาญให้แก่ผู้อื่นโดยการใส่คำที่มาจากบทละครร้อง "Monty Python Spam Song" ในขณะที่มีความเห็นแย้งว่า[8] คำว่า "สแปม" น่าจะมาจากระบบสนทนาอื่น โดยผ่านระบบคอมพิวเตอร์ที่เรียกว่า Bulletin broad system (BBS) [9] ที่มีเป็นจำนวนมาก โดยน่าจะมาจากคำจำกัดความที่ว่า "Single Post to All Messagebases" ซึ่งความเห็นเหล่านี้ ยังไม่มีหลักฐานสนับสนุนเพียงพอที่จะเชื่อได้ว่าเป็นต้นกำเนิดของสแปมเท่ากับการสนทนาใน MUDs

---

[7] เรื่องเดียวกัน

[8] เรื่องเดียวกัน

[9] ดูเพิ่มเติมใน http://en.wikipedia.org/wiki/Bulletin_board_system

2.2.2 ที่มาของคำว่า "สแปม"

"สแปม" (SPAM) นั้น เป็นชื่อของผลิตภัณฑ์อาหารกระป๋องชนิดหนึ่งในหลายๆ ผลิตภัณฑ์ของบริษัท ฮอร์เมล ฟู้ด จำกัด (Hormel Foods Corporation) ซึ่งผลิตเนื้อกระป๋องที่ใช้รับประทานสำหรับอาหารมื้อกลางวัน ซึ่งส่วนใหญ่ประกอบไปด้วยเนื้อที่ทำเทียมขึ้น ไม่ใช่เนื้อแท้ๆ โดยผลิตภัณฑ์ชนิดหนึ่งของบริษัทคือ "Shoulder Pork and hAM/SPiced hAM" หรือ "SPAM" ได้กลายมาเป็นชื่อเรียกจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงปรารถนาในภายหลัง โดยการเปรียบเทียบกับผลิตภัณฑ์ของบริษัทซึ่งเป็นเนื้อที่ทำเทียมขึ้นว่า เป็นอาหารขยะ (Junk food) และไม่มีคุณค่าทางโภชนาการที่สำคัญต่อร่างกายอย่างแท้จริง เช่นเดียวกับอีเมลที่ไม่เป็นที่ต้องการของผู้รับนั่นเอง

ข้อสันนิษฐานอีกประการหนึ่งที่ทำให้คำว่า "สแปม" กลายเป็นคำที่นิยมใช้เรียกจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่พึงปรารถนาโดยทั่วไป น่าจะมาจากบทละครร้องตอนหนึ่งของละครตลกเรื่องหนึ่งในประเทศอังกฤษที่ชื่อ "Monty Python's Flying Circus"* ซึ่งเนื้อหาในบทละครร้องตอนนั้น เป็นเรื่องของสามีภรรยาสองคนที่เข้ามาในร้านอาหาร และพยายามจะสั่งอาหารอย่างอื่นนอกจาก "สแปม" จากพนักงานบริการ แต่พนักงานบริการก็ยังยืนยันที่จะเสนอรายการอาหารที่ประกอบไปด้วย "สแปม" ให้อยู่ตลอดเวลา ในภายหลังคำว่า "สแปม" จึงถูกนำมาเรียกขานการส่งข้อความมายังผู้รับโดยที่ผู้รับมิได้ร้องขอ และก่อให้เกิดความรำคาญ เหมือนกับที่พนักงานบริการพยายามยัดเยียดอาหารที่ชื่อว่า "สแปม" ให้กับสองสามีภรรยานั่นเอง

นอกจากนี้ในขณะที่ละครกำลังดำเนินเรื่องราวอยู่นั้น ก็จะมีกลุ่มนักร้องประสานเสียงที่แสดงเป็นไวกิ้งคอยร้องประสานเสียงตามอยู่ตลอดเวลา โดยร้องคำว่า S-P-A-M ซ้ำไปซ้ำมาหลายครั้ง และร้องเสียงดังจนกลบบทสนทนาอื่นๆ ไป คำว่า "สแปม" จึงถูกนำมาใช้อธิบายวิธีการส่งข้อความจำนวนมากเกินไปจนบดบังความสำคัญของการสื่อสารอื่นๆ หรือในความหมายที่ว่าทำสิ่งใดซ้ำไปซ้ำมา หลายครั้ง จนก่อให้เกิดความรำคาญอย่างมากแก่ผู้อื่น

ผลจากการนี้ ทำให้บริษัท ฮอร์เมล ฟู้ด จำกัด (Hormel Foods Corporation) ผู้ผลิตอาหารกระป๋องที่ชื่อว่า "สแปม" ได้รับความเดือดร้อนจากความเข้าใจผิดดังกล่าวเป็นอย่างมาก จนถึง

---

* ดูภาคผนวก ก

ขนาดต้องมีเวปไซต์เพื่อทำความเข้าใจกับบุคคลทั่วไปที่ยังไม่ทราบว่าสแปมคืออะไร[10]และแก้ไขข้อข้องใจว่าหากได้รับสแปมเมล ที่ส่งมาโดยมีที่อยู่ที่ระบุว่า SPAM.COM นั้น ก็ขอให้เข้าใจด้วยว่าไม่ได้ส่งมาจากบริษัทของตน อย่างไรก็ตาม บริษัท ก็มิได้ขัดข้องหากจะใช้คำว่า "spam" เป็นคำแสลงเพื่ออธิบายถึงจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่ได้ให้ความยินยอม เพียงแต่ขอสงวนให้ใช้ คำว่า "SPAM" โดยตัวอักษรตัวใหญ่ในการใช้เป็นเครื่องหมายการค้าของเขา และรักษาไว้ซึ่งชื่อเสียงของบริษัทที่สะสมมานาน จนเป็นที่รู้จัก ก่อนที่คนรุ่นใหม่จะรู้จักกับสแปมในความหมายของจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่ได้ร้องขอ มากกว่าผลิตภัณฑ์ที่มีชื่อเสียงของพวกเขาเท่านั้น

2.3 ลักษณะโดยทั่วไปของสแปมเมล

แม้ว่าจะเป็นการยากที่จะให้คำนิยามอย่างชัดแจ้งว่าสแปมเมลคืออะไรก็ตาม แต่จากการศึกษาพบว่า สแปมเมลส่วนใหญ่มักจะมีลักษณะดังต่อไปนี้

(1) สแปมเมล เป็นจดหมายออนไลน์ที่ส่งได้ทั่วโลก (global) โดยส่งออกไปยังที่อยู่อีเมลจำนวนมากอย่างต่อเนื่องและไม่จำกัดกลุ่มเป้าหมาย (indiscrimination)[11] โดยที่ผู้รับ สแปมเมลไม่เคยให้ความยินยอมต่อการส่งสแปมเมลเหล่านั้นเลย ทั้งนี้ เนื่องจากสแปมเมอร์ได้ที่อยู่อีเมลเหล่านี้ จากการใช้โปรแกรมค้นหาอัตโนมัติที่เรียกว่า "harvester" หรือ "spider" โดยการค้นหาจากเว็บเพจ กระดานข่าว หรือดึงมาจากรายชื่อลูกค้าของผู้ให้บริการอินเตอร์เนต (หากว่าผู้ให้บริการรายนั้นไม่มีมาตรการการป้องกันการเข้าถึงข้อมูลที่ดีพอ) ซึ่งการดูจากที่อยู่อีเมลเพียงอย่างเดียวนั้นไม่อาจทำให้สแปมเมอร์ทราบข้อมูลส่วนตัวที่ดีเพียงพอในการสุ่มเลือกกลุ่มเป้าหมายให้ตรงกับเนื้อหาของสแปมเมลได้ อย่างไรก็ดี หากเป็นกรณีที่เป็นการซื้อขายรายชื่ออีเมล (mailing list) จากผู้ให้บริการอีเมล หรือจากเว็บไซต์ต่างๆ ที่ต้องมีการกรอกข้อความเพื่อสมัครเป็นสมาชิกก่อนเข้าเยี่ยมชมเว็บไซต์ หรือการซื้อขายข้อมูลที่รวบรวมได้จากการฝังตัวของโปรแกรมบางอย่าง เช่น cookie ซึ่งโปรแกรมนี้จะทำการเก็บรวบรวมข้อมูลต่างๆ ของผู้เข้าเยี่ยมชม ส่งไปยังเว็บไซต์นั้นๆ เพื่อเก็บเป็นฐานข้อมูลเอาไว้ ดังนั้นรายชื่ออีเมลเหล่านี้จึงจัดเป็นรายชื่ออีเมลคุณภาพดี อันประกอบไปด้วยรายละเอียด และพฤติกรรมการ

---

[10] Spam Corporate Info, "SPAM & the Internet," at http://www.spam.com/ci/ci_in.htm (last visited February 2006).

[11] อรรยา สิงห์สงบ, "ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ (Spam Mail)," นักบริหาร 23,4 (ต.ค. – ธ.ค. 2546) : 84-90.

ใช้อินเตอร์เนตที่มากเพียงพอจะวิเคราะห์ได้ว่าเจ้าของที่อยู่อีเมลเหล่านี้ มีความสนใจในเรื่องใด ซึ่งก็จะกลายเป็นกลุ่มเป้าหมายสำคัญที่จะได้รับ สแปมเมลจำนวนมากต่อไป

(2) การส่งสแปมเมลมีต้นทุนที่ต่ำมาก จึงเป็นวิธีที่ได้รับความนิยมอย่างมากในการทำการตลาดออนไลน์เมื่อเทียบกับการทำการตลาดโดยวิธีอื่น เช่น การส่งทางไปรษณีย์ การแจกใบปลิวโฆษณา หรือการใช้วิธีการโทรศัพท์ ฯลฯ เพราะสามารถส่งออกไปได้ถึงกลุ่มคนจำนวนมากๆ ในคราวเดียว และยังเข้าถึงกลุ่มเป้าหมายได้อย่างรวดเร็ว โดยไม่จำกัดเพศ เชื้อชาติ และถิ่นที่อยู่ รวมถึงโอกาสในการประสบผลสำเร็จ แม้มีเพียง 1% ของสแปมเมลทั้งหมด แต่เมื่อเทียบกับต้นทุนที่ต่ำมากแล้ว ก็นับว่าสแปมเมลเป็นวิธีการที่ให้ผลตอบแทนที่สูงมาก อีกทั้งยังสามารถพลิกแพลงไปใช้วิธีการอื่นๆ ได้อีก ที่สำคัญการส่งสแปมเมลเป็นการสื่อสารแบบทางเดียวคือ หากผู้รับไม่พอใจก็ไม่สามารถส่งข้อความกลับ หรือบ่นใดๆ ได้ เพราะผู้รับไม่ได้รู้จักผู้ส่ง จึงเป็นช่องทางทางการค้าที่น่าสนใจในปัจจุบันนี้ ดังนั้น ตราบใดที่ยังไม่มีรูปแบบการโฆษณาแบบใหม่ที่มีต้นทุนที่ต่ำกว่าการส่งสแปมเมล วิธีการทำการโฆษณาโดยการส่งสแปมเมลก็จะยังคงได้รับความสนใจและเป็นที่นิยมไปอีกนาน

(3) เนื้อหาของสแปมเมลมักจะมีความหลากหลาย และมีวัตถุประสงค์แตกต่างกัน ซึ่งโดยเนื้อหาของสแปมเมลแล้ว อาจเป็นเรื่องเท็จ หรือเรื่องหลอกลวงก็ได้ เช่น การให้ข้อมูลข่าวสารที่เป็นประโยชน์ หรือการส่งเรื่องตลกขบขัน, จดหมายลูกโซ่ หรือข้อเท็จจริงต่างๆ แต่ สแปมเมลส่วนใหญ่มักเป็นสแปมเมลเชิงพาณิชย์ (Unsolicited Commercial Email (UCE)) คืออยู่ในรูปของการโฆษณาสินค้าหรือบริการ หรือการโฆษณาเวปไซท์ต่างๆ ทั้งที่ถูกกฎหมายและไม่ถูกกฎหมาย ซึ่งไม่สามารถใช้ช่องทางการโฆษณาตามปกติได้โดยสะดวก เช่นการโฆษณาเวปไซท์ หนังหรือภาพลามกอปรกับค่าใช้จ่ายในการโฆษณาที่น้อยกว่าการส่งจดหมายปกติมาก รวมถึงเข้ากลุ่มคนได้ทั่วโลก ทำให้การโฆษณาสินค้า และบริการ โดยวิธีการส่งสแปมเมลได้รับความนิยมอย่างมากทั้งนอกประเทศและในประเทศ

(4) โดยที่ผู้ส่งสแปมเมลมักจะไม่ปรากฏชื่อผู้ส่ง (anonymous) หรือถ้าปรากฏก็จะเป็นชื่อผู้ส่งและที่อยู่ที่ไม่มีตัวตนจริง (spoofing) ทั้งนี้เพราะผู้ส่งสแปมต้องการปกปิดตัวตนที่แท้จริงเพื่อป้องกันการโดนสแปมกลับ และหลีกเลี่ยงความเสี่ยงจากข้อกฎหมาย โดยเฉพาะในต่างประเทศซึ่งมีกฎหมายในเรื่องนี้ รวมถึงเสี่ยงต่อเว็บไซต์ของผู้ส่งที่อาจต้องถูกปิดลงจากการละเมิดการใช้งาน เพราะโดยทั่วไป ผู้ให้บริการพื้นที่เว็บไซต์ และผู้ให้บริการอีเมล มักจะมีข้อตกลงที่ว่าการส่งสแปมเมลเป็นการละเมิดข้อตกลงในการใช้งาน ผู้ส่งสแปมเมลจึงอาศัยช่องโหว่ของระบบรับ-ส่งอีเมล ในการส่ง

อีเมล โดยโปรแกรมที่ได้รับการออกแบบมาโดยเฉพาะ ทำให้ผู้รับไม่สามารถทราบถึงตัวตนที่แท้จริงของผู้ส่งได้ หรือหากชื่อและที่อยู่อีเมลเป็นของบุคคลที่มีตัวตนจริงๆ แต่บุคคลนั้นก็อาจจะไม่มีความเกี่ยวพันแต่อย่างใดกับผู้ส่งสแปมเมล หรือสแปมเมลฉบับนั้นก็ได้

(5) การยกเลิกการรับสแปมเมลเหล่านั้น ไม่สามารถกระทำได้ และถึงแม้จะมีเงื่อนไขหรือข้อกำหนดให้ยกเลิกการรับสแปมเมลได้ แต่ช่องทางและวิธีการบอกเลิกเหล่านั้น กลับเป็นช่องทางให้สแปมเมอร์ใช้เป็นวิธีการที่จะยืนยันถึงความมีตัวตนที่แท้จริง และการใช้งานของเจ้าของอีเมล และใช้เป็นข้อมูลในการส่งสแปมเมลมายังผู้รับตามที่อยู่อีเมลนี้มากยิ่งขึ้น

(6) สแปมเมลมักจะมีเนื้อหาที่อยู่ในรูปของ HTML [12] * หรือรูปแบบโครงสร้างเดียวกับเวปไซท์ต่างๆ ทั้งนี้เพื่อความสวยงาม จูงใจผู้รับให้เข้าไปชมแล้ว สแปมเมอร์ยังสามารถสอดแทรกคำสั่ง หรือโปรแกรมต่างๆ เข้ามาทำงานในระบบคอมพิวเตอร์ของผู้รับได้อีกด้วย เช่น หนอนไวรัส สปายแวร์* หรือการส่งคำยืนยันกลับไปยังต้นทางเมื่อผู้รับได้เปิดดูอีเมลฉบับนั้นแล้ว

(7) หัวข้อเรื่องที่ส่งมากับสแปมเมลมักเป็นข้อความที่น่าสนใจเชิญชวนให้ผู้รับเปิดอ่าน แม้จะทราบว่าไม่เป็นความจริง เช่น "นี่คือคำตอบที่เราได้ร้องขอคุณไป" หรือ "ผมได้ส่งไฟล์มาแล้วตามที่ร้องขอ" หรือ "คุณได้รับอนุมัติบัตรเครดิตแล้ว" หรือ "อ้างถึง: อีเมลที่ร้องขอมานั้น" ซึ่งเมื่อเปิดดูเนื้อหาภายในแล้ว กลับพบว่าไม่มีความเกี่ยวข้องกับหัวข้อเรื่องที่ได้รับแต่อย่างใด

---

[12] ธันวา ศรีประโมง, จดหมายขยะ โฆษณาบนความรำคาญของผู้ใช้อินเตอร์เน็ต[ออนไลน์]. แหล่งที่มา : http://www.eng.mut.ac.th/Computer/Article_detail.asp?ArticleID=82 (13 ตุลาคม 2547)

* HTML คือ รูปแบบการแสดงผลที่ปรากฏในรูปของเวปไซต์

* สปายแวร์ (spyware) จะเก็บรวบรวมข้อมูลเกี่ยวกับตัวผู้ใช้จากเครื่องคอมพิวเตอร์ของคุณโดยไม่ได้รับอนุญาต (ซึ่งจะไม่เหมือนคุกกี้ ซึ่งบราวเซอร์และคุณสามารถเลือกที่จะยอมรับหรือปฏิเสธได้) ผู้รับอาจตกเป็นเหยื่อของสปายแวร์ ถ้ามีการดาวน์โหลด (download) เพลงหรือหนังจากโปรแกรมบางตัวที่มีไฟล์อยู่ด้วย เกมส์ หรือบางโปรแกรมบางอย่างที่คุณไม่ทราบแหล่งที่มา

2.4 ประเภทของสแปมเมล[13]

2.4.1 Internal Spam

คือ การส่งสแปมเมลที่มาจากภายในเครือข่ายเดียวกัน เช่น การส่งเรื่องตลกขบขัน เรื่องคอลัมน์นินทาต่างๆ ระหว่างเพื่อนร่วมงาน การส่งข่าวสินค้าลดราคา หรือจดหมายแจ้งข่าวเพื่อให้บุคลากรภายในองค์กรได้รับทราบ

2.4.2 External Spam

คือ การส่งสแปมเมลที่มาจากภายนอกเครือข่าย ซึ่งสามารถแบ่งออกได้เป็น

- จดหมายที่มีข้อความโฆษณาสินค้า บริการ (Commercial Message) เช่น แนะนำหรือทดลองใช้สินค้าหรือบริการ
- เพศ เช่น เว็บไซต์ภาพลามก ซึ่งมักจะเป็นการนำเสนอข้อมูลที่ไม่เหมาะสมต่อเยาวชน
- จดหมายลูกโซ่ (Chain Letters) โดยมีการขู่ว่าถ้าไม่ส่งต่อผู้รับจดหมายจะต้องเผชิญกับความหายนะ
- การเงิน เช่น แนะนำวิธีการหาเงินบนอินเตอร์เนต หรือเชิญชวนให้ลงทุนหุ้นตัวใดตัวหนึ่ง หรือโครงการหารายได้เสริมแบบรวดเร็ว (Make Money Fast)
- สุขภาพ เช่น แนะนำสถานที่ออกกำลังกาย หรือยาบำรุงร่างกาย
- คอมพิวเตอร์ เช่นการขายคอมพิวเตอร์ หรือซอฟต์แวร์ราคาพิเศษในระยะเวลาจำกัด
- การหลอกว่ามีไวรัส (Virus Hoaxes)
- บทความทางศาสนา (Religious Treatise)

ทั้งนี้ จดหมายลูกโซ่ และการหลอกว่ามีไวรัส เป็นลักษณะที่พยายามทำให้ผู้รับทำการส่งต่อจดหมายไปยังผู้อื่นต่อไป

---

[13] Debbie Wilde, "How to Mininise The Effect of Spam 98," PC NETWORK ADVISOR 7 (1998), อ้างถึงใน อรรยา สิงห์สงบ, "ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ (Spam Mail)," นักบริหาร 23,4 (ต.ค. – ธ.ค. 2546) : 84-90.

2.4.3 Usenet Spam

คือ การส่งสแปมเมลไปยังกลุ่มข่าวบนยูสเนตแต่ละกลุ่มโดยมักจะส่งไปพร้อมๆ กับกลุ่มข่าวต่างๆ ที่ผู้ส่งสแปมเมลจะไม่อ่านอีกต่อไป ซึ่งมีผลทำให้กลุ่มข่าวนั้นไม่อาจที่จะจัดให้สามารถติดตามข่าวได้อย่างเป็นระบบ

2.5 วิธีการ และขั้นตอนในการส่งสแปมเมล

2.5.1 วิธีการรวบรวมรายชื่อ

เป็นที่ทราบกันดีว่า สแปมเมล เป็นจดหมายอิเล็กทรอนิกส์ประเภทหนึ่งที่ส่งออกไปคราวละมากๆ และผู้รับไม่พึงปรารถนาที่จะได้รับจดหมายอิเล็กทรอนิกส์ฉบับนั้น อีกทั้งยังไม่เคยร้องขอให้ผู้ส่ง ส่งจดหมายอิเล็กทรอนิกส์เหล่านั้นมายังผู้รับอีกด้วย

ดังนั้น เพราะเหตุใดผู้ใช้อินเตอร์เนตโดยทั่วไป จึงยังคงได้รับสแปมเมลเหล่านี้กันอยู่อย่างต่อเนื่อง ทั้งๆ ที่ผู้รับเองก็ไม่เคยรู้จักกับผู้ส่งสแปมเมลมาก่อน และไม่เคยได้ติดต่อหรือให้อีเมลไว้กับบุคคลเหล่านั้น และถึงแม้ว่าผู้รับจะระมัดระวังตัวไม่ทิ้งอีเมลของตนเองไว้ตามสถานที่สาธารณะ เช่น ตามกระดานข่าว หรือเวปบอร์ดทั่วไปก็ดี ก็ยังมีโอกาสอย่างมากที่จะได้รับสแปมเมลอยู่

ก่อนที่สแปมเมลจำนวนนับพัน นับหมื่นฉบับจะถูกส่งออกไปนั้น สิ่งสำคัญที่สแปมเมอร์ทั้งหลายต้องมีในมือเป็นอันดับแรกเลย ก็คือ ที่อยู่อีเมลของผู้รับ (Email Address) ทั้งหลายนั่นเอง และเนื่องจากว่าลักษณะของสแปมเมล ซึ่งเป็นจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่ให้ความยินยอม เพราะผู้รับกับผู้ส่งไม่เคยรู้จัก หรือผู้รับไม่เคยให้ที่อยู่อีเมลกับผู้ส่งมาก่อน ดังนั้น การที่สแปมเมอร์แต่ละรายจะได้ที่อยู่อีเมลของผู้รับมา จึงต้องอาศัยวิธีการรวบรวมรายชื่อเอาเอง โดยใช้โปรแกรมที่สร้างขึ้นในการกวาดต้อน หรือรวบรวมเอาที่อยู่อีเมลบนเครือข่ายต่างๆ ซึ่งโปรแกรมที่ใช้ก็มีรูปแบบ และมีการพัฒนาให้มีความทันสมัยอยู่ตลอดเวลา เพื่อให้มีประสิทธิภาพในการทำงาน และหลีกเลี่ยงจากการป้องกันของเซิร์ฟเวอร์ทั้งหลายได้

วิธีการรวบรวมที่อยู่อีเมลมีตั้งแต่วิธีง่ายๆ ไปจนถึงการใช้โปรแกรมต่างๆ ซึ่งก็จะมีค่าใช้จ่ายเพิ่มขึ้น ซึ่งเป็นจำนวนเงินที่น้อยมากเมื่อเทียบกับประสิทธิภาพที่ได้รับ การรวบรวมที่อยู่อีเมล

อย่างง่ายๆ เช่น การไปลงทะเบียนเป็นสมาชิกตามกระดานข่าว[14] หรือเวปไซต์ต่าง ๆ ซึ่งหากเจ้าของเวปไซท์ไม่มีจรรยาบรรณพอ ก็อาจจะรวบรวมรายชื่อสมาชิกไปขายต่อให้แก่เหล่า สแปมเมอร์ได้ หรือการไปทิ้งอีเมลของตัวเองไว้ ตามเวปบอร์ดต่างๆ ซึ่งเป็นที่สาธารณะ ไม่ว่าในประเทศไทยหรือต่างประเทศ เทศ ต่างก็สามารถเห็นอีเมลของผู้ใช้ได้ แล้วนำไปใส่อยู่ในบัญชีส่งสแปมเมลได้ รวมไปถึงอีเมลที่ส่งคุยถึงกันเฉพาะกลุ่ม อาจจะถูกส่งต่อ (Forward) ไปหาคนอื่นต่อๆ กันไป ทั้งโดยตั้งใจและไม่ตั้งใจ ทำให้ง่ายต่อการที่จะรวบรวมที่อยู่อีเมลจำนวนมากเอาไว้ เพื่อใช้ในวัตถุประสงค์อื่นๆ โดยเฉพาะเมื่อตกถึงมือของบรรดาสแปมเมอร์

อีกวิธีหนึ่งที่บางบริษัทใช้คือ[15] การใช้โปรแกรมที่เรียกว่า Robot เช่น Spider ในโปรแกรมสืบค้นข้อมูล (Search Engine) เพื่อทำการค้นหาและรวบรวมอีเมล จากกลุ่มข่าว (newsgroup) สมุดหน้าเหลืองออนไลน์ (online yellow pages) หรือตามกระทู้ต่างๆ ที่ตั้งถามกันในเวปบอร์ด (webboard) สาธารณะ ที่มีการใส่อีเมลของผู้ถามและผู้ตอบเอาไว้ โดยอาศัยช่องโหว่ของเซิร์ฟเวอร์ที่ไม่มีระบบการป้องกันใดๆ ก็จะได้ที่อยู่อีเมลจำนวนมากที่อาจจะนำไปใช้ส่งสแปม หรือบางครั้ง ก็ได้มาจากสปายแวร์ (spyware) ที่แฝงมากับพวก*ซอฟท์แวร์ (software), แชร์แวร์ (shareware), ฟรีแวร์ (freeware) หรือเดโม (demo) ต่าง ๆ ที่เราไปดาวน์โหลดเอามาจากอินเตอร์เนต สปายแวร์จะทำหน้าที่ในการรวบรวมข้อมูลพฤติกรรมการใช้งานอินเตอร์เนตของผู้ใช้ (รวมถึงอีเมลด้วย) เพื่อส่งไปรวบรวมไว้ที่เซิร์ฟเวอร์ แล้วจะส่งเมลโฆษณามาให้เรา ตามข้อมูลที่ได้รับจากเครื่องของผู้ใช้งานว่าสนใจในเรื่องใด โดยปกติสปายแวร์ จะมีบอกไว้ในข้อตกลงและนโยบาย (Term & Policy) ในตอนติดตั้ง ว่าจะมีการฝังโปรแกรมบางอย่างเพื่อรวบรวมข้อมูลส่งไปทางเซิร์ฟเวอร์

สำหรับวิธีที่ง่ายที่สุดในการส่งสแปมอีกอย่างหนึ่ง[16] คือไปซื้อข้อมูลจากบริษัทที่รวบรวมอีเมลเหล่านี้ไว้เพื่อขาย ซึ่งบริษัทส่วนใหญ่ก็ใช้วิธีการดังกล่าว ส่วนผู้ให้บริการฟรีอีเมลต่างๆ

---

[14] wasanast@csloxinfo.net, **"รู้ทันและรับมือกับ spam mail," ผู้จัดการออนไลน์(4 มีนาคม 2547) ที่** http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=4795271431802.

[15] เรื่องเดียวกัน

* ซอฟต์แวร์ (software) หมายถึงชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน, แชร์แวร์ (shareware) คือโปรแกรมทดลองใช้ ที่ต้องจ่ายเงินหากต้องการใช้ต่อไป หรืออยากได้โปรแกรมฉบับสมบูรณ์, ฟรีแวร์ (freeware) คือโปรแกรมที่สามารถนำไปใช้ได้โดยไม่ต้องเสียเงิน, เดโม (demo) คือ โปรแกรมเวอร์ชั่นที่ผู้ผลิตทำมาให้ทดลองใช้ก่อน ซึ่งหากมีปัญหาก็สามารถอีเมลไปบอกกับผู้ผลิตได้

[16] เรื่องเดียวกัน

นั้นก็ขึ้นอยู่กับนโยบายความลับของบริษัทผู้ให้บริการว่าจะนำข้อมูลอีเมลเหล่านั้นไปขาย หรือนำไปใช้งานร่วมกับบริษัทอื่นๆ อย่างไร

2.5.2 วิธีการส่งสแปมเมล

ในปัจจุบันมีวิธีการมากมายที่เหล่าสแปมเมอร์ใช้ในการส่งสแปมเมล และก็ยังมีการคิดค้นวิธีการ หรือโปรแกรมใหม่ๆ อยู่เรื่อยๆ เพื่อช่วยในการกระจายสแปมเมลให้เป็นไปได้โดยรวดเร็วถึงกลุ่มเป้าหมาย ในปริมาณที่มากกว่าเดิม ซึ่งแม้จะมีการพัฒนาโปรแกรมต่อต้าน สแปมเมลขึ้นมาเพื่อทำการกลั่นกรองสแปมเมลให้มีประสิทธิภาพมากเพียงใดก็ตาม ก็ยังไม่สามารถที่จะสกัดกั้นสแปมเมลจำนวนมากที่ส่งกันอยู่ในแต่ละวันได้

สาเหตุที่สำคัญที่สแปมเมอร์สามารถส่งสแปมเมลเข้ามาได้นั้น ก็เพราะโปรโตคอล* SMTP• ที่ใช้งานอยู่ทุกวันนี้ไม่มีกลไกที่ผู้ใช้สามารถป้องกันตนเองจากผู้ส่งได้ นั่นคือไม่ว่าผู้ส่งจะส่งอีเมลอะไรก็ตามมายังผู้รับ หากไม่มีสิ่งใดผิดพลาด ผู้รับจะต้องรับอีเมลนั้นเสมอ หากผู้รับไม่ต้องการก็ให้ลบทิ้งไปเอง ถึงแม้ว่าจะมีการปรับปรุง SMTP โดยการเพิ่มเครื่องมือเข้าไป คือ โดยก่อนที่ MTA (Message Mail Transfer Agent)♣ จะทำการส่งอีเมลออกไปนั้นจะต้องทำการตรวจสอบชื่อและรหัสผ่านของผู้ส่งเสียก่อน แต่เครื่องมือดังกล่าวนำมาใช้กับ MTA ขาออกเพื่อป้องกันการลักลอบใช้ MTA เพื่อส่งอีเมลออกไปหาผู้อื่นเป็นหลัก ไม่เหมาะที่จะนำมาใช้งานกับ MTA ขาเข้า ในเมื่อผู้ใช้ไม่มีการป้องกันใดๆ ดังนั้นเมื่อสแปมเมอร์ได้ที่อยู่อีเมลที่ถูกต้องของผู้ใช้และส่งสแปมเมลเข้ามา สแปมเมลเหล่านั้นก็จะเข้ามายังกล่องจดหมาย (mailbox) ของผู้รับได้เสมอ

เพื่อความเข้าใจมากยิ่งขึ้น จึงขอยกตัวอย่างวิธีการส่งสแปมเมลอย่างง่ายๆ ที่สแปมเมอร์นำมาใช้ได้แก่

---

* โปรโตคอล (protocol) คือ กลุ่มของกฎหรือกติกาที่มีการบัญญัติขึ้นสำหรับการแลกเปลี่ยนข้อมูลกันระหว่างตัวส่งและตัวรับ เพื่อให้ตัวส่งและตัวรับใช้กติกานี้ ร่วมกัน ทำให้การสื่อสารเป็นไปได้อย่างถูกต้องและมีระเบียบ

• SMTP (Simple Mail Tranfer Protocol) เป็นโปรโตคอลแบบหนึ่งที่ติดต่อกันระหว่างเครื่องคอมพิวเตอร์ที่เป็นเครื่องรับและเครื่องส่ง เพื่อให้สามารถรับส่งอีเมลระหว่างกันได้

♣ Mail Transport Agent (MTA) คือส่วนที่ทำหน้าที่ในการรับและส่งเมล โดยจะตรวจหาเส้นทางของเมลแล้วจัดการส่งต่อไปยังเซิร์ฟเวอร์ปลายทาง หรือคัดแยกเมลที่เข้ามา เพื่อทำการจัดส่งให้แก่ผู้รับแต่ละคน

2.5.2.1 การใช้วิธีสมัครเป็นสมาชิกกับผู้ให้บริการอินเตอร์เนต[17]

เมื่อสแปมเมอร์ได้รายชื่อที่อยู่อีเมลของผู้รับดังได้กล่าวมาแล้วนั้น ผู้ส่งสแปมเมลก็จะต้องหาโปรแกรมที่ใช้เพื่อช่วยกระจายสแปมเมล ซึ่งโดยส่วนมากมักจะเป็นโปรแกรมที่ไม่ต้องเสียเงิน (Freeware หรือ Shareware Program) โดยโปรแกรมเหล่านี้สามารถส่งอีเมลได้ครั้งละไม่เกิน 20,000 ข้อความต่อชั่วโมง จากนั้น ผู้ส่งสแปมเมลจะต้องหาระบบที่จะต้องส่งสแปมเมล ซึ่งวิธีง่ายๆ ที่ผู้ส่งมักจะใช้กันเป็นส่วนใหญ่ ก็เช่น การสมัครลองเป็นสมาชิกกับผู้ให้บริการอินเตอร์เนต ของบริษัทใดก็ได้ที่ให้บริการให้ลองใช้ฟรี โดยไม่ต้องเสียค่าใช้จ่ายแต่อย่างใด โดยบัญชีของสมาชิกทดลองใช้จะถูกลบทิ้งหลังจากระยะเวลาการทดลองใช้สิ้นสุดลง ซึ่งระบบนี้ทำให้ผู้ส่งสแปมเมลมั่นใจได้ว่า ผู้รับจะไม่สามารถติดต่อกลับมายังผู้ส่งสแปมเมลได้อีก อย่างไรก็ดีในปัจจุบันนี้ ผู้ให้บริการอินเตอร์เนตจำนวนมาก มักกำหนดเงื่อนไขให้การส่งสแปมเมล เป็นการกระทำที่ผิดข้อตกลงและเงื่อนไขการเป็นสมาชิกของบริษัท ซึ่งทำให้บริษัทมีสิทธิที่จะระงับการใช้บัญชีอีเมลของผู้นั้นได้

2.5.2.2 การใช้วิธีที่เรียกว่า การทำเมลรีเลย์ (Mail relay)

วิธีนี้เป็นวิธีการหนึ่งที่ได้รับความนิยมมากที่สุดในการส่งสแปมเมลออกไป โดยการอาศัยช่องโหว่ของระบบรับ-ส่งเมล [18] ที่ผู้ติดตั้งเซิร์ฟเวอร์ขาดความรู้เกี่ยวกับการดูแลระบบเมลเซิร์ฟเวอร์ เช่น การติดต่อผ่านเข้าไปยังพอร์ตเมลของเซิร์ฟเวอร์แล้วทำการส่งเมลออกไปที่อื่นๆ ซึ่งการส่งเมลด้วยวิธีการส่งตรงให้พอร์ตของผู้ส่งเมลนี้ ไม่จำเป็นต้องมีกล่องจดหมายในเซิร์ฟเวอร์นั้น ดังนั้นจึงสามารถปลอมแปลงที่อยู่ของต้นทางได้ ขณะเดียวกันก็ส่งไปยังเป้าหมายปลายทางที่ใดก็ได้ โดยใช้ตัวรับส่งเมลของเซิร์ฟเวอร์เป็นผู้ส่งให้ หรือวิธีการอาศัยตัวกลางในการส่งสแปมเมลไปยังผู้อื่น (การทำเมลรีเลย์) คือการส่งต่ออีเมลออกไปเป็นทอดต่อกันโดยอาศัย MTA[19] เป็นตัวกลางในการส่งเพื่อรับฝากอีเมล แล้วส่งต่อไปยังสแปมปลายทางอีกครั้ง ถ้าหากเป็นสแปมเมอร์ที่มีความเชี่ยวชาญหรือชำนาญการก็จะหลีกเลี่ยงการนำโฮสต์ของตนเองเป็น MTA ไปสแปมผู้อื่น เพื่อไม่ให้สามารถทำการสืบค้นกลับมายังโฮสต์ต้นตอของผู้ส่งสแปมเมลตัวจริงได้ เพียงแต่พบว่ามีต้นกำเนิดมาจากอีเมลเท่านั้น โดยวิธีการที่สแปมเมอร์นิยมใช้มากที่สุดก็คือ พยายามสอดส่องดูว่าเมลเซิร์ฟเวอร์ใดบนอินเตอร์เนตที่ทำการติดตั้ง

---

[17] อรรยา สิงห์สงบ, "ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ (Spam Mail)," นักบริหาร 23,4 (ต.ค. – ธ.ค. 2546) : 84-90.

[18] นรินทร์ พนาวาส, "เมลขยะ(Junk Mail) บนระบบอินเทอร์เนต," ที่ http://www.spu.ac.th/announcement/articles/junkmail.html (มีนาคม 2549).

[19] เรืองไกร รังสิต, เปิดโลก Firewall และ Internet Security พิมพ์ครั้งที่ 1(กรุงเทพฯ : โปรวิชั่น, 2545), หน้า 255.

MTA ไว้อย่างไม่ถูกต้องและเป็นช่องทางให้สแปมเมอร์อาศัยเป็นตัวกลางได้ เมื่อพบก็จะทำการส่งสแปมเมลโดยใช้โปรแกรม MUA* (Message User Agent) บนโฮสต์ของตัวเองไปทิ้งไปบน MTA ตัวแรกที่เป็นเหยื่อ หลังจากนั้น MTA ที่เป็นเหยื่อก็จะต้องรับภาระในการทยอยส่งสแปมเมลต่อไปจนถึงปลายทาง ด้วยวิธีการเช่นนี้จะเกิดประโยชน์ต่อสแปมเมอร์หลายประการ กล่าวคือการส่งอีเมลในโปรโตคอล SMTP นั้นเป็นแบบ Store and Forward คือรับอีเมลจนครบทั้งฉบับแล้วเก็บไว้เป็นการชั่วคราว หลังจากนั้นจึงทำการส่งต่อ และลบจดหมายทิ้งเมื่อได้ส่งต่อเป็นที่เรียบร้อยแล้ว ซึ่งทำให้สแปมเมอร์ไม่ต้องเสียเวลารับภาระในการพยายามส่งอีเมลให้ไปถึงปลายทางด้วยตัวเอง ขอเพียงให้ส่งจดหมายไปยัง MTA ตัวแรกให้สำเร็จเท่านั้นก็สามารถปิดเครื่องไปทำอย่างอื่นได้ ส่วนอีเมลทั้งหมดก็จะไปกองรวมกันอยู่ที่ MTA และ MTA ก็จะต้องพยายามทยอยส่งไปยังปลายทางให้ได้จนครบทุกฉบับ โดยส่วนใหญ่พวกสแปมเมอร์จะมีโปรแกรมที่ทำหน้าที่ในการส่งข้อความ (Message Deliver Agent - MDA) ซึ่งสามารถส่งสแปมเมลจำนวนมากไปยัง MTA ที่ตกเป็นเหยื่อได้อย่างรวดเร็วกว่าโปรแกรมการส่งเมลโดยปกติทั่วไป ทั้งนี้เพื่อให้สามารถส่งเมลไปทิ้งไว้ที่ MTA โดยใช้เวลาน้อยที่สุดและเสร็จสิ้นภารกิจได้โดยรวดเร็ว เมื่อผู้ใช้ปลายทางได้รับและทำการสืบค้นมายังต้นตอก็จะพบเพียงว่า MTA ที่ถูกสแปมเมอร์ใช้นั้นเป็นต้นกำเนิดของอีเมล โดยที่ไม่สามารถตามไปจนถึงสแปมเมอร์ตัวจริงได้

2.5.2.3 การใช้วิธีที่เรียกว่า DHA (Directory Harvest Attacks)

อีกวิธีหนึ่งที่ได้รับความนิยมอย่างมากในการส่งสแปม นั่นคือวิธีการที่เรียกว่า DHA (Directory Harvest Attacks)[20] ซึ่งเป็นการกวาดเอาอีเมลของผู้ใช้อินเตอร์เนตจากเซิร์ฟเวอร์ไปสแปมเมอร์พยายามที่จะเข้าถึงสารบบอีเมล (email directory) หรือรายชื่ออีเมลที่อยู่ในเซิร์ฟเวอร์นั้นๆ โดยสแปมเมอร์จะทำการส่งข้อความออกไปในลักษณะที่เรียกว่า Multiple address คือส่งออกไปหลายๆ ที่อยู่อีเมล ซึ่งชื่อนั้นก็จะมีความใกล้เคียงกัน เช่น johndoe@yourcompany.com, jdoe@yourcompany.com หรือ john@yourcompany.com จากนั้นก็จะมีเครื่องมือในการตรวจสอบและสุ่มหาอีเมลที่ถูกต้องในเซิร์ฟเวอร์อีเมลนั้นอีกครั้ง

หรืออีกวิธีการหนึ่งคือการส่งอีเมลสแปมมายัง support@yourcompany.com, services@yourcompany.com หรือไม่ก็

---

* MUA (Message User Agent) ทำหน้าที่ในการติดต่อกับผู้ใช้เพื่อรับและส่งเมล เพื่อให้ผู้ใช้ทำงานอ่านและเขียนจดหมายได้สะดวกขึ้น

[20] นักรบ เนียมนามธรรม, " Spam Scam Part II," Micro Computer User 21.221 (ธันวาคม 2546) : 100-102.

admin@yourcompany.com ซึ่งเป็นอีเมลที่ใช้ในการกระจายข่าวสารของแต่ละบริษัท ในนั้นก็จะประกอบด้วยอีเมลของพนักงานหรือบุคคลที่เกี่ยวข้องอยู่มากมาย ซึ่งหากสแปมเมอร์ส่งสแปมมายังที่อยู่อีเมลนี้แล้ว บุคคลที่มีรายชื่ออยู่อีเมลนั้น ก็จะพลอยได้รับสแปมเมลไปด้วย เป็นการแพร่กระจายสแปมเมลที่รวดเร็วอีกวิธีหนึ่ง โดยเฉพาะในบริษัทใหญ่ หรือบริษัท ที่มีลูกค้าเป็นสมาชิกอยู่เป็นจำนวนมาก

หลังจากที่สแปมเมอร์ได้ส่งอีเมลจำนวนมหาศาลมาที่เซิร์ฟเวอร์แล้ว หากที่อยู่อีเมลนั้นมีอยู่จริง หรือมีการใช้งานอยู่ อีเมลนั้นก็จะเป็นที่อยู่อีเมลที่สมบูรณ์ (Valid email address) แต่ถ้าหากว่าที่อยู่อีเมลนั้นไม่มีอยู่จริงเซิร์ฟเวอร์ก็จะทำการส่งข้อความแจ้งกลับไปว่าไม่มีที่อยู่อีเมลตามที่แจ้งไว้ ที่อยู่อีเมลที่สมบูรณ์เหล่านั้น ก็จะไปรวมกันอยู่ที่เซิร์ฟเวอร์สแปมเพื่อนำไปใช้งาน หรือนำไปขายหรือแลกเปลี่ยนระหว่างเหล่าสแปมเมอร์ต่อไป ซึ่งการทำเช่นนี้จะทำให้ได้รับที่อยู่อีเมลที่สมบูรณ์มากมายมหาศาลทุกวัน

นอกจากนั้น หากผู้รับสแปมเมลไม่ต้องการที่จะรับสแปมเมลนั้นอีกต่อไป โดยการบอกปฏิเสธ (Unsubscribe) สแปมเมลฉบับนั้น โดยหวังว่าการทำเช่นนั้นจะทำให้ สแปมเมอร์ทั้งหลายไม่ส่งสแปมเมลมายังตนอีก ซึ่งนอกนอกจากจะไม่เกิดผลตามที่หวังไว้แล้ว ยังอาจเป็นสาเหตุของการถูกโจมตีโดยสแปมเมลมากยิ่งขึ้น เนื่องจากว่า การตอบรับใดๆ กลับไปยัง สแปมเมอร์นั้น ถือเป็นการยืนยันความมีตัวตนของเจ้าของอีเมลที่ดีเยี่ยมอีกวิธีหนึ่ง และยังเป็นการแสดงให้เห็นว่าที่อยู่อีเมลนั้นยังมีการใช้งานอยู่ตลอดเวลา ซึ่งสแปมเมอร์ก็จะจัดระดับของที่อยู่อีเมลนี้ไว้อีกระดับหนึ่ง ซึ่งที่อยู่อีเมลนี้ก็จะมีมูลค่ามากขึ้นในการขายต่อ หรือการนำไปใช้ต่อไป

โดยปกติแล้วการค้นหาคนที่สร้างสแปมเมลนั้นเป็นเรื่องยาก เพราะพวกเขาเหล่านั้นมีวิธีการอำพรางตัว โดยอาศัยการเข้าสู่ระบบจากเครื่องเซิร์ฟเวอร์หนึ่งไปอาศัยอีกเซิร์ฟเวอร์หนึ่งในการส่ง ซึ่งจริง ๆ แล้วเครื่องเซิร์ฟเวอร์ของหน่วยงานแต่ละแห่ง จะไม่อนุญาตและไม่มีบริการให้สมาชิกส่งสแปมเมล แต่เครื่องเซิร์ฟเวอร์บางแห่งซึ่งมีระบบรักษาความปลอดภัยไม่ดีพอ ก็เปิดช่องให้สแปมเมอร์สามารถเข้าไปติดตั้งโปรแกรม หรือตั้งค่าระบบให้ส่งสแปมเมลออกไปได้โดยอัตโนมัติ หากผู้ดูแลระบบไม่มีความรู้เท่าทันก็จะไม่สามารถจัดการอะไรได้เลย

2.6 ผลกระทบที่เกิดขึ้นจากการส่งสแปมเมล

แม้ว่าในระยะเริ่มแรก สแปมเมลจะมิได้สร้างปัญหาให้กับผู้รับมากนัก ซึ่งส่วนใหญ่ก็เป็นแต่เพียงการสร้างความรำคาญในการที่จะต้องมาคอยลบสแปมเมลที่ตนไม่ต้องการเหล่านี้ แต่เมื่อการหลั่งไหลเข้ามาของสแปมเมลมีจำนวนเพิ่มขึ้นทุกวัน จนทำให้กล่องจดหมายของผู้รับเต็มไปด้วยสแปมเมล จากความรำคาญต่อการลบสแปมเมลในแต่ละครั้ง ได้กลับกลายเป็นสิ่งที่สร้างปัญหาให้กับ

บุคคลที่เกี่ยวข้องซึ่งมิใช่มีเพียงแต่ผู้รับเท่านั้น แต่ยังขยายออกไปในวงกว้าง จนกลายเป็นปัญหาที่หลายฝ่าย หลายประเทศ ต่างให้ความสำคัญ จนถึงกับมีองค์กร หรือหน่วยงานที่ตั้งขึ้นเพื่อศึกษาปัญหา และหาวิธีการต่อต้านกับสแปมเมล เช่นการขึ้นบัญชีเซิร์ฟเวอร์ที่เป็นตัวกลางในการส่งสแปมเมล รวมถึงมาตรการทางเทคนิคต่างๆ ที่ถูกพัฒนาขึ้นเพื่อนำมาใช้ในการสกัดกั้นสแปมเมล

เหตุผลที่ทำให้สแปมเมล ได้กลายมาเป็นปัญหาสำคัญที่ทั่วโลกต่างให้ความสนใจ ก็เนื่องมาจากสแปมเมลก่อให้เกิดผลกระทบต่อบุคคลที่เกี่ยวข้องดังต่อไปนี้

2.6.1 ผลกระทบทางเศรษฐกิจต่อบุคคลที่เกี่ยวข้อง

ด้วยค่าใช้จ่ายและต้นทุนที่ต่ำมาก ในการส่งสแปมเมลแต่ละครั้ง จึงเป็นเหตุผลที่สำคัญว่าทำไมการทำการตลาดโดยการส่งสแปมเมลจึงได้รับความนิยมอย่างมาก เพราะเมื่อเทียบกับผลตอบแทนที่ได้รับแล้ว ค่าใช้จ่ายหรือต้นทุนที่ต้องเสียไปในการส่งสแปมเมลแต่ละครั้ง นับว่าเป็นจำนวนที่น้อยมาก ทั้งนี้ เนื่องจากการส่งสแปมเมลนั้นมีลักษณะที่เป็นการผลักภาระค่าใช้จ่าย (Cost-shifting) มายังผู้ให้บริการอินเตอร์เนต และผู้ใช้อินเตอร์เนต ซึ่งเป็นผู้บริโภคนั่นเอง อันแตกต่างจากการทำการตลาดโดยวิธีอื่น เช่น การแจกใบปลิว การใช้การโทรศัพท์ การส่งโทรสาร หรือการจ้างคนมาทำโปรโมชั่น ซึ่งก่อให้เกิดค่าใช้จ่ายจำนวนมากที่ผู้ทำการตลาดต้องแบกรับ

ค่าใช้จ่ายที่ถูกผลักภาระไปยังผู้อื่น ซึ่งเป็นผลจากการทำการตลาดโดยการส่งสแปมเมลนั้น เป็นค่าใช้จ่ายที่เกิดขึ้นทั้งทางตรงและทางอ้อม และได้กลายเป็นต้นทุนในการดำเนินงาน ที่ผู้รับต้องแบกรับจากการรับสแปมเมลจำนวนมากในแต่ละวัน ซึ่งโดยปกติผู้ทำการตลาดต้องเป็นผู้รับภาระในการเสียค่าใช้จ่ายเหล่านี้ ค่าใช้จ่ายที่เกิดขึ้นต่างๆ เหล่านี้ เป็นผลเนื่องมาจาก[21]

2.6.1.1 สิ้นเปลืองเนื้อที่ในกล่องจดหมาย (Mailbox)

สแปมเมลจำนวนมากที่เข้ามาในกล่องจดหมายของผู้รับ กินเนื้อที่การรับอีเมลที่สำคัญอื่นๆ ของผู้ใช้ โดยหากกล่องจดหมายนั้นถูกจำกัดเนื้อที่จัดเก็บอีเมลของผู้ใช้ หากผู้ใช้ทิ้งไว้ไม่ได้เข้ามาตรวจสอบบ่อยๆ ก็อาจจะทำให้เนื้อที่หมดลงไปโดยไม่รู้ตัวเนื่องจากจดหมายขยะก็เป็นได้ ซึ่งเมื่อเมลบ๊อกซ์เหลือเนื้อที่ไม่พอจดหมายใหม่ก็ไม่สามารถส่งเข้ามาได้ หากจดหมายนั่นเป็นจดหมายธุรกิจที่สำคัญก็ย่อมจะส่งความเสียหายต่อธุรกิจ และความน่าเชื่อถือได้ไม่มากก็น้อย ดังนั้น หากผู้ใช้

---

[21] เรืองไกร รังสิต, เปิดโลก Firewall และ Internet Security พิมพ์ครั้งที่ 1(กรุงเทพฯ : โปรวิชั่น, 2545), หน้า 254.

ต้องการเพิ่มเนื้อที่กล่องจดหมายของตนให้ใหญ่ขึ้น เพื่อให้เพียงพอต่อการรับสแปมเมลจำนวนมากที่เข้ามาในแต่ละวันได้ โดยไม่ต้องการเสียเวลาในการแยกจดหมายของตนออกจากสแปมเมล ผู้ใช้อินเตอร์เนตก็ต้องเสียค่าใช้จ่ายเพิ่มขึ้นเพื่อการนี้ด้วย

2.6.1.2 สิ้นเปลืองแบนด์วิดธ์* (Bandwidth)

การที่สแปมเมลจะเข้ามาอยู่ในกล่องจดหมายได้นั้น ก็จะต้องใช้แบนด์วิดธ์ที่มีอยู่ของเมลเซิร์ฟเวอร์ไปพอๆ กับขนาดของเมลนั้น หากแบนด์วิดธ์มีอย่างจำกัดก็จะทำให้ เมลอื่นที่จะส่งเข้ามาจะต้องใช้เวลานานกว่าปกติ หากมีการใช้แบนด์วิดธ์มากจนเมลอื่นส่งเข้ามาไม่ได้ก็จะทำให้เมลนั้นจะต้องเลื่อนเวลาการส่งออกไป โดยปกติหาก MTA ส่งเมลต่อไม่ได้ก็จะทำการพยายามส่งใหม่ทุก 4 ชั่วโมง หากภายใน 3 วันตามที่ได้กำหนดไว้ใน MTA ยังส่งไม่ได้ก็จะส่งเมลฉบับนั้นคืนผู้ส่ง) ซึ่งการที่มีแบนด์วิดธ์ที่จำกัดจะส่งผลให้เมลได้รับช้าลงและอาจจะไม่ได้รับได้ในที่สุด ซึ่งส่งผลต่อผู้ใช้ระบบการสื่อสารในเครือข่ายนั้นได้

การใช้แบนด์วิดธ์ข้างต้นเป็นการใช้เพื่อการส่งอีเมลเข้าไปยังเซิร์ฟเวอร์ การใช้แบนด์วิดธ์อีกกรณีหนึ่งที่ผู้ใช้ประสบโดยตรงก็คือ กรณีที่ผู้ใช้ต้องเชื่อมต่อไปยังเมลเซิร์ฟเวอร์ โดยผ่านโมเด็มเพื่อทำการดาวน์โหลดอีเมลลงมาเก็บและเปิดอ่านในเครื่องตนเองโดยโปรแกรมเมลไคลเอนต์ ในกรณีนี้จะเห็นได้ชัดมากว่าแบนด์วิดธ์ถูกใช้ไปอย่างไร หากมีจำนวนเมลมากเวลาที่ใช้ในการดาวน์โหลดก็จะนานมากขึ้น

หากผู้ให้บริการอินเตอร์เนต (ISP) ต้องการรักษาระดับความเร็วของการเข้าสู่ระบบ เพื่อให้เป็นที่พึงพอใจของลูกค้า และรักษาระดับฐานลูกค้าของตนไว้ ผู้ให้บริการอินเตอร์เนต ก็ต้องเสียค่าใช้จ่ายในการจ้างพนักงานเพิ่ม เพื่อคัดแยกสแปมเมลออกจากระบบ หรือมิเช่นนั้น ก็จะต้องขยายความกว้างของแบนด์วิดธ์ซึ่งก่อให้เกิดค่าใช้จ่ายที่เพิ่มขึ้นสำหรับผู้ให้บริการอินเตอร์เนตด้วย

---

* แบนด์วิดธ์ (bandwidth) หรือช่องสัญญาณของการส่งผ่านสัญญาณสื่อสารเป็นการวัดช่วงความถี่ ใช้เรียกปริมาณการรับส่งข้อมูลที่เข้าออกของเซิร์ฟเวอร์ หรือบนเว็บไซต์ ในระบบดิจิตอล bandwidth คือความเร็วข้อมูลเป็น bits per second (จำนวนบิตต่อวินาที)

2.6.1.3 สิ้นเปลืองเวลาประมวลผลของซีพียู* (Central Processor Unit)

เมลทุกฉบับที่เข้ามายังเมลเซิร์ฟเวอร์ ย่อมจะต้องใช้เวลาในการประมวลผลของซีพียูไม่มากก็น้อย และถึงแม้ว่าการประมวลผลเพื่อรับอีเมลฉบับหนึ่ง และนำไปจัดเก็บยังกล่องจดหมายของผู้ใช้แต่ละคน จนกระทั่งถึงการอ่านออกมาจากกล่องจดหมาย และส่งไปให้ผู้ใช้เมื่อมีการขอดาวน์โหลดเมลจนครบกระบวนการนั้น จะไม่ได้ใช้เวลาการประมวลผลของซีพียูเท่าใดนัก แต่หากเซิร์ฟเวอร์นั้นมีภาระต้องรับส่งอีเมลจำนวนมากก็ย่อมจะต้องใช้เวลาของซีพียูมากขึ้นเป็นเท่าทวีคูณ ดังนั้น การเข้ามาของสแปมเมลก็ย่อมจะสร้างภาระในการประมวลผลของซีพียูมากขึ้นจากเดิมอย่างแน่นอน ซึ่งถึงแม้ว่าซีพียูจะมีความเร็วมากเท่าไรก็ตามก็ย่อมจะมีขีดจำกัดในการประมวลผลอยู่ว่าจะสามารถรองรับจดหมายได้เท่าใด หากเกินกว่าขีดจำกัด แล้วก็ไม่สามารถที่จะประมวลผลได้ทันจดหมายที่เข้ามาก็จะต้องถูกเลื่อนเวลาการรับออกไปเช่นกัน

2.6.1.4 สิ้นเปลืองเวลาของผู้ใช้[22]

ในแง่ของผู้ใช้อินเตอร์เนตในฐานะผู้บริโภคนั้น หากมีสแปมเมลเข้ามายังกล่องจดหมายของตนเป็นจำนวนมากในแต่ละวัน ผู้ใช้ก็จะต้องเสียเวลาเพื่อลบสแปมเมลออกไป ซึ่งนอกจากจะเป็นการเสียเวลาในการจัดการกับสแปมเมลแล้ว หากเป็นกรณีที่ผู้ใช้อินเตอร์เนตไม่ได้เหมาจ่ายค่าธรรมเนียมการใช้อินเตอร์เนต โดยอาจจ่ายจากการคำนวณตามเวลาของการใช้งาน เวลาที่ผู้ใช้ต้องเสียไปในการดาวน์โหลดและลบสแปมเมลจำนวนมากในแต่ละวันนั้นกินเวลาการใช้อินเตอร์เนต ซึ่งมีผลทำให้ผู้ใช้อินเตอร์เนตต้องเสียค่าธรรมเนียมการใช้อินเตอร์เนตไปกับเมลที่ผู้ใช้ไม่เคยร้องขอด้วย

ในบางกรณีสแปมเมลได้ส่งผลให้เกิดความเสียหายได้มากกว่าที่คิด เช่น กรณีที่มีการใช้ที่อยู่อีเมลของกลุ่ม กล่าวคืออีเมลที่เป็น "แอเลียซ" ซึ่งไม่ได้เป็นกล่องจดหมายจริง แต่อีเมลที่เข้ามายังแอดเดรสนี้จะถูกกระจายไปยังกล่องจดหมายของผู้ที่เป็นสมาชิกทุกคน ดังนั้นหากภายในแอเลียซนั้นมีสมาชิกอยู่จำนวนเท่าใด เมลก็จะถูกกระจายออกไปเท่ากับจำนวนสมาชิกที่อยู่ภายในกลุ่มนั้น ซึ่งทำให้เกิดการขยายขอบเขตของสแปมเมลโดยอัตโนมัติ โดยส่วนใหญ่การมีแอเลียซก็เพื่อง่ายต่อการส่งจดหมายไปยังกลุ่มของผู้ใช้โดยไม่ต้องเลือกอีเมลแอดเดรสของแต่ละคน เช่นแอเลียซของพนักงาน

---

* ซีพียู (Central Precessor Unit) คือหน่วยประมวลผลกลางในคอมพิวเตอร์ ประกอบด้วยวงจรตรรกะ เพื่อประมวลผลคำสั่งของโปรแกรมคอมพิวเตอร์ ให้แสดงออกมาทางจอคอมพิวเตอร์ เปรียบได้กับสมองของมนุษย์

[22] อรรยา สิงห์สงบ, "ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ (Spam Mail)," นักบริหาร 23,4 (ต.ค. – ธ.ค. 2546) : 84-90.

แต่ละแผนก แอเลียซของคณะทำงาน แอเลียซของพนักงานทั้งบริษัท ดังนั้นถึงแม้ว่าสแปมเมลจะเข้ามายังอีเมลแอดเดรสของแอเลียซเพียงฉบับเดียว แต่เมื่อมาถึงเมลเซิร์ฟเวอร์ก็จะถูกกระจายออกเป็นหลายร้อยฉบับในทันที ซึ่งกรณีเช่นนี้จะส่งผลกระทบต่อเวลาในการประมวลผลของซีพียู และเนื้อที่ดิสก์ที่เก็บอีเมลอย่างมากมาย จนอาจจะทำให้เมลเซิร์ฟเวอร์หยุดทำงานลงไปได้

2.6.1.5 สิ้นเปลืองค่าใช้จ่ายในการป้องกัน

ค่าใช้จ่ายในการติดตั้งโปรแกรมแอนตี้สแปม รวมถึงค่าบำรุงรักษาให้มีความทันสมัยอยู่เสมอ เป็นค่าใช้จ่ายที่สูงและมีความจำเป็นอย่างมาก เพราะหากว่าไม่มีการติดตั้งระบบป้องกันความปลอดภัยที่ดีเพียงพอ ความเสียหายที่เกิดขึ้นอาจจะมีมูลค่ามากกว่าจำนวนเงินที่ต้องเสียไปในการแก้ไขก็ได้ โดยเฉพาะในองค์กรใหญ่ หากระบบคอมพิวเตอร์ล่มแล้ว ความเสียหายในการแก้ไขให้กลับคืนมาใช้ได้ดังเดิม รวมถึงค่าเสียโอกาสทางธุรกิจต่างๆ อาจจะมีมูลค่าที่ไม่สามารถประเมินค่าได้เลยทีเดียว และบ่อยครั้งที่สแปมเมลบางตัวจะมีไวรัส โปรแกรมเวิร์ม (Worm) หรือพวกสปายแวร์แฝงมาด้วย ซึ่งนอกจากจะเป็นภัยต่อเครื่องคอมพิวเตอร์เองแล้ว บางครั้งยังเป็นภัยต่อผู้ใช้เครื่องคอมพิวเตอร์โดยไม่รู้ตัวอีกด้วย เพราะข้อมูลส่วนตัวของตนอาจจะถูกเก็บรวบรวม และนำไปใช้โดยบุคคลที่เราไม่ทราบว่าเป็นใครก็ได้ หรือเป็นค่าใช้จ่ายที่เกิดจากการที่บริษัทผู้ให้บริการอินเตอร์เนตบางรายต้องจ้างบุคคลากรเพิ่มขึ้นเพื่อคอยสอดส่องดูแล และคอยจัดการกับสแปมเมลที่เข้ามาในแต่ละวัน นอกจากนั้นเครื่องคอมพิวเตอร์อาจจะทำงานได้เร็วกว่านี้หากไม่ต้องเสียกำลังของเครื่องไปกับการทำงานของโปรแกรมเหล่านี้

2.6.2 ผลกระทบต่อชื่อเสียง

เนื่องจากสแปมเมลเป็นเรื่องที่สร้างความรำคาญใจให้แก่ผู้รับ และก่อให้เกิดผลกระทบแก่ผู้ที่เกี่ยวข้องมากมาย ดังนั้น ผู้ส่งสแปมเมลจึงเป็นที่รังเกียจ และไม่ได้รับการยอมรับจากสังคมทั่วไป ซึ่งรวมถึงผู้ที่ยอมให้ใช้เมลเซิร์ฟเวอร์ของตนเป็นตัวกลางในการกระจายอีเมลด้วย อย่างไรก็ดี ในกรณีที่เครื่องเซิร์ฟเวอร์ที่เราใช้ส่งอีเมลไปนั้น เปิดให้ผู้อื่นใช้เป็นตัวกลางส่งอีเมลหรือที่เรียกว่าเปิด Relay ด้วย อันอาจเป็นผลให้เซิร์ฟเวอร์เครื่องนั้นถูกใช้เป็นตัวกลางในการสแปมเมลโดยที่ตัวเองไม่ทราบ หรือมีระบบการป้องกันที่ไม่ดีพอ ก็อาจถูกขึ้นบัญชีดำจากองค์กรอื่น เพื่อไม่อนุญาตให้รับอีเมลใดก็ตามที่มาจากเครื่องเซิร์ฟเวอร์นั้น อันทำให้ต้องพลาดโอกาสในการส่งอีเมลที่ถูกกฎหมาย เสียชื่อเสียง เสียลูกค้าไปในที่สุด ส่งผลกระทบต่อธุรกิจ ความน่าเชื่อถือ และลูกค้าที่อยู่ในระบบเครือข่ายนั้นได้

นอกจากนี้ ลักษณะสำคัญประการหนึ่งของสแปมเมล คือ การส่งอีเมลโดยใช้ที่อยู่ หรือหัวเรื่องของอีเมลที่ไม่เป็นความจริง เพื่อป้องกันตนเองจากข้อกฎหมาย และการถูกโจมตีกลับจากผู้รับ โดยบางครั้งก็ใช้ชื่อและที่อยู่ของหน่วยงาน หรือบริษัทที่มีชื่อเสียง เพื่อที่จะหลอกให้ผู้รับสนใจที่จะเปิดอ่านจดหมายของตน หรือตอบกลับ อันเป็นการทำลายชื่อเสียงของหน่วยงาน หรือบริษัทนั้นๆ และยังถือว่าเป็นการปลอมแปลง หรือใช้เครื่องหมายการค้านั้นโดยมิได้รับความยินยอมอีกด้วย

2.6.3 ผลกระทบต่อสิทธิและความเป็นส่วนตัวของผู้รับ (Privacy)

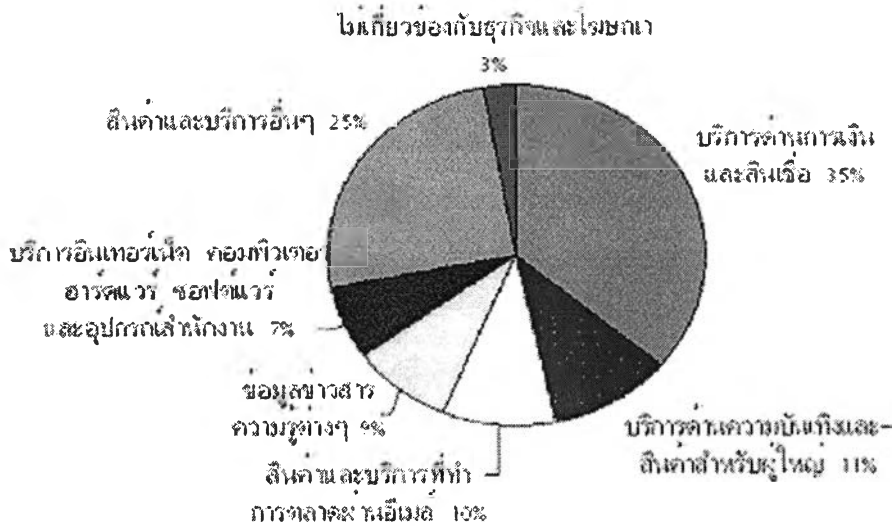
สแปมเมลถือเป็นการรบกวนการครอบครองสังหาริมทรัพย์ (Trespass) อันเป็นสิทธิพื้นฐานที่พึงมีของผู้เป็นเจ้าของกรรมสิทธิ์ เนื่องจากการส่งสแปมเมลต้องอาศัยเครื่องมือ และอุปกรณ์มากมายเพื่อเป็นตัวเชื่อมไปยังผู้รับ ไม่ว่าจะเป็นเซิร์ฟเวอร์ของผู้ให้บริการอีเมล หรือแบนด์วิดธ์ของผู้ให้บริการอินเตอร์เนต อุปกรณ์ต่างๆ เหล่านี้ต้องอาศัยการลงทุนเป็นจำนวนมากและเป็นสิทธิของผู้เป็นเจ้าของในอันที่จะใช้ประโยชน์ให้เต็มที่จากทรัพย์สินเหล่านั้น การนำเอาเครื่องมือต่างๆ เหล่านั้นไปหาประโยชน์จากการส่งสแปมเมล โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ เป็นการรบกวนสิทธิในการครอบครองสังหาริมทรัพย์ของผู้เป็นเจ้าของสังหาริมทรัพย์นั้น เพราะหากจำนวนสแปมเมลมีมากเกินไป ก็จะทำให้เซิร์ฟเวอร์ และแบนด์วิทธ์ของผู้ให้บริการต้องทำงานหนัก สูญเสียเนื้อที่จำนวนมากให้กับสแปมเมล และไม่สามารถใช้ประโยชน์ได้อย่างเต็มที่

ผลกระทบเรื่องความเป็นส่วนตัวของผู้ที่ได้รับสแปมเมลนั้น คือการรวบรวมรายชื่อและที่อยู่ของผู้ใช้อีเมลโดยเจ้าของเว็บไซต์ นายหน้า หรือบุคคลใดก็ตาม เพื่อนำไปจำหน่ายให้กับผู้ส่งสแปมเมลเพื่อใช้ในการส่งสแปมเมล โดยที่ผู้เป็นเจ้าของชื่อและที่อยู่นั้นไม่ทราบ และไม่ได้ให้ความยินยอม อันเป็นการละเมิดความเป็นส่วนตัวของเจ้าของอีเมล และเมื่อสแปมเมลจำ นวนมากหลั่งไหลเข้ามาในอีเมลของผู้รับ โดยสแปมเมลส่วนใหญ่ไม่สามารถบอกเลิก หรือปฏิเสธได้ จึงเป็นการบังคับให้เจ้าของอีเมลต้องยอมรับสแปมเมลเหล่านั้นไปโดยปริยายโดยที่ไม่สามารถแก้ไขอย่างไรได้ อันก่อให้เกิดผลกระทบถึงความเป็นส่วนตัวของผู้รับที่จะเลือกรับรู้ รับฟัง ข่าวสารอย่างใด ก็แต่เฉพาะที่ตนเลือก หรือพอในเท่านั้น นอกจากนั้น ความเป็นส่วนตัวยังถูกคุกคามจากการที่กล่องจดหมายของผู้รับเต็มไปด้วยสแปมเมลมากกว่าจดหมายที่ผู้รับต้องการ ส่วนในกรณีของผู้ให้บริการฟรีอีเมลนั้น ก็ขึ้นอยู่กับนโยบายความลับของบริษัทด้วยว่าจะนำอีเมลแอดเดรสไปขาย หรือนำไปใช้งานร่วมกับบริษัทอื่นๆ หรือไม่ ซึ่งหากในข้อตกลงการใช้บริการฟรีอีเมลไม่ได้ระบุไว้ การนำอีเมลแอดเดรสของลูกค้าไปขายก็ย่อมเป็นการผิดข้อตกลงการให้บริการและกระทบต่อความเป็นส่วนตัวของผู้ใช้บริการด้วยเช่นกัน

2.6.4 ผลกระทบต่อสังคมและศีลธรรมอันดี

เนื้อหาของสแปมเมลนั้น มีความหลากหลาย โดยมีทั้งที่เป็นการโฆษณาสินค้า บริการ จดหมายลูกโซ่ การหารายได้เสริมพิเศษ แต่สแปมเมลที่มักจะก่อให้เกิดปัญหามักจะเป็น สแปมเมลที่เป็นการโฆษณาสินค้าและบริการที่ไม่ชอบด้วยกฎหมาย มีเนื้อหาที่ขัดต่อศีลธรรมอันดี หรือมีข้อความที่มีลักษณะหลอกลวง ใส่ร้ายคู่แข่งทางการค้า เช่น โฆษณาว่ามีการแจกสินค้าฟรี หากส่งจดหมายนี้ต่อไปยังคนที่รู้จักอย่างน้อย 20 คน หรือโฆษณาชวนเชื่อในลักษณะแชร์ลูกโซ่ โดยหลอกให้จ่ายเงินล่วงหน้าเพื่อรับโชคก้อนใหญ่ หรือโฆษณาที่มีเนื้อหาขัดต่อศีลธรรมอันดี เช่นสแปมเมลที่เป็นการชักชวนให้เข้าชมภาพลามกอนาจารต่างๆ หรือโฆษณาเว็บไซต์ หรือสินค้าสำหรับผู้ใหญ่ การพนัน เป็นต้น ซึ่งสแปมเมล เป็นสิ่งที่ส่งไปยังผู้รับจำนวนมากๆ ได้ โดยไม่จำกัดการส่ง ดังนั้นจึงเป็นการยากในการจำกัดกลุ่มเป้าหมายในการส่งสแปมเมลได้ และมีความเป็นไปได้สูงที่เด็กอายุยังไม่ถึง 10 ขวบก็มีสิทธิที่จะได้รับสแปมเมลที่เป็นการโฆษณาเว็บไซต์ภาพลามกได้เช่นกัน

นอกจากนี้ ก็อาจมีผู้อาศัยการส่งสแปมเมลเป็นเครื่องมือในการโจมตีว่าร้ายผู้อื่น หรือหลอกลวงถึงภัยร้าย หรืออันตรายต่างๆ ที่เกินจริง โดยไม่มีการตรวจสอบข้อเท็จจริง หรือมีการพิสูจน์แล้วแต่อย่างใด หรือที่เรียกว่า Hoax ที่มักจะมีการส่งต่อเนื่องกันไปอยู่บ่อยๆ ก่อให้เกิดความสับสนและตื่นตระหนก และความเข้าใจที่ผิดแก่ผู้รับในลักษณะที่เกินจริงโดยที่ยังไม่มีการตรวจสอบข้อเท็จจริงแต่อย่างใด แต่ไม่ว่าสแปมเมลจะมีเนื้อหาอย่างไรก็ตาม การส่งสแปมเมลก็ก่อให้เกิดผลกระทบต่อสังคมในวงกว้าง ทั้งทางด้านเศรษฐกิจ สังคม และการเมือง อย่างหลีกเลี่ยงไม่ได้ ไม่ทางใดก็ทางหนึ่ง



ประเภทของโฆษณาและผลิตภัณฑ์จากสแปมเมล[23]

2.6.7 ผลกระทบในเรื่องอื่นๆ

เนื่องจากคุณสมบัติของสแปมเมลที่ส่งได้คราวละมากๆ โดยไม่จำกัดจำนวน และส่งออกไปได้ทั่วโลก ทำให้มีไวรัสจำนวนไม่น้อยที่อาศัยคุณสมบัติในการกระจายตัวได้อย่างรวดเร็วของสแปมเมลนี้ แฝงตัวมากับสแปมเมลแต่ละฉบับด้วย ซึ่งไวรัสบางตัวก็อาจจะก่อความเสียหายให้แก่เครื่องคอมพิวเตอร์เพียงเล็กน้อย แต่ก็มีบางครั้งที่ไวรัสบางตัวได้เปลี่ยนเครื่องคอมพิวเตอร์ของเราให้กลายเป็นเครื่องกระจายสแปมเมลออกไปอีก อีกทั้งยังเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเก็บเกี่ยวข้อมูลของเราไปใช้ด้วย ไวรัสที่ส่งมากลับสแปมเมลกระตุ้นให้ผู้รับเปิดไวรัสออกมาได้ง่ายมากขึ้น เพราะมีการหลอกล่อต่างๆ เช่นการแจ้งเตือนให้อัพเดทโปรแกรมที่สำคัญ โดยการกดเชื่อมต่อไปยังลิงค์ที่ส่งมาให้ ซึ่งหากเราไม่ทราบและทำการอัพเดทไป ก็จะทำให้เครื่องคอมพิวเตอร์ของผู้ใช้ติดไวรัส อันก่อให้เกิดความเสียหายอย่างมากมายโดยไม่รู้ตัว

ดังนั้นเมื่อพิจารณาถึงผลกระทบ และจำนวนสแปมเมลที่เพิ่มขึ้นทุกปีแล้ว มาตรการทางเทคนิคเพียงอย่างเดียว เช่น การติดตั้งโปรแกรมในการกลั่นกรองสแปมเมล อาจไม่เพียงพอที่จะหยุดยั้งหรือลดจำนวนสแปมเมลได้ เพราะสแปมเมอร์ก็มักจะหาช่องทางใหม่ๆ ในการหลีกเลี่ยงการดักจับจากโปรแกรมต่อต้านสแปมทั้งหลาย ผนวกกับความสามารถทางเทคโนโลยีที่เพิ่มมากขึ้นทุกขณะทำ

---

[23] เกียรติศักดิ์ อนุธรรม, **"จัดระเบียบอีเมลด้วยกฎและการกลั่นกรอง," ที่** http://industrial.se-ed.com/itr114/itr114_170.asp**(13 ตุลาคม 2547) : 3.**

ให้ขีดความสามารถในการส่งสแปมเมลเพิ่มมากขึ้น และมีรูปแบบที่พัฒนาไปอย่างต่อเนื่อง จนกระทั่งการใช้โปรแกรมในการต่อต้านสแปมเมลเพียงอย่างเดียวไม่เพียงพออีกต่อไป สแปมเมลไม่ใช่เป็นเพียงแต่ปัญหาของประเทศใดประเทศหนึ่งที่จะต้องแก้ไขเท่านั้น แต่สแปมเมลยังได้กลายเป็นประเด็นสำคัญระดับโลกไปแล้ว ทุกประเทศต่างหามาตรการป้องกันสแปมเมล ดังนั้น เพื่อแก้ไขปัญหาสแปมเมลมาตรการทางกฎหมายจึงเป็นทางเลือกที่หลายๆ ประเทศเริ่มนำมาใช้เพื่อจัดการกับสแปมเมอร์ และผู้ประกอบการต่างๆ ที่ใช้วิธีการสแปมเมลในการทำการตลาด