# รูปแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย



สิทธิพร พุ่มพวง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2554

# Spam Filtering installation Location to Reduce the Network Traffic

**SITTIPORN PHUMPUANG**



**A Thesis Submitted in Partial Fulfillment of the Requirements**

**for the Degree of Master of Engineering**

**Department of Computer and Telecommunication Engineering**

**Graduate School, Dhurakij Pundit University**

**2011**

# ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญาวิศวกรรมศาสตรมหาบัณฑิต

หัวข้อวิทยานิพนธ์ รูปแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย

เสนอโดย จ่าสิบตรีสิทธิพร พุ่มพวง

สาขา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ อาจารย์ ดร.เนื่องวงศ์ ทวยเจริญ

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบวิทยานิพนธ์แล้ว

.....ประธานกรรมการ

(อาจารย์ ดร.ประศาสน์ จันทราทิพย์)

.....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์

(อาจารย์ ดร.เนื่องวงศ์ ทวยเจริญ)

.....กรรมการ

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

.....กรรมการ

(อาจารย์ ดร.กุลธิดา โรจน์วิบูลย์ชัย)

บัณฑิตวิทยาลัยรับรองแล้ว

.....คณบดีบัณฑิตวิทยาลัย

(รองศาสตราจารย์ ดร.ธนิดา จิตร์น้อมรัตน์)

วันที่ 6 เดือน สิงหาคม พ.ศ. 2554

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาจากอาจารย์ ดร.เนื่องวงศ์ ทวยเจริญ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่ได้กรุณาให้ความรู้ คำแนะนำ ตรวจทาน ตลอดจนแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่ทุกขั้นตอน เพื่อให้วิทยานิพนธ์ฉบับนี้สมบูรณ์ที่สุด ขอขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์อาจารย์ ดร.กุลธิดา โรจน์วิบูลย์ชัย อาจารย์ ดร.ประศาสน์ จันทราทิพย์ และอาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ ซึ่งได้สละเวลามาเป็นกรรมการสอบวิทยานิพนธ์ ตลอดจนให้ข้อคิดเห็นที่เป็นประโยชน์ต่องานวิจัยอย่างยิ่ง นอกจากนี้ผู้วิจัยขอขอบพระคุณคณาจารย์ทุกๆ ท่านในสาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม ที่ได้ถ่ายทอดความรู้แก่ผู้วิจัยตลอดระยะเวลาการศึกษา

ผู้วิจัยขอขอบพระคุณ เจ้าหน้าที่ที่เกี่ยวข้องทุกท่าน ในสาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม ที่คอยให้ความช่วยเหลือ ตลอดจนแนะนำกระบวนการในการทำงานให้แก่ผู้วิจัยด้วยดีเสมอมา

ผู้วิจัยขอขอบพระคุณ กรมพลาธิการทหารบก และกองทัพบก ที่ส่งเสริมการศึกษาและให้ข้อมูลที่เป็นประโยชน์ต่อการทำวิจัยครั้งนี้จนสำเร็จลุล่วงได้ด้วยดี

สุดท้ายนี้ ขอกราบขอบพระคุณบิดา มารดา และครอบครัว ตลอดจนเพื่อน ๆ ทุกท่านที่คอยเป็นกำลังใจและให้การสนับสนุนผู้วิจัยในทุก ๆ ด้านเสมอมาจวบจนสำเร็จการศึกษา

สิทธิพร พุ่มพวง

# สารบัญ

หน้า

# สารบัญ (ต่อ)

# สารบัญตาราง

# สารบัญภาพ

ภาพที่ หน้า

# สารบัญภาพ(ต่อ)

ภาพที่ หน้า

| | |
|---|---|
| หัวข้อวิทยานิพนธ์ | รูปแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย |
| ชื่อผู้เขียน | สิทธิพร พุ่มพวง |
| อาจารย์ที่ปรึกษาวิทยานิพนธ์ | อาจารย์ ดร. เนื่องวงศ์ ทวยเจริญ |
| สาขาวิชา | วิศวกรรมคอมพิวเตอร์และโทรคมนาคม |
| ปีการศึกษา | 2554 |

## บทคัดย่อ

งานวิจัยนี้ได้พัฒนาระบบจดหมายอิเล็กทรอนิกส์ขึ้น ภายในกองยุทธการและการข่าว กรมพลาธิการทหารบก เพื่อเป็นการปฏิบัติตามมติคณะรัฐมนตรี เมื่อวันที่ 18 ธันวาคม พ.ศ. 2550 ที่ให้ข้าราชการและพนักงานของรัฐยุติการใช้งานอีเมลฟรีของเอกชน ทั้งนี้ เพื่อแก้ปัญหาการรั่วไหลข้อมูลลับของทางราชการ

อย่างไรก็ตามในปัจจุบันการใช้งานอีเมลส่วนใหญ่ ผู้ให้บริการต้องเสียพื้นที่และค่าใช้จ่ายไปกับ Spam mail ถึง 97 % ดังนั้นการใช้ตัวกรองสแปมที่มีประสิทธิภาพจะสามารถลดค่าใช้จ่ายได้อย่างมหาศาล

ดังนั้น งานวิจัยนี้จึงศึกษาผลความแตกต่างของตำแหน่งการติดตั้งตัวกรองข้อความสแปม ระหว่างตำแหน่งของแม่ข่ายและตำแหน่งของลูกข่าย โดยมีวัตถุประสงค์เพื่อออกแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย .

จากการวัดประสิทธิภาพของตัวกรองข้อความสแปมด้วยปริมาณการจราจรบนเครือข่าย พบว่าเมื่อติดตั้งตัวกรองข้อความสแปมที่เครื่องลูกข่าย สามารถลดปริมาณการจราจรลงได้ถึง 72.38 % และเมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย ตัวกรองข้อความสแปมสามารถลดปริมาณการจราจรลงได้ถึง 81.55 %

ดังนั้น ตัวกรองข้อความสแปมในฝั่งลูกข่ายสามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับตัวกรองที่ฝั่งแม่ข่าย พร้อมทั้งลดภาระการทำงานที่เครื่องแม่ข่าย ด้วยเหตุนี้ การติดตั้งตัวกรองสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองสแปมที่น่าสนใจในอนาคต

| | |
|---|---|
| Thesis Title | Spam Filtering installation Location to Reduce the Network Traffic |
| Author | Sittiporn Phumpuang |
| Thesis Advisor | Nuengwong Tuaycharoen, Ph.D. |
| Department | Computer and Telecommunication Engineering |
| Academic Year | 2011 |

## ABSTRACT

Due to the Thai Cabinet's Resolution on December 18th, 2007, the government agencies have to discontinue using free private email services, which lead to the disclosure of the government classified information. This research has developed an electronic mail system for the Battle and News Division, the Department of the Army Quartermaster.

However, a recent research indicates that most e-mail service providers need to waste 97% of space and money with Spam mails. Therefore, an effective spam filter can reduce costs dramatically.

Therefore, this research is to study the impact of installing the spam-mail filters, i.e. server-side installation versus client-side installation. The objective is to explore various installation locations in the mail system architecture for the purpose of reducing the network traffic.

The experimental results show that installing the spam filter at the client can reduce the traffic up to 72.38%, while installing the filter at the server can reduce traffic up to 81.55%.

In conclusion, the client-side spam filter can reduce the network traffic as effective as the server-side filters. Also, it reduces the workload on the server as well. Additionally, the effectiveness of the client-side filtering can be improved if the filter is included in the default feature of a web browser, which will process all web mail forms. Therefore, client-side spam filtering is a promising alternative in spam filter.

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมาและความสำคัญของปัญหา

งานวิจัยนี้ได้พัฒนาระบบจดหมายอิเล็กทรอนิกส์ขึ้น ภายในกองยุทธการและการข่าว กรมพลาธิการทหารบก เพื่อเป็นการปฏิบัติตามมติคณะรัฐมนตรี เมื่อวันที่ 18 ธันวาคม พ.ศ. 2550[1] ที่ให้ข้าราชการและพนักงานรัฐยุติการใช้งานอีเมลฟรีของเอกชน ทั้งนี้ เพื่อแก้ปัญหาการรั่วไหลข้อมูลลับของทางราชการ อย่างไรก็ตามระหว่างที่หน่วยงานของรัฐได้ดำเนินการตามมตินี้อย่างค่อยเป็นค่อยไป การปฏิบัติตามมตินี้จำเป็นต้องพิจารณาปัญหาด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างยิ่ง เนื่องจากปัจจุบันอีเมลได้กลายเป็นช่องทางการสื่อสารสำคัญอีกช่องทางหนึ่ง ที่กลุ่มอาชญากรไซเบอร์ได้ใช้ช่องทางดังกล่าวในการสร้างความเสียหาย โดยมุ่งเป้าหมาย 3 ลักษณะ คือ

1) การนำความลับไปเปิดเผย (Data Confidentiality)

2) การเปลี่ยนแปลงข้อมูล (Data Integrity)

3) การทำให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System Availability)

รูปแบบภัยคุกคามที่เกิดขึ้นในปัจจุบันได้เปลี่ยนแปลงไป โดยถูกส่งมาในรูปของข้อมูลข่าวสาร ความรู้ วิทยาการต่างๆ เรื่องตลกขบขัน เรื่องคอลัมน์นินทาระหว่างเพื่อนร่วมงาน การส่งข่าวของลดราคาหรือจดหมายแจ้งข่าว จดหมายที่มีข้อความโฆษณาสินค้า บริการต่างๆ และเว็บไซต์ภาพลามก (Commercial Message Advertising) จดหมายลูกโซ่ (Chain Letters) ที่มีการขู่ว่าถ้าไม่ส่งต่อผู้รับจดหมายจะต้องเผชิญกับความหายนะเช่น Chain Mail เป็นข้อความลูกโซ่ที่แสดงเนื้อหาคำเตือนเกี่ยวกับไวรัสหรือเรื่องอื่นใด โดยมีจุดมุ่งหมายเพื่อแพร่กระจายด้วยการส่งต่อ Chain Mail ซึ่งสร้างความเสียหายกับตัว Mail Server ของผู้ให้บริการอินเทอร์เน็ตทำให้ Server down หรือทำงานช้าลง ทำให้ traffic ของเครือข่ายอินเทอร์เน็ตติดขัด นอกจากนี้ยังก่อให้เกิดความรำคาญใจแก่ผู้ใช้บริการอีกด้วย รูปแบบภัยคุกคามข้างต้นที่กล่าวมานี้ถูกเรียกว่า Spam

สแปมเมล ( Spam Mail) หมายถึง จดหมายอิเล็กทรอนิกส์ที่ผู้ส่ง (ซึ่งมักจะไม่ปรากฏชื่อและที่อยู่ของผู้ส่ง) ได้ส่งไปยังผู้รับอย่างต่อเนื่อง โดยส่งจำนวนครั้งละมากๆ และมิได้รับความ

---

[1] รัฐบาลไทย (2550). **ผลการประชุมคณะรัฐมนตรี ประจำวันที่ 18 ธันวาคม 2550.** หน้า 18.

ยินยอมจากผู้รับ โดยการส่งสแปมเมลนั้นอาจมีวัตถุประสงค์ในเชิงพาณิชย์หรือไม่ก็ได้ ซึ่งในปัจจุบันการส่งสแปมเมลนั้นสามารถส่งผ่านได้โดยทางไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) หรือทางโทรศัพท์มือถือเป็นข้อความสั้นๆ (SMS) อย่างไรก็ตามงานวิจัยนี้จะกล่าวถึงแต่การส่งสแปมเมลทางไปรษณีย์อิเล็กทรอนิกส์เท่านั้น

Spam Mail คือ อีเมลที่มีลักษณะดังต่อไปนี้

1) ผู้ส่งอีเมลไม่มีที่มาหรือไม่มีความสำคัญกับธุรกิจหรือองค์กร

2) ไม่ทราบแหล่งที่มาหรือมีแหล่งที่มาซึ่งผิดกฎหมาย

3) ยากที่จะหาตัวตนหรือติดตามแหล่งอ้างอิงผู้ส่งซึ่งบ่งบอกว่าผู้ส่งไม่มีความน่าเชื่อถือ

4) ไม่ใช่จดหมายที่ส่งจากบุคคลหนึ่งถึงอีกบุคคลหนึ่ง แต่กระจายไปยังผู้รับหลายคน

5) เรียกร้องให้ผู้รับตอบสนองในทันทีทันใด ด้วยจุดดึงดูดความสนใจต่างๆ และมีข้อความเกินจริง

6) มีเนื้อหาผิดศีลธรรม ขัดกับอุตสาหกรรมขององค์กร หรือความเป็นมืออาชีพ

7) มีรูปแบบหรือชุดที่ผิดปกติ รวมถึงความพยายามที่จะฝ่าเทคนิคในการตรวจจับอัตโนมัติ

องค์กรธุรกิจที่จดทะเบียน Domain จะมีที่อยู่ไอพี ( IP Address ) เป็นหลักแหล่งทำให้ Spam Mail สามารถส่งมาถึงได้โดยไม่มีสิทธิหลีกเลี่ยง นั่นหมายถึงค่าใช้จ่ายในการใช้งานอีเมลที่เพิ่มขึ้นพร้อมๆ กับการสูญเสียทรัพยากรไปกับกองขยะ โดยเฉพาะ Mailbox จะต้องเสียค่าใช้จ่ายตามจำนวนข้อความที่ได้รับ เสียเวลา เสียทรัพยากร และเงินทุนของบริษัทในการดาวน์โหลดอีเมลขยะเหล่านั้น นอกจากนี้ในปัจจุบันการเข้าถึงอีเมลสามารถเข้าถึงได้ด้วยช่องทางพิเศษ เช่น การเปิดอีเมลผ่านระบบโทรศัพท์มือถือหรือการใช้งานอินเทอร์เน็ตผ่านระบบ EDGE, GPRS หรือ 3G ที่คิดค่าใช้จ่ายตามจำนวน Bandwidth ที่ใช้งาน เพราะฉะนั้นมันคุ้มแล้วหรือที่ต้องจ่ายเงินให้อีเมลขยะ (Spam Mail)

ในปัจจุบันการใช้งานอีเมลส่วนใหญ่ผู้ให้บริการต้องเสียพื้นที่และค่าใช้จ่ายไปกับสแปมถึง 97%[1] ดังนั้น การใช้ตัวกรองสแปมที่มีประสิทธิภาพจะสามารถลดค่าใช้จ่ายได้อย่างมหาศาล

ดังนั้น การศึกษาและทำความเข้าใจเกี่ยวกับภัยคุกคามทางอินเตอร์เน็ตที่กลุ่มอาชญากรไซเบอร์พยายามพัฒนาไปในทิศทางที่รุนแรงและซับซ้อนมากขึ้น อาทิ Spam Mail ที่สร้างความเสียหายกับตัว Mail Server เพื่อมุ่งหมายให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System

---

[1] บริษัท Microsoft (2009).**Microsoft report.** หน้า 1.

Availability) เป็นสิ่งจำเป็นและสำคัญยิ่งต่อการพัฒนาและการนำไปใช้ในการควบคุมการแพร่กระจาย การปกป้องข้อมูล และระบบไม่ให้ถูกทำลายจาก Spam Mail ซึ่งจากปัญหาด้านความปลอดภัยของคอมพิวเตอร์ที่เกิดจากการบุกรุกข้อมูลของ Spam Mail ต่อระบบเครือข่ายดังกล่าว จึงเป็นสาเหตุให้ผู้วิจัยมีแนวคิดที่จะพัฒนาโปรแกรมสำหรับตรวจสอบและทำการบล็อกข้อความที่ไม่เหมาะสมและข้อความสแปม อย่างไรก็ตามการติดตั้งโปรแกรมตรวจสอบและบล็อก สแปม สามารถทำได้หลายตำแหน่ง เช่น ที่เครื่องแม่ข่าย ที่เครื่องลูกข่าย หรือติดตั้งในอุปกรณ์เครือข่าย เช่น เราต์เตอร์ ซึ่งแต่ละตำแหน่งอาจให้ผลการกรองต่างกัน ผู้วิจัยจึงต้องการศึกษาผลกระทบของตำแหน่งการติดตั้งตัวกรองสแปมในเครือข่ายต่อประสิทธิภาพของตัวกรองสแปม

## 1.2 วัตถุประสงค์ของการวิจัย

เพื่อออกแบบตำแหน่งการติดตั้งตัวกรองข้อความสแปมเมลที่สามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้อย่างมีประสิทธิภาพ โดยพิจารณาการส่งข้อความสแปมเมลจากมนุษย์เป็นหลัก

## 1.3 สมมติฐานงานวิจัย

1. ศึกษาและรวบรวมข้อมูลเกี่ยวกับการโพสข้อความที่ไม่เหมาะสมเฉพาะภายในเครือข่ายคอมพิวเตอร์ของกรมพลาธิการทหารบก

2. วิเคราะห์ปัญหาจากสถิติการโพสข้อความที่ไม่เหมาะสม ภายในเครือข่ายคอมพิวเตอร์ของกรมพลาธิการทหารบก โดยพิจารณาข้อความที่ไม่เหมาะสมดังกล่าว พบว่าจัดอยู่ในกลุ่ม Spam จึงนำมาเป็นปัญหาในการทำวิทยานิพนธ์

3. ออกแบบและพัฒนาระบบตรวจสอบข้อความที่ไม่เหมาะสม เพื่อทำการบล็อกข้อความนั้นมิให้ถูกจัดส่งออกไป และแจ้งเตือนการกระทำความผิดนั้น

4. ติดตั้งระบบตรวจสอบและบล็อกข้อความสแปมที่เครื่องแม่ข่าย และเครื่องลูกข่ายในเครือข่ายคอมพิวเตอร์ของกรมพลาธิการทหารบก

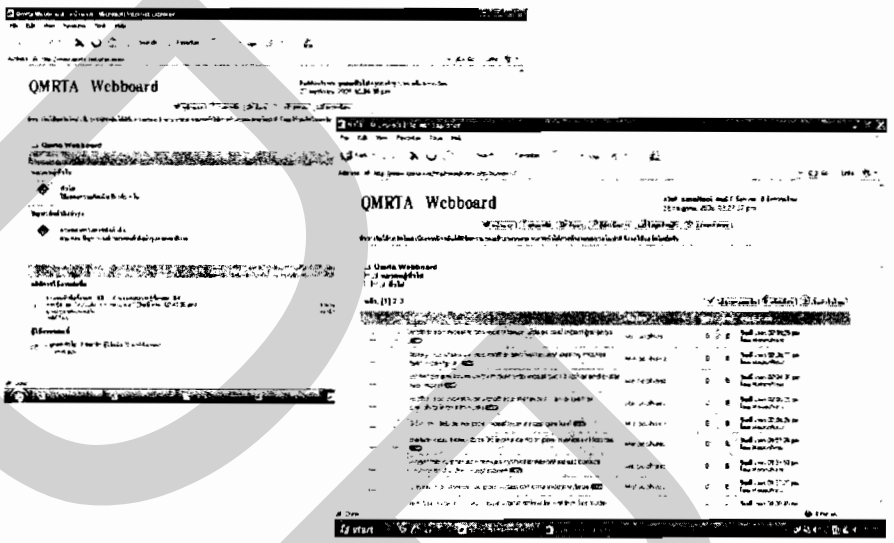
5. ทดสอบระบบตรวจสอบข้อความไม่เหมาะสมและแจ้งเตือนผู้กระทำผิดในเครือข่ายกรมพลาธิการทหารบก และเก็บข้อมูลปริมาณการจราจรในเครือข่ายของกรม

6. วิเคราะห์ข้อมูลปริมาณการจราจรในเครือข่ายคอมพิวเตอร์ของกรม เพื่อประเมินประสิทธิภาพการทำงานของตำแหน่งการติดตั้งระบบตรวจสอบและบล็อกข้อความสแปม

**1.4 ประโยชน์ที่คาดว่าจะได้รับ**

ลดปริมาณการส่งข้อมูลที่ไม่มีประโยชน์ในองค์กรอันเนื่องมาจากสแปม

# บทที่ 2
# บทความวิจัยที่เกี่ยวข้อง




ภาพที่ 2.1 Spam โจมตีเว็บบอร์ดกรมพลาธิการทหารบก

## 2.1 ความหมาย

สแปมเมล (Spam Mail) หมายถึง จดหมายอิเล็กทรอนิกส์ที่ผู้ส่ง (ซึ่งมักจะไม่ปรากฏชื่อและที่อยู่ของผู้ส่ง) ได้ส่งไปยังผู้รับอย่างต่อเนื่อง โดยส่งจำนวนครั้งละมากๆ และมิได้รับความยินยอมจากผู้รับ โดยการส่งสแปมเมลนั้นอาจมีวัตถุประสงค์ในเชิงพาณิชย์หรือไม่ก็ได้ ซึ่งในปัจจุบันการส่งสแปมเมลนั้นสามารถส่งผ่านได้โดยทางไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) หรือทางโทรศัพท์มือถือเป็นข้อความสั้นๆ (SMS) อย่างไรก็ตาม งานวิจัยนี้จะกล่าวถึงแต่การส่งสแปมเมลทางไปรษณีย์อิเล็กทรอนิกส์เท่านั้น

## 2.2 ที่มา

มีการสันนิษฐานกันว่า คำว่า " สแปม (Spam)" มาจากละครสั้นทางโทรทัศน์ชื่อ Monty Python's Flying Circus ซึ่งมีการร้องประสานเสียงโดยร้องคำว่า S-P-A-M ซ้ำไปซ้ำมาและร้องเสียง

ดังมากจนไม่สามารถได้ยินบทสนทนาอื่นในละครนั้น[1] ในขณะที่บางคนสันนิษฐานว่าคำว่า Spam มาจากเนื้อกระป๋องที่ใช้รับประทานสำหรับอาหารมื้อกลางวัน ซึ่งส่วนใหญ่ประกอบไปด้วยเนื้อที่ทำเทียมขึ้นไม่ใช่เนื้อแท้ๆ[2] แต่บางคนกลับกล่าวว่า คำว่า Spam มาจากพฤติกรรมของผู้ที่เป็นสมาชิกชมรม MUSH (Multi User Shared Hallucination) ซึ่งมักจะพิมพ์ คำว่า S-P-A-M เพื่อทำให้ผู้ใช้รายอื่นไม่สามารถเข้าร่วมสนทนาออนไลน์ของกลุ่มได้[3]

## 2.3 ลักษณะ ประเภท และวิธีการส่งสแปมเมล

### 2.3.1 ลักษณะของสแปมเมล

สแปมเมลเป็นจดหมายที่ส่งออนไลน์โดยไม่จำกัดกลุ่มเป้าหมาย ซึ่งอาจเป็นการส่งจดหมายต่อๆ กันมาที่มีวัตถุประสงค์แตกต่างกัน แต่สแปมเมลที่มักจะก่อให้เกิดปัญหามากในขณะนี้ก็คือ จดหมายที่มีการโฆษณาสินค้าและบริการที่ไม่ชอบด้วยกฎหมาย มีเนื้อหาที่ขัดต่อศีลธรรมอันดี และมีข้อความที่มีลักษณะหลอกลวง โดยที่ผู้ส่งสแปมเมลมักจะใช้ชื่อผู้ส่งและที่อยู่ที่ไม่มีตัวตนจริง จากรายงานของ AC Neilsen.consult ระบุว่าประเภทของสแปมเมลที่นิยมส่งมากที่สุดคือ ภาพลามก(ร้อยละ 100) และโครงการหารายได้พิเศษจากบ้าน(ร้อยละ 97) และต้นทางของการส่งสแปมนั้นส่วนใหญ่มาจากประเทศสหรัฐอเมริกา นอกจากนี้ US Federal Trade Commission ยังระบุว่าร้อยละ 66 ของการส่งสแปมเมลนั้นมีลักษณะที่หลอกลวง นอกจากนี้คุณลักษณะพิเศษของสแปมเมลคือ การส่งที่ไม่ปรากฏชื่อผู้ส่ง (Anonymous) สามารถส่งได้โดยไม่เลือกเจาะจง (Indiscriminate) และสามารถส่งได้ทั่วโลก (Global) ที่สำคัญคือการส่งสแปมเมลนั้น ผู้ส่งไม่ต้องเสียค่าใช้จ่ายในการส่งเนื่องจากผู้รับเป็นผู้เสียค่าใช้จ่ายเพราะเป็นการส่งแบบ .Postage due ซึ่งแตกต่างจากกลยุทธ์การขายโดยวิธีอื่น เช่น direct mail ซึ่งผู้ส่งจะต้องชำระค่าธรรมเนียมการส่ง

### 2.3.2 ประเภทของสแปมเมล

1) Internal Spam คือ การส่งสแปมเมลที่มาจากภายในเครือข่ายเดียวกัน เช่น การส่งเรื่องตลกขบขัน เรื่องคอลัมน์นินทาต่างๆ ระหว่างเพื่อนร่วมงาน การส่งข่าวของลดราคา หรือจดหมายแจ้งข่าว เพื่อให้บุคลากรภายในองค์กรได้รับทราบ

2) External Spam คือ การส่งสแปมเมลที่มาจากภายนอกเครือข่าย แบ่งออกได้เป็น

---

[1] Gary S. Moorefield.(1999). **Note-SPAM It's not Just for breakfast Anymore Anymore: Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-Mail.** P.1

[2] Jennifer M. Kappel.(1999). **Note and Comments -Government Intervention on the Internet: Should the Federal Trade Commission Regulate Unsolicited E-mail Advertising.** P.5

[3] David E. Sorkin.(2001). **Technical and Legal Approaches to Unsolicited Electronic Mail.** P.3

2.1) จดหมายที่มีข้อความโฆษณาสินค้า การบริการต่างๆ และเว็บไซด์ภาพลามก (Commercial Message Advertising)

2.2) จดหมายลูกโซ่ (Chain Letters) โดยมีการขู่ว่าถ้าไม่ส่งต่อผู้รับจดหมายจะต้องเผชิญกับความหายนะ เช่น Chain Mail เป็นข้อความลูกโซ่ที่แสดงเนื้อหาคำเตือนเกี่ยวกับไวรัส หรือเรื่องอื่นใด โดยมีจุดมุ่งหมายเพื่อแพร่กระจายด้วยการส่งต่อ Chain Mail จะสร้างความเสียหายกับตัว Mail Server ของผู้ให้บริการอินเทอร์เน็ตทำให้ Server down หรือทำงานช้าลง ทำให้ traffic ของเครือข่ายอินเทอร์เน็ตติดขัด นอกจากนี้ยังก่อให้เกิดความรำคาญใจแก่ผู้ใช้บริการอีกด้วย

2.3) โครงการหารายได้เสริมแบบรวดเร็ว (Make Money Fast)

2.4) การหลอกว่ามีไวรัส (Virus Hoaxes)

2.5) บทความทางศาสนา (Religious Treatise)

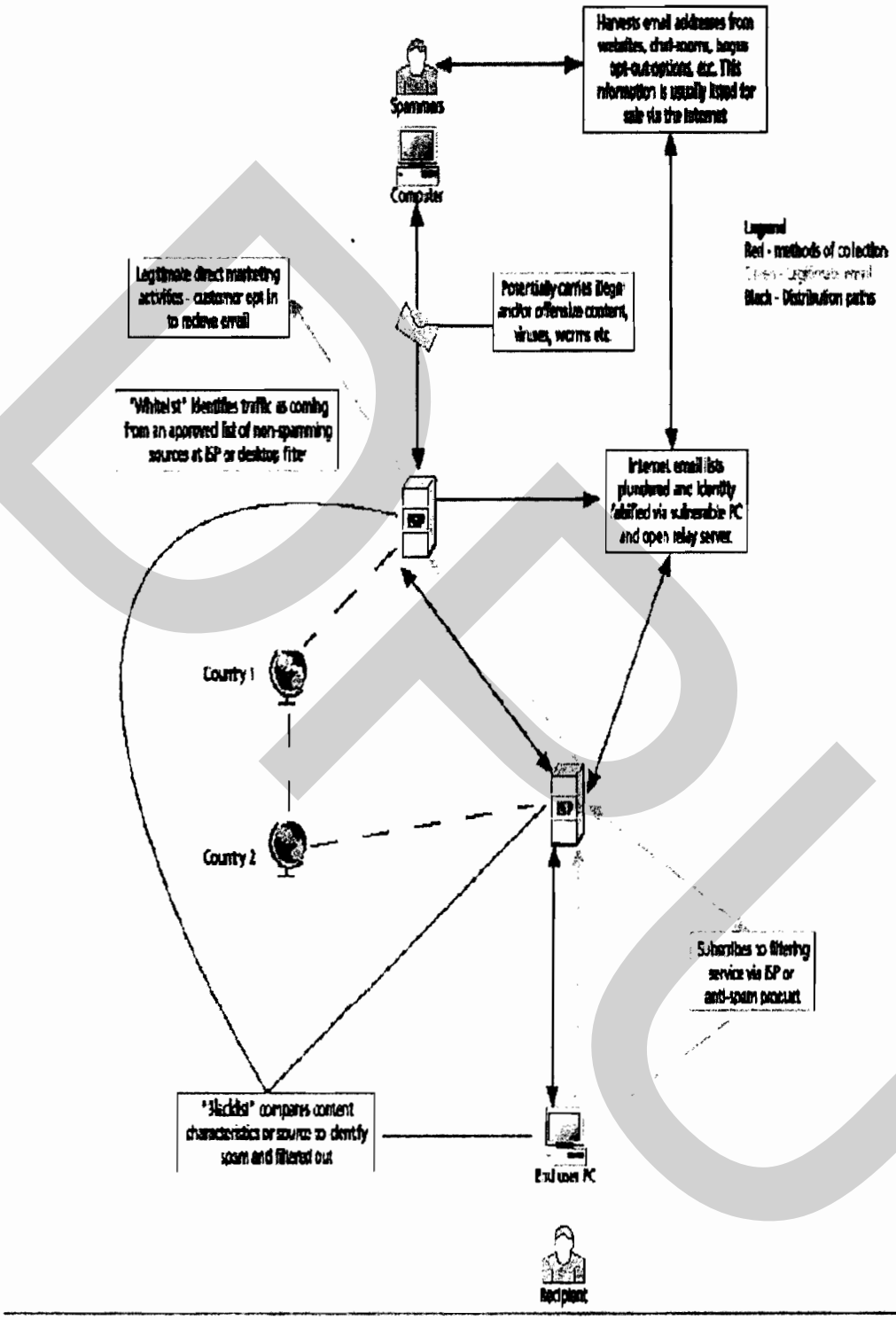
ทั้งนี้จดหมายลูกโซ่และการหลอกว่ามีไวรัสเป็นลักษณะที่พยายามให้ผู้รับทำการส่งต่อจดหมายไปยังผู้อื่นต่อไป

3) Usenet Spam คือ การส่งสแปมเมลไปยังกลุ่มข่าวยูสเน็ตแต่ละกลุ่มโดยมักจะส่งไปพร้อมๆ กับกลุ่มข่าวต่างๆ ที่ผู้ส่งสแปมเมลจะไม่อ่านอีกต่อไป ซึ่งมีผลทำให้กลุ่มข่าวนั้นไม่อาจที่จะจัดให้ข่าวนั้นสามารถติดตามข่าวได้อย่างเป็นระบบ

2.3.3 วิธีการส่งสแปมเมล

ขั้นตอนแรกของการส่งสแปมเมล คือ การหาชื่อและที่อยู่ของผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ โดยผู้ส่งสแปมเมลมักจะได้ชื่อและที่อยู่ของผู้รับด้วยการค้นหาอัตโนมัติ (จากเว็บเพจ กระดานข่าว หรือจากรายชื่อผู้ใช้บริการอินเทอร์เน็ต) โดยการซื้อมาจากนายหน้ารายชื่อผู้ใช้บริการจดหมายอิเล็กทรอนิกส์

ขั้นตอนถัดมา คือ ผู้ส่งสแปมมักจะหาโปรแกรมที่ใช้เพื่อช่วยกระจายการส่งสแปมเมล ซึ่งโดยส่วนมากจะเป็นโปรแกรมที่ไม่ต้องเสียเงิน เช่น Freeware และ/หรือ Shareware Program โปรแกรมเหล่านี้สามารถส่งได้ครั้งละไม่เกิน 20,000 ข้อความต่อชั่วโมงและขั้นตอนสุดท้าย คือ การหาระบบส่งสแปมเมล ซึ่งวิธีที่ผู้ส่งมักจะใช้กันเป็นส่วนใหญ่คือ การสมัครเป็นสมาชิกกับ ISP ของบริษัทใดก็ได้ที่ให้บริการทดลองใช้ฟรีโดยไม่เสียค่าใช้จ่าย เช่น AOL ให้ทดลองใช้ฟรี 50 ชั่วโมง โดยบัญชีของสมาชิกทดลองใช้งานจะถูกลบทิ้งภายหลังจากระยะเวลาการทดลองใช้งานสิ้นสุดลง ซึ่งระบบนี้ทำให้ผู้ส่งสแปมเมลมั่นใจว่าผู้รับจะไม่สามารถติดต่อกลับมายังผู้ส่งได้




ภาพที่ 2.2 วิธีการส่งสแปมเมล

## 2.4 ตัวอย่างของสแปมเมลในตู้ไปรษณีย์อิเล็กทรอนิกส์

| | | | |
|---|---|---|---|
| Alva gene | Anna Kournikova Topless | May 27 | 6k |
| FunPageLand | *** A Rose For A Rose *** | May 27 | 3k |
| Driver | Learn How to Get Paid to Drive your car | May 27 | 4k |
| shawnda Oshinsky | Your Casino Winnings | May 27 | 4k |
| FlowGo Fun Flash | A Little Valentine's Puss <--New Flowgo Fun | May 27 | 4k |
| Eat to Lose | Eat your way Thinner in 10 days Guaranteed! | May 28 | 2k |
| Marni Crofutt | Hot casino offers for you | May 28 | 4k |
| debt-man NjExOQ | Let us help you get out of debt | May 28 | 4k |
| ernest Arboleda | Find a longer long-term creation today | May 28 | 2k |
| Int'l Wine Cellars | Get 3 Bottles of Wine FREE + a $29.95 Corkscr... | May 29 | 14k |
| FlipPhone | Motorola i60 Flip Phone, With Direct Connect,... | May 29 | 6k |
| Coleman Marv | Coleman Marv | May 29 | 3k |
| Sean Francis | Sean Francis | May 29 | 3k |
| Dollar Store | Own a Dollar Store for less than a dollar a d... | May 29 | 2k |
| Coffee Lovers | Taste the Difference. Try Gevalia - Get a FRE... | May 30 | 16k |
| BMW Offer from Diqit... | Prize Entry for 2 BMW Mini Coopers #968895435 | May 30 | 7k |
| Its Natural | Increase bust size naturally... Guaranteed | May 30 | 3k |
| cupids arrow MDExOQ | Web to door flower delivery to your valentine | May 30 | 5k |
| FunPageLand | *** I Love You (in 8 languages) and Lots More... | May 31 | 3k |
| SmilePop | Shed a tear for fallen heroes | May 31 | 8k |
| Needahug@funstun.com | Warm your HEART with the best fun all week! | May 31 | 4k |
| FlowGo Fun Flash | Prickly Lovin'<-- New Valentine's Flowgo Fun | May 31 | 4k |
| "Royal" brokins dfps... | Hot casino offers for you | May 31 | 5k |

ภาพที่ 2.3 ตัวอย่างของสแปมเมลในตู้ไปรษณีย์อิเล็กทรอนิกส์

## 2.5 ผลกระทบจากสแปมเมล

2.5.1 ค่าใช้จ่ายจากการส่งสแปมเมล (Cost)

ตามที่ได้กล่าวมาแล้วว่าในการส่งสแปมเมลนั้น ผู้ส่งสแปมเมลเสียค่าใช้จ่ายน้อยมาก เมื่อเปรียบเทียบกับการส่ง Junk Mail ทั่วไป เนื่องจากการส่งนั้นมีลักษณะที่ผลักภาระค่าใช้จ่ายมายังผู้ให้บริการอินเทอร์เน็ตและผู้ใช้อินเทอร์เน็ต (Cost Shifting to ISP Costs and Consumer Costs) ได้แก่ ค่าใช้จ่ายในการดาวน์โหลด (Download cost) ปัญหาเรื่องเนื้อที่ของการใช้ดิสก์ (Disk space) รวมถึงการเสียเวลาของลูกจ้างในการจัดการกับสแปมเมล (Employee time wasted)

ในแง่ของผู้ใช้อินเทอร์เน็ตในฐานะผู้บริโภคนั้น จะเห็นได้ว่าผู้ใช้จะต้องเสียเวลา เพื่อลบสแปมออกจากตู้ไปรษณีย์อิเล็กทรอนิกส์ (Mailbox)ของตน ซึ่งถ้าหากเป็นกรณีที่ผู้ใช้อินเทอร์เน็ตไม่ได้เหมาจ่ายค่าธรรมเนียมการใช้อินเทอร์เน็ต ซึ่งอาจจ่ายจากการคำนวณตามเวลาของการใช้งาน การลบสแปมเมลทำให้เสียเวลามากและกินเวลาการใช้อินเทอร์เน็ต อันมีผลทำให้ผู้ใช้อินเทอร์เน็ตต้องเสียค่าธรรมเนียมการใช้อินเทอร์เน็ตเพิ่มขึ้น หรือไม่เช่นนั้นผู้ใช้อินเทอร์เน็ตก็

ต้องเสียค่าใช้จ่ายเพิ่มจากการซื้อเนื้อที่ในการรับและส่งจดหมายเพิ่มขึ้น ถ้าหากตนไม่ต้องการเสียเวลาในการแยกจดหมายของตนออกจากสแปม

สำหรับผู้ให้บริการอินเทอร์เน็ต (ISP)นั้น ต้องเสียค่าใช้จ่ายในการจ้างพนักงานเพิ่มขึ้นเพื่อคัดสแปมเมลออกจากระบบ นอกจากนี้ (ISP)นั้นยังจะต้องขยายความกว้างของช่องสัญญาณ (Bandwidth) เพื่อรักษาระดับความเร็วของระบบและค่าใช้จ่ายในการเพิ่มระบบกลั่นกรองสแปมเมลเพื่อรักษาลูกค้าของตนเองไว้

2.5.2 ความเป็นส่วนตัว (Privacy)

การรวบรวมชื่อและที่อยู่ผู้ใช้ไปรษณีย์อิเล็กทรอนิกส์ของผู้ส่งสแปม เพื่อใช้ในการส่งสแปมเมล โดยผู้เป็นเจ้าของชื่อและที่อยู่นั้นไม่ทราบและไม่ได้ให้ความยินยอม ถือเป็นการละเมิดความเป็นส่วนตัว

2.5.3 การหลอกลวงโดยส่งจดหมายซึ่งใช้ที่อยู่หรือหัวเรื่องของไปรษณีย์อิเล็กทรอนิกส์ปลอม (Spoofing)

การส่งจดหมายโดยใช้ที่อยู่หรือหัวเรื่องของไปรษณีย์อิเล็กทรอนิกส์ปลอม ซึ่งบางครั้งก็ใช้ชื่อและที่อยู่ของหน่วยงานที่มีชื่อเสียง เพื่อที่จะหลอกให้ผู้รับเกิดความสนใจและเปิดอ่านจดหมายของตน หรือตอบกลับ

2.5.4 เนื้อหาของจดหมายที่มีลักษณะหลอกลวงและขัดต่อกฎหมายและศีลธรรมอันดี (Content – Fraudlent & Deceptive Advertising)

นอกจากนี้การโฆษณาสินค้าของสแปมส่วนใหญ่มีลักษณะฉ้อฉล เช่น โฆษณาว่ามีการแจกสินค้าฟรี หากส่งจดหมายนี้ต่อไปยังคนรู้จักอย่างน้อย 20 คน หรือมีการโฆษณาที่มีเนื้อหาขัดต่อกฎหมายหรือศีลธรรมอันดี เช่น การโฆษณาเว็บไซต์ภาพลามก การพนัน เป็นต้น

2.5.5 การบุกรุก (Trespass)

มีการโต้แย้งกันว่าการส่งสแปมเมลถือเป็นการบุกรุกสังหาริมทรัพย์ของผู้รับสแปมเมล แม้ว่าสแปมจะให้สิทธิผู้รับในการเลือกยกเลิกมิให้มีการส่งสแปม (A Remove from List) แต่การกระทำดังกล่าวไม่ได้ผล เนื่องจากการกระทำดังกล่าวเป็นการยืนยันให้กับผู้ส่งสแปมเมลว่าชื่อและที่อยู่ดังกล่าวนั้นมีอยู่จริง โดยผู้ส่งสแปมจะนำชื่อและที่อยู่ดังกล่าวไปสร้าง List ใหม่เพื่อทำการส่งสแปมต่อๆ ไป

**2.6 ความพยายามในการแก้ปัญหาสแปมเมล**

2.6.1 ความพยายามเบื้องต้น (Informal Approaches)

เป็นการสร้างมารยาททางสังคมของการใช้อินเทอร์เน็ต รวมทั้งการทำข้อตกลงและการออกกฎเกณฑ์ หรือหลักจริยธรรมระหว่างกันในอุตสาหกรรมอินเทอร์เน็ตเพื่อควบคุมกันเอง เช่น Hotmail ซึ่งให้บริการไปรษณีย์อิเล็กทรอนิกส์ฟรีได้ออกนโยบายห้ามส่งสแปมเมล หรือนโยบายของ ISP ทั้งหลายที่ได้ประกาศไว้อย่างชัดเจนห้ามมิให้มีการส่งสแปมเมล อย่างไรก็ตามนโยบายดังกล่าวแทบไม่ส่งผลอะไรกับผู้ส่งสแปมเมลเลย เนื่องจากข้อตกลงหรือนโยบายที่ออกมานั้น ขาดประสิทธิภาพในการใช้บังคับได้จริงกับผู้ที่ฝ่าฝืน

2.6.2 ความพยายามทางเทคนิค ( Technical Approaches )

เป็นการใช้โปรแกรมของผู้ใช้อินเทอร์เน็ตเอง ผู้ให้บริการอินเทอร์เน็ต หรือผู้ควบคุมระบบปลายทาง เพื่อกลั่นกรองและป้องกันสแปมเมลที่จะถูกส่งเข้ามา (Filtering and Blocking) ซึ่งโปรแกรมเหล่านี้มีมากมาย เช่น โปรแกรม Brightmail, ORDB, Spambam, Spamtrap, Spamcop, Spamkiller, Surfcontrol เป็นต้น

<u>อัลกอริทึมสำหรับการกรองสแปม</u>[1] ในอดีต – ปัจจุบัน

1) Bogoflter

เป็น Open source spam filter ใช้เทคนิคการตรวจจับด้วยวิธีการ Naïve Bayesisn (NB) และการเทียบคำที่กำหนดไว้(Keyword Matching) เพื่อแยกข้อความ Spam ออกจากข้อความทั่วไป โดยคำนึงถึงบริเวณที่มีการเทียบ เช่น ความหมายของคำว่า " platypus " ที่อยู่ส่วนของ Subject กับที่อยู่ใน from จะมีคุณลักษณะในการเปรียบเทียบต่างกัน

2) OSBF-Lua

เป็น Open source spam filter ที่พัฒนาขึ้นจากภาษา C ชนิดหนึ่ง (ภาษา C แบบLua)ที่ใช้เทคนิค orthogonal sparse bi-grams[2] ซึ่งเป็นวิธีการตรวจจับของ e-Mail โดยเน้นที่การทำงานแบบ pairs of collocated words

3) DMC (Dynamic Markov Compression)

เน้นการประมวลผลกับข้อมูลที่ถูกบีบอัด โดยใช้หลักการพิจารณาข้อความเป็น String เพื่อตรวจสอบและทำนายว่าข้อความนั้นจัดเป็นข้อความ Spam หรือไม่

---

[1] Gordon V. Cormack, Jose Maria Gomez Hidalgo and Enrique Puertas Sanz. (2007). **Spam filtering for short messages**. P.1-8.

Fidelis Assis. (2006). **OSBF-Lua, Text classification module for the Lua Programming Language and a production class anti-spam in Lua using the module.** P. 1.

4) LR (Logistic Regression)

เป็น Open source spam filter ที่ใช้หลักการคำนวณทางตรรกศาสตร์เพื่อหาค่าสัมประสิทธิ์ของฟังก์ชั่นเชิงเส้นแล้วพิจารณาความเป็นไปได้ที่จะเป็นข้อความ Spam คล้ายกับSVM แต่มีระดับการคำนวณต่ำกว่า

5) SVM (Support Vector Machine)

ค้นหาข้อความ Spam ด้วยหลักการหาสัมประสิทธิ์ของฟังก์ชั่นเชิงเส้น เพื่อแยกข้อความ Spam ด้วยระยะห่างบนกราฟ และมีคุณลักษณะในการตรวจสอบข้อมูล Alphanumeric characters อีกด้วย ซึ่งให้ผลการกรองได้ดีที่สุดในการทดสอบ

6) LOHIT Algorithm

LOHIT Filter[1] สำหรับกรองข้อความ Spam ใช้สมการคณิตศาสตร์ เพื่อระบุความน่าจะเป็นของข้อความ Spam และทำการจำลองการส่งข้อมูล เพื่อทดสอบประสิทธิภาพโดยแสดงผลออกมาในรูป 3D subspace

7) Rule Base

เป็นวิธีการตรวจจับข้อความด้วยกฎและเงื่อนไขการใช้ Keywords Matching ความซับซ้อนในการคำนวณทางคณิตศาสตร์สามารถทำงานได้รวดเร็ว แต่มีความถูกต้องน้อยกว่าวิธีอื่น ถูกนำมาใช้ในการกรองข้อความ SMS ในรูปแบบของ Software ขนาดเล็กที่ติดตั้งบนโทรศัพท์เคลื่อนที่[2] การทำงานของวิธีการนี้ผู้ใช้งานต้องเป็นผู้กำหนดกฎและเงื่อนไขขึ้น เพื่อให้สามารถกรองข้อความได้ถูกต้อง เช่น

การใช้กฎ Black/white list ซึ่งจะตรวจสอบผู้ส่งข้อความว่าได้รับอนุญาตหรือไม่

การใช้ Keywords Matching ที่จะตรวจสอบคำในข้อความหากพบคำที่ผู้ใช้งานกำหนดให้เป็นข้อความ Spam จะดำเนินการคัดแยก

8) TFIDF[3]

เป็นวิธีการค้นหาลักษณะเด่นของเอกสาร(Document)ให้อยู่ในรูปของกลุ่มข้อมูล (Feature Vector) โดยอ้างอิงจากชุดตัวอักษรหรือคำ(Term)ในเอกสาร และจำนวนเอกสารทั้งหมดที่ถูกกำหนดให้เป็นข้อมูลฝึกสอน ดังสมการต่อไปนี้

$$TFIDF(i, j) = TF(i, j)\, IDF(i) \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

---

S. Dixit, S. Gupta, and C.V. Ravishankar. (2005). **LOHIT: An Online Detection & Control System for Cellular SMS Spam.** P. 1.

WebGate JSC (2007). **SMS Spam Manager**. P 1

อดิชาต ขานทอง, วัลลภา ตันติประสงค์ชัย และ ชุลีรัตน์ จรัสกุลชัย. (2544). **Document Summarization.** หน้า 4-6.

$$IDF(i) = \frac{\log N}{DF(i)} \quad \text{.....(2)}$$

TF คือ ความถี่ของ Term นี้ที่ปรากฏใน Document

DF คือ ความถี่ของ Document m มี Term นี้

IDF คือ ค่าแทน Discrimination power ของ DF

ในการจัดกลุ่มเอกสารหรือการกรองข้อความแบบต่างๆ ที่ใช้การคำนวณทางคณิตศาสตร์ จะใช้วิธีการ TFIDF ในการแปลงเอกสารที่ต้องการนำไปคำนวณ ให้เป็นชุดข้อมูล เพื่อนำไปคำนวณต่อไป

9) Text Normalization[1]

เป็นวิธีลบสัญลักษณ์พิเศษ เช่น $ # @ ? ! หรือตัวเลขที่ไม่ต้องการ เพื่อกำจัดข้อมูลส่วนเกินออก ใช้ในการประมวลผลข้อมูลที่อยู่ในรูปแบบ text หรือ string เมื่อต้องการนำข้อมูลเหล่านั้นไปคำนวณค่า

2.6.3 ความพยายามทางกฎหมาย (Legal Approaches)

1) ตัวอย่างคดีเกี่ยวกับสแปมเมล

ในสหรัฐอเมริกาได้มีการฟ้องร้องคดีเกี่ยวกับสแปมเมลหลายคดี เช่น American Online (AOL) ซึ่งเป็น ISP ที่ใหญ่ที่สุดในสหรัฐอเมริกาได้ยื่นฟ้องคดีเกี่ยวกับสแปมเมลกว่า 100 บริษัท โดย AOL ชนะคดีถึง 25 คดี และคดีล่าสุดของ AOL คือ คดี AOL v. CN Production ซึ่งศาลได้พิพากษาให้จำเลย (CN Production) จ่ายค่าเสียหายจากการส่งสแปมเมลให้กับโจทก์ (AOL) เป็นเงิน 6.9 ล้านเหรียญสหรัฐ ฯ

นอกจากนี้ในเดือน พ.ค. Earthlink ซึ่งเป็น ISP อันดับ 3 ของสหรัฐได้ชนะคดีเกี่ยวกับสแปมเมลโดยศาลได้พิพากษาให้จำเลย (Carmack) จ่ายค่าเสียหายจากการส่งสแปมเมลให้กับโจทก์ (Earthlink) เป็นเงินถึง 16.5 ล้านเหรียญสหรัฐฯ

2) แนวคิดในการออกมาตรการทางกฎหมายเพื่อแก้ไขปัญหาสแปมเมล

เนื่องจากความพยายามที่จะต่อสู้ เพื่อป้องกันการส่งสแปมเมลข้างต้นนั้นไม่ประสบความสำเร็จเพราะค่าใช้จ่ายในการส่งสแปมเมลนั้นต่ำมาก เมื่อเทียบกับการส่ง Junk Mail ในรูปของแผ่นกระดาษ อีกทั้งการดำเนินคดีทางกฎหมายก็ยังไม่มีความชัดเจน เนื่องจากยังไม่มีกฎหมายมาควบคุมสแปมโดยเฉพาะ ดังนั้นจึงมีแนวความคิดที่จะออกมาตรการทางกฎหมายเพื่อเป็นแนวทางในการแก้ปัญหาของการส่งสแปมเมล โดยความพยายามดังกล่าวได้เกิดขึ้นในหลายประเทศ เช่น

---

[1] István Pilászy. (2005). **Text Categorization and Support Vector Machines.** P. 2 – 3.

2.1) สหรัฐอเมริกา

สภาคองเกรสของสหรัฐ ฯ ได้มีความพยายามหลายครั้งในการร่างกฎหมายออกมา เพื่อแก้ไขและควบคุมปัญหาเกี่ยวกับสแปมที่ดูจะรุนแรงขึ้นอย่างต่อเนื่อง อย่างไรก็ตามความพยายามดังกล่าว ดูเหมือนจะยังไม่ประสบความสำเร็จ เพราะในขณะนี้สหรัฐอเมริกาก็ยังไม่มีกฎหมายเฉพาะออกมาควบคุมปัญหาสแปมเมล ร่างกฎหมายที่ได้มีการนำเสนอ และไม่ผ่านสภามีดังต่อไปนี้

2.1.1) สมัยประชุมที่ 106 (ร่างพระราชบัญญัติที่เสนอทั้งหมดไม่ผ่านสภา)

1) Unsolicited Electronic Mail Act of 2000 (H.R. 3113)

2) Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000 (S.2542)

3) Can Spam Act (H.R.2162)

4) e-Mail User Protection Act (H.R.1910)

5) Inbox Privacy Act of 1999 (S.759)

6) Internet Freedom Act (H.R.1686)

7) Internet Growth and Development Act of 1999 (H.R.1685)

8) Netizens Protection Act of 1999 (H.R.3024)

9) Protection against Scams on Seniors Act of 1999 (H.R.612) and Telemarketing Fraud and Seniors Protection Act (S.699)

10) Wireless Telephone Spam Protection Act (H.R.5300)

2.1.2) สมัยประชุมที่ 107 (ร่างพระราชบัญญัติที่เสนอทั้งหมดไม่ผ่านสภา)

1) Anti-Spamming Act of 2001 (H.R. 718)

2) Anti-Spamming Act of 2001 (H.R. 1017)

3) Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2001/2002 (S. 603)

4) Netizens Potection Act of 2001 (H.R. 3146)

5) Protect Children From E-Mail Smut Act of 2001(H.R. 2472)

6) Who Is E-Mailing Our Kids Act (H.R. 1846)

7) Unsolicited Electronic Mail Act of 2001 (H.R. 95)

8) Wireless Telephone Spam Protection Act (H.R. 113)

2.1.3) สมัยประชุมที่108 (ร่างพระราชบัญญัติทั้งหมดกำลังอยู่ในระหว่างการพิจารณาของสภา)

1) CAN-SPAM Act of 2003 (S. 877)

2) Computer Owners' Bill of Rights (S. 563)

3) Reduce Spam Act of 2003 (H.R. 1933)

4) Wireless Telephone Spam Protection Act (H.R. 122)

จากร่างกฎหมายข้างต้นสามารถสรุปได้ว่าเนื้อหาของร่างพระราชบัญญัติที่เสนอมามักจะมีแนวทางใหญ่ๆ ที่คล้ายกันกล่าวคือ การใช้ชื่อและที่อยู่ของผู้ส่งที่ไม่เป็นจริงถือว่าผิดกฎหมายการส่งสแปมเมลต้องแจ้งให้ผู้รับทราบว่าจดหมายที่ส่งนั้นเป็นสแปมเมล ต้องปฏิบัติตามนโยบายของ ISP โดยเคร่งครัดรวมทั้งการจัดให้สิทธิของผู้รับสแปมเมลเลือกที่จะปฏิเสธไม่รับสแปมต่อไปในอนาคต (Opt-out)

2.2) สหภาพยุโรป

1) E-Privacy Directive 2002/58/EC

2) E-Commerce Directive 2000/31/EC

3) Telecommunications Privacy Directive 97/66/EC

4) Distance Contract Directive 97/7/EC

5) Data Protection Directive 95/46/EC

กฎหมายยุโรปค่อนข้างชัดเจนในแง่ของการส่งสแปม โดยเฉพาะบทบัญญัติของมาตรา 13 ว่าด้วยเรื่อง Unsolicited Communications ของ e-Privacy Directive 2002/58/EC ว่าการส่งสแปมจะทำไม่ได้หากไม่ได้รับความยินยอมจากผู้รับเสียก่อน (Opt-in) นอกจากนี้ยังห้ามปกปิดการใช้ชื่อและที่อยู่ของผู้ส่งในการส่งไปรษณีย์อิเล็กทรอนิกส์

**2.7 ข้อโต้แย้งของผู้ส่งสแปม (Spammer) กับแนวคิดที่จะควบคุมสแปมเมล**

สมาคมการตลาดทางตรงของสหรัฐฯ (Direct Marketing Association-DMA) โต้แย้งว่าสแปมเป็นเครื่องมืออย่างหนึ่งของการตลาดทางตรง ดังนั้นทางสมาคมจึงไม่เห็นด้วยกับการออกกฎหมายห้ามมิให้มีการส่งสแปมเมล นอกจากนี้ผู้ส่งสแปมเมลกล่าวอ้างว่า " บุคคลย่อมมีเสรีภาพในการพูด (Free Speech) ภายใต้รัฐธรรมนูญ " ในขณะที่ฝ่ายต่อต้านสแปมเมลอ้างว่า " บุคคลย่อมมีสิทธิในการหลีกเลี่ยงรับฟังการพูดที่มีลักษณะเป็นการคุกคามตน (Right to avoid Harmful Speech) " โดยอ้างคำตัดสินของคดี Rowan v. United States Post Office Department ว่า " รัฐธรรมนูญไม่ได้บังคับให้บุคคลต้องรับฟังหรือชมการสื่อสารใดๆ ที่ตนไม่ประสงค์ไม่ว่าสิ่งนั้นจะควรค่าแก่การรับฟังและชมหรือไม่ก็ตาม "

## 2.8 ประเทศไทยกับแนวทางการแก้ไขปัญหาสแปมในอนาคต

ถึงแม้ว่าปัญหาของสแปมเมลจะยังไม่รุนแรงเท่ากับในต่างประเทศ แต่การส่งสแปมเมลก็ก่อให้เกิดปัญหาต่อผู้ใช้อีเมลในหลายประเด็นดังที่ได้กล่าวมาแล้ว จากรายงานของผู้ให้บริการอินเทอร์เน็ต(ISP) ของไทยทั้ง 18 รายระบุว่าทุกวันนี้ ISP เสียเนื้อที่ให้กับสแปมเมลอย่างน้อยวันละ 18 กิกะไบต์[1]

ด้านกฎหมายไทยประเทศไทยได้ให้ความสำคัญในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจเป็นช่องว่างที่ผู้ก่อการร้ายจะแสวงประโยชน์จากช่องทางนี้ จึงได้มีการออก " ร่างพระราชบัญญัติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ พ.ศ.2544 " แต่กฎหมายดังกล่าวไม่ได้ครอบคลุมในเรื่องของสแปมเมล ทำให้ยังไม่มีกฎหมายที่สามารถนำมาปรับใช้กับสแปมเมลได้ชัดเจน ดังนั้นการส่งสแปมเมลจึงยังไม่เข้าข่ายความผิดตามกฎหมายที่มีอยู่ ในปัจจุบันประเทศไทยได้ออกพระราชบัญญัติ" ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 "และกำลังร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งคาดว่าจะครอบคลุมปัญหาเหล่าทั้งหมด

ตัวอย่างบทลงโทษผู้กระทำผิด

" มาตรา 11[2] ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท "

## 2.9 ระบบไปรษณีย์อิเล็กทรอนิกส์[3]

ระบบไปรษณีย์อิเล็กทรอนิกส์ในอินเทอร์เน็ต ระบบจะประกอบด้วย 3 ส่วนหลักคือ Mail Server, User Agent และ Simple Mail Transfer Protocol (SMTP) โดยใช้ User Agent ทำหน้าที่เชื่อมต่อกับผู้ใช้ในการอ่านและตอบจดหมายผ่านระบบไปรษณีย์อิเล็กทรอนิกส์ Mail Server จะใช้ในการจัดเก็บและบริหารจัดการตู้ไปรษณีย์อิเล็กทรอนิกส์ของผู้ใช้แต่ละคนโดยส่วน Simple Mail Transfer Protocol (SMTP) ซึ่งเป็นโพรโทคอลในชั้นแอพพลิเคชั่นสำหรับโอนถ่ายจดหมายอิเล็กทรอนิกส์ของผู้รับผ่านเครือข่ายอินเทอร์เน็ต

---

[1] อรรยา สิงห์สงบ , (2546). **ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเล็กทรอนิกส์ขยะ**.หน้า 9-10.

[2] สำนักงานปลัดกระทรวง.(2550).**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550**. หน้า 6.

[3] James F. Kurose and Keith W.Ross.(2003). **Computer Networking : A Top-Down Approach Featuring the Internet. 2nd ed : Pearson Addison-Wesley.** P.6

**2.10 Mail Server**[1]

คือ เครื่องบริการรับ – ส่งจดหมายสำหรับสมาชิกบริการที่มีให้ใช้เช่น รับ – ส่งจดหมายทั้งแบบที่เป็นข้อความและรูปภาพ โดยส่งในรูปแบบ Attach file และมีที่เก็บข้อมูลผู้ติดต่อ เรียกว่า Address book เป็นต้น ตัวอย่าง Mail Server ที่รู้จักกันทั่วไป เช่น Hotmail.com หรือ Thaimail.com เป็นต้น

SMTP server คือ Simple Mail Transfer Protocol Server หมายถึง เครื่องบริการส่ง e-Mail ไปยังเครื่องบริการอื่นๆ สำหรับ SMTP ส่วนใหญ่จะไม่ยอมให้คนนอกองค์กรหรือ IP ที่อยู่นอกองค์กรใช้งาน SMTP เพราะอาจมีคนในโลกใบนี้มาแอบใช้ทำให้บริการ SMTP ทำงานหนักให้กับคนภายนอกโดยไม่เกิดประโยชน์ใดๆ หากเครื่องคอมพิวเตอร์ที่เปิดให้บริการ SMTP แก่คนนอกแสดงว่าไม่ได้กำหนด Reply ไว้ เพราะคนทั่วโลกอาจใช้เครื่องมือค้นหาOpen Reply แล้วพบว่าเครื่องคอมพิวเตอร์ที่เปิดให้บริการเป็นเครื่องหนึ่งไม่ได้ทำ Reply ไว้ก็ได้ และที่อันตรายคืออาจมีคนบางคนใช้โปรแกรม MOBI+ กำหนดให้เครื่องคอมพิวเตอร์ที่เปิดให้บริการ SMTP เป็น Bomb Mail ไปยัง Mail Box ของเป้าหมาย และหมายเลขเครื่องที่โจมตีก็คือ เครื่อง SMTP ที่เปิดให้บริการนั่นเอง

POP server คือ Post Ofice Protocal Server คือ บริการรับ – ส่งอีเมลจาก Mail Server กับเครื่องสมาชิกบริการนี้ทำให้สามารถอ่าน Mail ด้วยมือถือ หรือ PDA แต่ถ้าท่านใช้ Mail ของ Thaimail.com จะเป็น Web-based mail ที่เปิดอ่าน e-Mail ได้จาก web เท่านั่น จะเปิดด้วย Outlook หรือ PDA ไม่ได้

**2.11 งานวิจัยที่เกี่ยวข้อง**

2.11.1 การกรองสแปมเมลด้วยระบบ Whitelist[2] ลักษณะการทำงานตรงข้ามกับแบบ Blacklist กล่าวคือเมื่อมีอีเมลส่งเข้ามาก็จะทำการตรวจสอบเบอร์อีเมลของผู้ส่งกับรายการในบัญชี Whitelist หากไม่ปรากฏเบอร์อีเมลผู้ส่งในรายการบัญชีก็แสดงว่าอีเมลนั้นเป็นสแปม ให้ทำการลบทิ้งหรือคัดแยกไปไว้ในตู้สแปม เป็นต้น

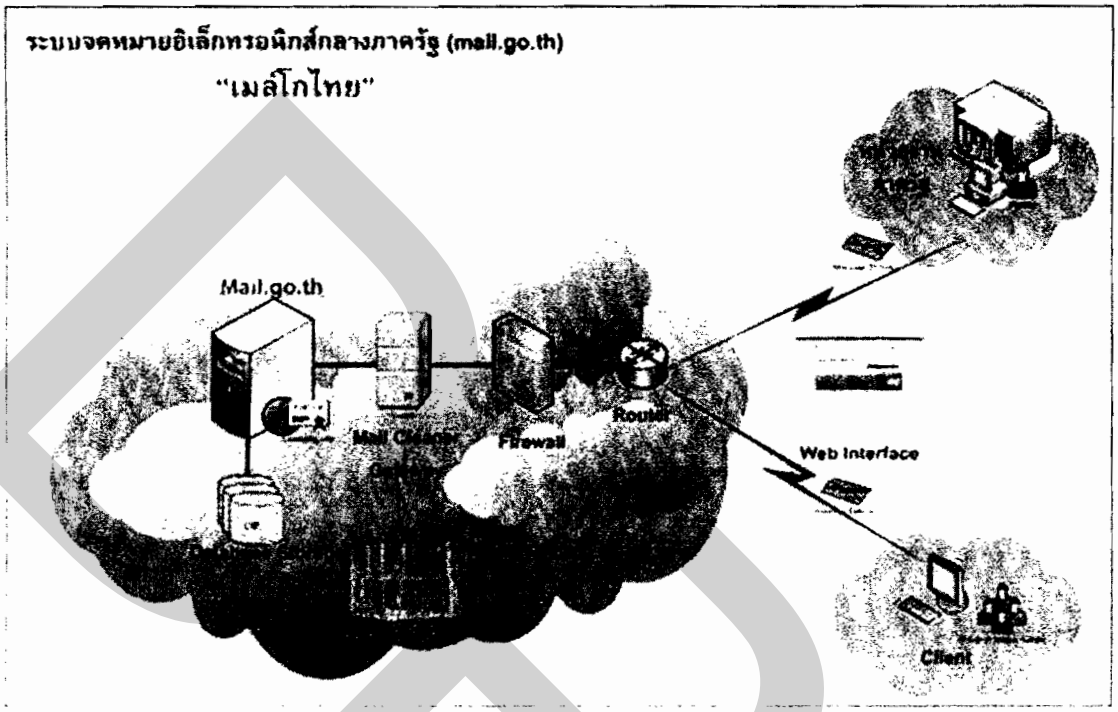
ข้อเสียของระบบนี้คือ มีข้อผิดพลาดสูงเนื่องจากผู้ที่มาติดต่อธุรกิจรายใหม่ อาจจะไม่มีรายชื่ออยู่ในบัญชี Whitelist ทำให้องค์กรหรือหน่วยงานพลาดโอกาสทางธุรกิจ

---

[1] ยุทธนา ชื่นจิตร.(2548). **ระบบการส่งอีเมลตอบกลับ.** หน้า 56.

[2] บริษัท เวิลด์ ไซเบอร์ เซอร์วิส จำกัด.(2009). **Anti Spam ระบบป้องกันอีเมลขยะ.** หน้า 1-3.

2.11.2 ระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ " เมล์โกไทย "[1]




ภาพที่ 2.4 หลักการทำงานระบบเมล์ของ สบทร.

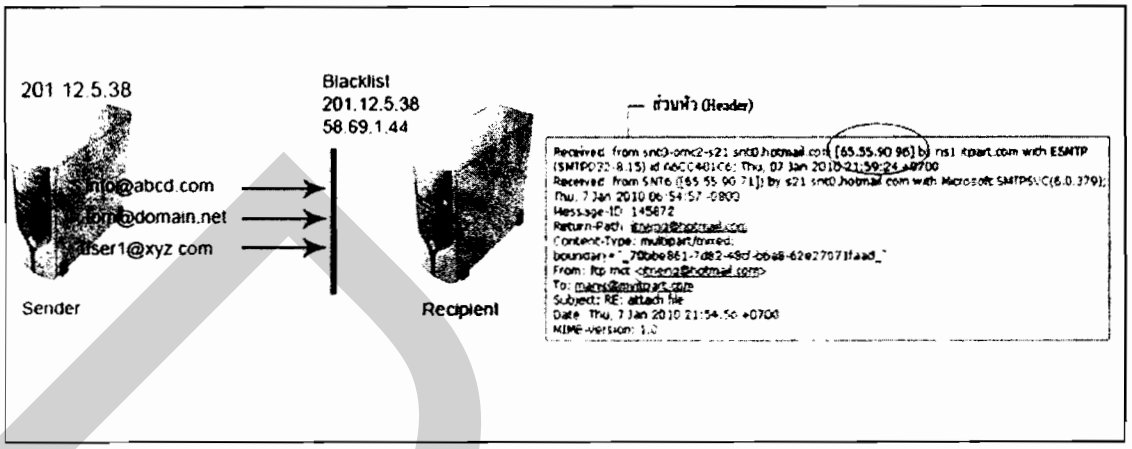
ภาพที่ 2.4 การทำงานระบบเมล์ของ สบทร. การติดตั้งตัวกรองสแปม(โปรแกรม Mail Cleaner) จะติดตั้งตัวกรองที่ Server ของผู้ให้บริการ โดยกรองจดหมายขยะของผู้ใช้ ด้วยวิธีการเพิ่มข้อความ "[SPAM?]" ลงบนหัวจดหมาย จากนั้นก็ใช้ความสามารถของโปรแกรมอ่านอีเมลในการแยกจดหมายขยะ ที่มีคำว่า "[SPAM?]" ออกจากเมล์ปกติ

2.11.3 การกรองสแปมเมลด้วยระบบ Blacklist[2] เป็นระบบพื้นฐานที่นิยมใช้ทั่วไป ทำโดยการเก็บไอพีของเครื่องเซิร์ฟเวอร์ที่ส่งสแปมไว้ในฐานข้อมูล เพื่อทำการสกัดกั้นเมล์ที่ส่งมาจากเครื่องดังกล่าว จากงานวิจัยการกรองสแปมจากบอทเน็ต พบว่าการวิเคราะห์เฮดเดอร์ของอีเมลด้วยระบบ Blacklist ปรากฏว่ามีจดหมาย 235 ฉบับต่อวัน แต่ใช้งานจริงเพียง 1-3 ฉบับเท่านั้น หลังจากการกรองสามารถลดปริมาณสแปมได้ ร้อยละ 96.23

---

[1] สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ.(2550).**โครงการระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ**.หน้า1-5.

[2] กอบเกียรติ สระอุบล และ เบญจพร ลิ้มธรรมาภรณ์ .(2552) **การกรองสแปมบอทเน็ต.** กรุงเทพ : มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ.




ภาพที่ 2.5 หลักการทำงานระบบ Blacklist

2.11.4 การกรองสแปมเมลด้วยระบบเก็บเป็นลายเซ็น Signature[1] โดยนำข้อความอีเมลผ่านฟังก์ชั่น Hash แล้วเก็บไว้เป็นข้อมูลลายเซ็นอีเมล ซึ่งเรียกว่า Signature อีเมลที่เป็นสแปมจะถูกบันทึกลายเซ็นเก็บไว้ในฐานข้อมูล เพื่อทำการเปรียบเทียบกับอีเมลที่เข้ามาใหม่ต่อไป

---

nectec. **Digital Signature**. P.1-2

# บทที่ 3
# ระเบียบวิธีวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบสถาปัตยกรรมการกรองข้อความสแปมที่สามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้อย่างมีประสิทธิภาพ และเพื่อออกแบบสถาปัตยกรรมการกรองข้อความสแปมที่มีความถูกต้องสูง ทั้งนี้ผู้วิจัยได้แบ่งขั้นตอนการดำเนินงานออกเป็น 5 ขั้นตอนดังนี้

3.1 ศึกษาปัญหาและความต้องการของระบบ( Feasibility Study )

3.2 การวิเคราะห์และออกแบบ ( Analysis and Design )

3.3 การพัฒนาโปรแกรม ( Development )

3.4 การทดสอบโปรแกรม ( Test )

3.5 การประเมินผลการวิจัย ( Conclusions of the Research Evaluation )

**3.1 ศึกษาปัญหาและความต้องการของระบบ ( Feasibility Study )**

การศึกษาปัญหาและความต้องการของการพัฒนาโปรแกรมตรวจสอบข้อความไม่เหมาะสม สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานระบบรับ - ส่งจดหมายอิเล็กทรอนิกส์เมล์เป็นการศึกษาถึงความเป็นไปได้ในการพัฒนาโปรแกรมในอนาคตว่าเป็นไปได้หรือไม่ ซึ่งจากปัญหาเรื่องการส่งผ่านข้อมูลสแปมเมล (ข้อความไม่เหมาะสม) ผ่านช่องทางระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์เมล์ของเครื่องคอมพิวเตอร์ลูกข่ายนั้น มีความเป็นไปได้ในการพัฒนาโปรแกรมนี้ จากการศึกษาข้อมูลในเบื้องต้น พบว่าในการพัฒนาโปรแกรมนี้สามารถที่จะใช้โปรแกรมอินเทอร์เน็ต เอ็กซ์พลอเรอร์ เบราว์เซอร์ ตั้งแต่เวอร์ชั่น 5 หรือสูงกว่าขึ้นไป ซึ่งเป็นโปรแกรมที่หาง่ายและมีการติดตั้งมาพร้อมกับระบบปฏิบัติการวินโดว์อยู่เรียบร้อยแล้วในปัจจุบัน ส่วนคุณสมบัติของเครื่องคอมพิวเตอร์ที่จะใช้งานระบบนี้ได้ คือ เครื่องที่สามารถต่อเชื่อมกับระบบอินเทอร์เน็ตได้ และมีการติดตั้งโปรแกรมอินเทอร์เน็ต เอ็กซ์พลอเรอร์ เบราว์เซอร์ไว้เรียบร้อยแล้ว

3.1.1 ศึกษาขั้นตอนการพัฒนาระบบ

ส่วนของโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Block Data Spam) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่เรียกใช้งานระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์เมล์ ซึ่งส่วนนี้จะทำการตรวจสอบข้อความ (Text) ต่างๆ ที่ผู้ใช้เรียกใช้งานระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์เมล์ผ่าน

โปรแกรมอินเทอร์เน็ต เอ็กซ์พลอเรอร์ เบราว์เซอร์ ตั้งแต่เวอร์ชั่น 5 ขึ้นไป มีรูปแบบการทำงานคือ เมื่อผู้ใช้ทำการเรียกใช้งานระบบรับ – ส่งจดหมายอิเล็กทรอนิสก์เมล์ และทำการกรอกข้อความใดๆ บนพื้นที่ของฟอร์มส่งจดหมาย และทำการคลิกปุ่ม Send ระบบจะนำข้อความดังกล่าวไปตรวจสอบด้วยการเปรียบเทียบกับรายชื่อของข้อความที่ไม่เหมาะสมที่ได้เก็บรวบรวมไว้ในฐานข้อมูลของโปรแกรม หากพบว่าตรงกันให้ทำการป้องกันไม่ให้ส่งข้อความดังกล่าวไปยังเมล์เซิร์ฟเวอร์ เพื่อเป็นการลดปริมาณสแปมเมลที่จะเกิดขึ้นในระบบ จากนั้นโปรแกรมจะทำการแจ้งเตือนผู้ใช้งานว่าจดหมายนี้มีเนื้อหาที่ไม่เหมาะสมเข้าข่ายการกระทำความผิดการส่งผ่านข้อมูลสแปมเปิดขึ้นมาบนคอมพิวเตอร์ลูกข่ายเครื่องที่กำลังกระทำความผิดอยู่

3.1.2 เครื่องมือในการพัฒนาโปรแกรมตรวจสอบข้อความไม่เหมาะสม มีดังต่อไปนี้

1) ด้านฮาร์ดแวร์

1.1) เครื่องคอมพิวเตอร์ลูกข่าย มีความเร็ว (CPU) ไม่น้อยกว่า 1 GHz

1.2) หน่วยความจำหลักมีความจุ (RAM) ไม่น้อยกว่า 128 MB

1.3) มีพื้นที่ว่าง (Free HardDisk) สำหรับติดตั้งโปรแกรมไม่น้อยกว่า 100 MB

2) ด้านซอฟต์แวร์

2.1) โปรแกรม Macromedia Dreamweaver MX สำหรับพัฒนาโปรแกรม

2.2) โปรแกรม MySql , Notepad สำหรับจัดทำฐานข้อมูล

2.3) โปรแกรม WPE Pro สำหรับตรวจจับ Packets และปริมาณ traffic ในระบบ

3.1.3 เครื่องมือในการทดสอบโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปม มีดังต่อไปนี้

1) ด้านฮาร์ดแวร์

1.1) เครื่องคอมพิวเตอร์มีความเร็ว (CPU) เทียบเท่ากับ Pentium 166 GHz หรือเป็นเครื่องที่มีประสิทธิภาพสูงกว่า เพื่อใช้ในการติดตั้งโปรแกรม อีกทั้งยังเป็นการไม่ให้กระทบกระเทือนการทำงานของโปรแกรมอื่นๆ อีกด้วย หากใช้เครื่องที่มีคุณสมบัติต่ำกว่านี้

1.2) หน่วยความจำหลักมีความจุ (RAM) ไม่น้อยกว่า 64 MB ใช้สำหรับเป็นที่เก็บและประมวลผลของโปรแกรม เพื่อให้เกิดความรวดเร็วและถูกต้องในการทำงาน

1.3) มีพื้นที่ว่างสำหรับติดตั้งโปรแกรม (Free Hard Disk) ไม่น้อยกว่า 10 MB ใช้สำหรับการติดตั้งโปรแกรม เพื่อให้มีพื้นที่เพียงพอกับการทำงานของโปรแกรม

2) ด้านซอฟต์แวร์

2.1) โปรแกรม Macromedia Dreamweaver MX สำหรับพัฒนาโปรแกรม ซึ่งเป็นโปรแกรมที่รองรับ Functions ต่างๆ รวมถึง Component ที่ต้องใช้ในการพัฒนาโปรแกรมอย่างครบถ้วนและเหมาะสม

2.2) โปรแกรม MySql , Notepad สำหรับจัดทำฐานข้อมูล เนื่องจากหาง่ายและราคาไม่แพง

2.3) ใช้ระบบปฏิบัติการ Windows 2000 หรือ Windows XP ขึ้นไป

2.4) โปรแกรม VMware Workstation v6 สำหรับสร้างเครื่องคอมพิวเตอร์จำลอง ซึ่งจะสามารถติดตั้งระบบปฏิบัติการและโปรแกรมประยุกต์ต่างๆ ได้ เพื่อใช้ในการจำลองเครื่องคอมพิวเตอร์ให้เป็นเครื่องเซิร์ฟเวอร์และเครื่องลูกข่ายในเครื่องเดียวกัน

2.5) โปรแกรม Argosoft Mail Server สำหรับทำเมล์เซิร์ฟเวอร์

2.6) โปรแกรม WPE Pro สำหรับตรวจจับ Packets และปริมาณ traffic ในระบบ

2.7) โปรแกรม Microsoft Outlook สำหรับรับ – ส่งจดหมายอิเล็กทรอนิกส์ เพื่อเปรียบเทียบประสิทธิภาพกับโปรแกรมเว็บเมล์ที่สร้างขึ้น

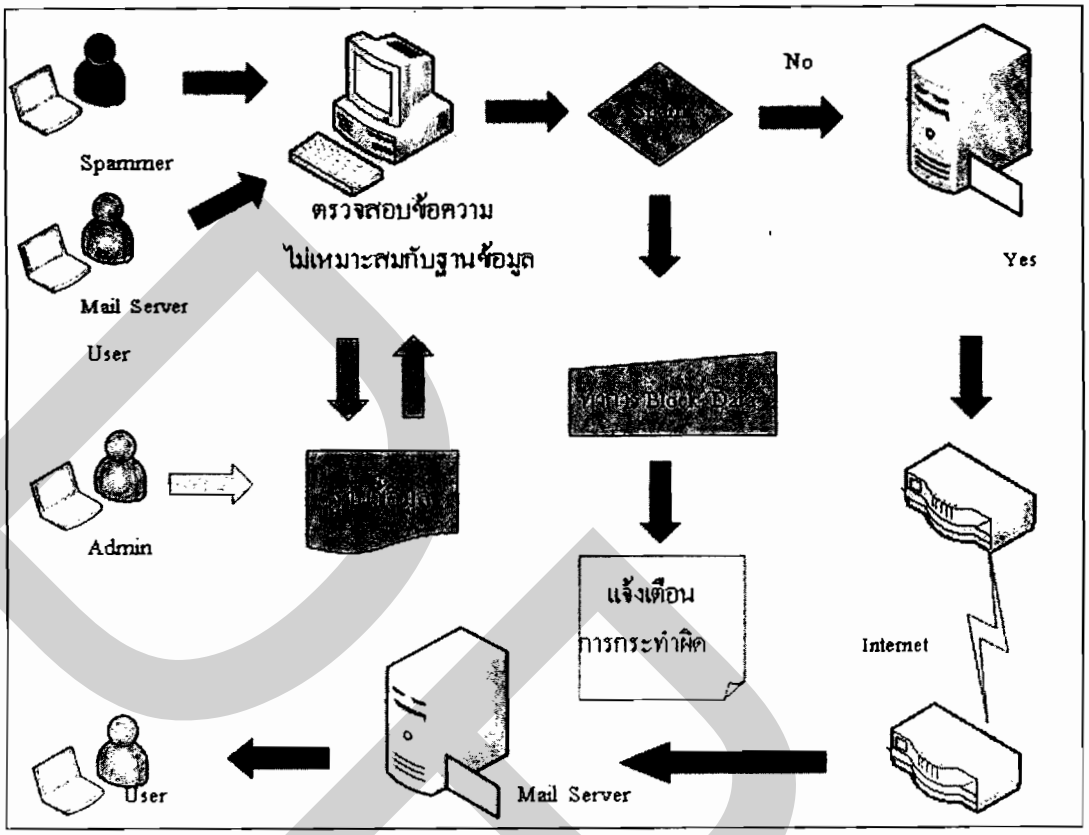
**3.2 การวิเคราะห์และออกแบบ ( Analysis and Design )**

การวิเคราะห์และออกแบบโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมสำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์เมล์ ผ่านอินเทอร์เน็ต เอ็กซ์ พลอเรอร์ เบราว์เซอร์ เพื่อให้มีความเหมาะสมสอดคล้องกับหลักการและทฤษฎีการออกแบบมีดังต่อไปนี้

3.2.1 วิเคราะห์และออกแบบโปรแกรม โดยมีการทำงานเป็น 2 โมดูล ประกอบด้วย

1) โมดูลแรก ทำหน้าที่ตรวจสอบข้อความไม่เหมาะสมกับฐานข้อมูลที่ได้จัดทำไว้ หากพบว่าเป็นข้อความไม่เหมาะสม (Spam) โปรแกรมจะระงับการส่งข้อความดังกล่าว พร้อมทั้งแสดงข้อความแจ้งเตือนให้ผู้ใช้งานทราบ ดังรายละเอียดในภาพที่ 3.1

2) โมดูลที่สอง ทำหน้าที่ปรับปรุงรายชื่อข้อความไม่เหมาะสมในฐานข้อมูล




ภาพที่ 3.1 หลักการทำงานของโปรแกรม

3.2.2 การออกแบบฐานข้อมูลสำหรับการกรองข้อความไม่สุภาพ และข้อความสแปม

1) นำข้อมูลที่ได้จากการสำรวจความคิดเห็นการนิยามข้อความ spam[1] มาสร้างเป็นฐานข้อมูล ประกอบด้วยข้อมูลดังนี้

[1] นนท์ บุญนิธิประเสริฐ, ชัยพร เขมะภาตะพันธ์ .(2552) **การกรองข้อความภาษาไทย และภาษาอังกฤษของบริการส่งข้อความสั้นบนเครือข่ายโทรศัพท์เคลื่อนที่**.หน้าที่ 33

ตารางที่ 3.1 ฐานข้อมูลสแปม

| ลำดับ | คำ | ลำดับ | คำ | ลำดับ | คำ | ลำดับ | คำ |
|---|---|---|---|---|---|---|---|
| 1 | Bonus | 21 | ซื้อ | 41 | ลักษณ์ | 61 | เชิญชวน |
| 2 | Download | 22 | ดวง | 42 | ลุ้น | 62 | เชียมซี |
| 3 | Duty | 23 | ดารา | 43 | สนุก | 63 | เด็ด |
| 4 | Free | 24 | ดาวน์ | 44 | สมัคร | 64 | เติม |
| 5 | Mail | 25 | ดาวน์โหลด | 45 | สลาก | 65 | เบอร์ |
| 6 | mms | 26 | ดูดวง | 46 | สอบถาม | 66 | เพลง |
| 7 | Promotion | 27 | ดูหมอ | 47 | สิทธิพิเศษ | 67 | เพิ่ม |
| 8 | Push | 28 | ด่วน | 48 | สินค้า | 68 | เพิ่มเติม |
| 9 | Ringtone | 29 | บริการ | 49 | สุขภาพ | 69 | เพียง |
| 10 | Sms | 30 | พยากรณ์ | 50 | ส่ง | 70 | เวลา |
| 11 | Vote | 31 | พิเศษ | 51 | ส่งเสริม | 71 | เสียง |
| 12 | www | 32 | ฟรี | 52 | ส่วนลด | 72 | แม่น |
| 13 | Xxx | 33 | ฟุตบอล | 53 | หาคู่ | 73 | โฆษณา |
| 14 | กด | 34 | ราคา | 54 | ห้างสรรพสินค้า | 74 | โชคดี |
| 15 | ขาย | 35 | รางวัล | 55 | อ้วน | 75 | โทน |
| 16 | คลิป | 36 | รายการ | 56 | ฮิต | 76 | โทรศัพท์ |
| 17 | คอร์ส | 37 | รายละเอียด | 57 | เกมส์ | 77 | โบนัส |
| 18 | คูปอง | 38 | รูปภาพ | 58 | เครดิต | 78 | โหลด |
| 19 | ค่าบริการ | 39 | ร้านค้า | 59 | เงิน | 79 | ใหม่ |
| 20 | ชิง | 40 | ลด | 60 | เงินพิเศษ | | |

2) ความหมายของข้อความ Spam แบ่งออกเป็น 4 ประเภทเรียงตามลำดับคะแนน ดังนี้

2.1) ข้อความโฆษณาประชาสัมพันธ์ การขายสินค้า หรือมีการเสนอของรางวัล โดยมีเงื่อนไขต่างๆ

2.2 ) ข่าวสารทั่วไป หรือข้อความแจ้งข้อมูลจากผู้ให้บริการ

2.3) ข้อความจากผู้ที่ท่านไม่รู้จัก หรือไม่ระบุที่มาของผู้ส่ง

2.4) ข้อความเดิมหรือข้อความที่มีความหมายใกล้เคียงกันที่ส่งหลายครั้ง

สิ่งที่เพิ่มเติมในงานวิจัยนี้ คือ ข้อความไม่สุภาพ คำหยาบ เนื่องจากในปัจจุบันมีการใช้คำไม่สุภาพและคำหยาบเป็นจำนวนมาก เพื่อเป็นการส่งเสริมการใช้ภาษาให้มีความถูกต้อง งานวิจัยนี้จึงได้บรรจุ " คำหยาบ , คำไม่สุภาพ " ( คำดิบ ) ลงในฐานข้อมูลด้วย

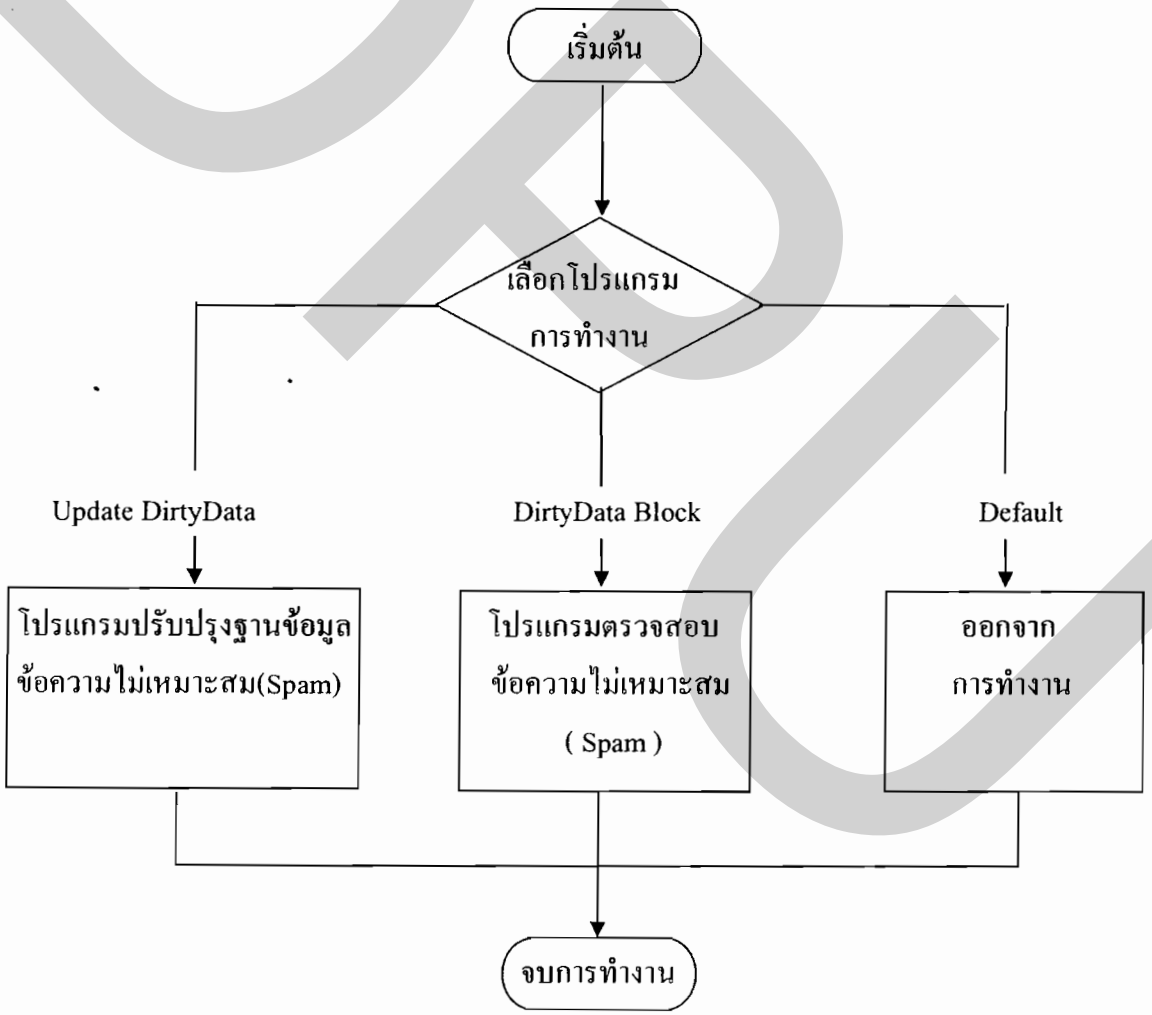
3) ผลกระทบและการแก้ไขปัญหาข้อความไม่สุภาพ ข้อความ spam

3.1) ก่อความรำคาญและทำให้ใช้งานไม่สะดวก

3.2) ถูกละเมิดสิทธิส่วนบุคคล

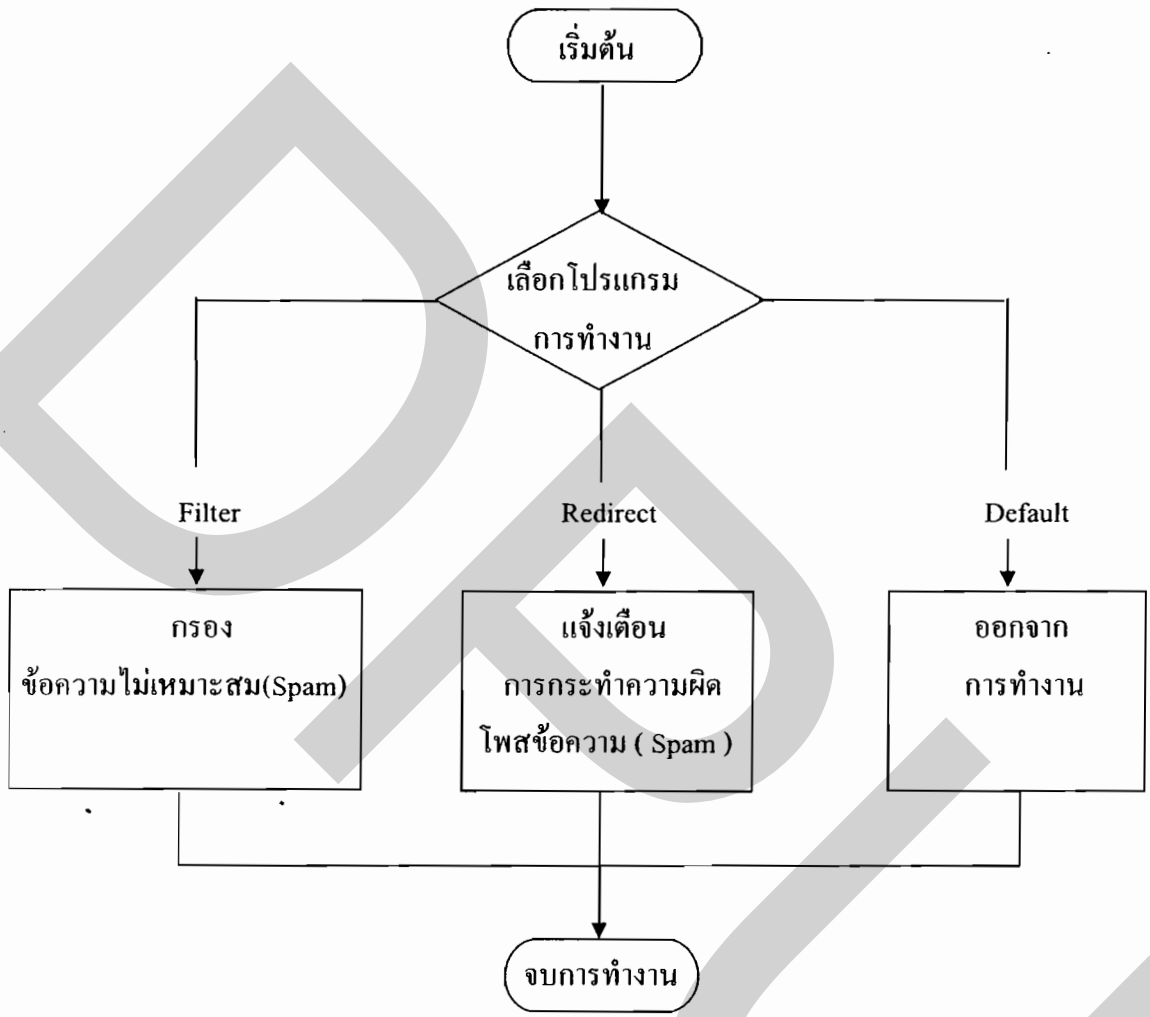
3.3) เสียพื้นที่ในการเก็บข้อความที่จำเป็น (Inbox เต็ม)

3.2.3 ผังงานระบบ ( System Flowchart)



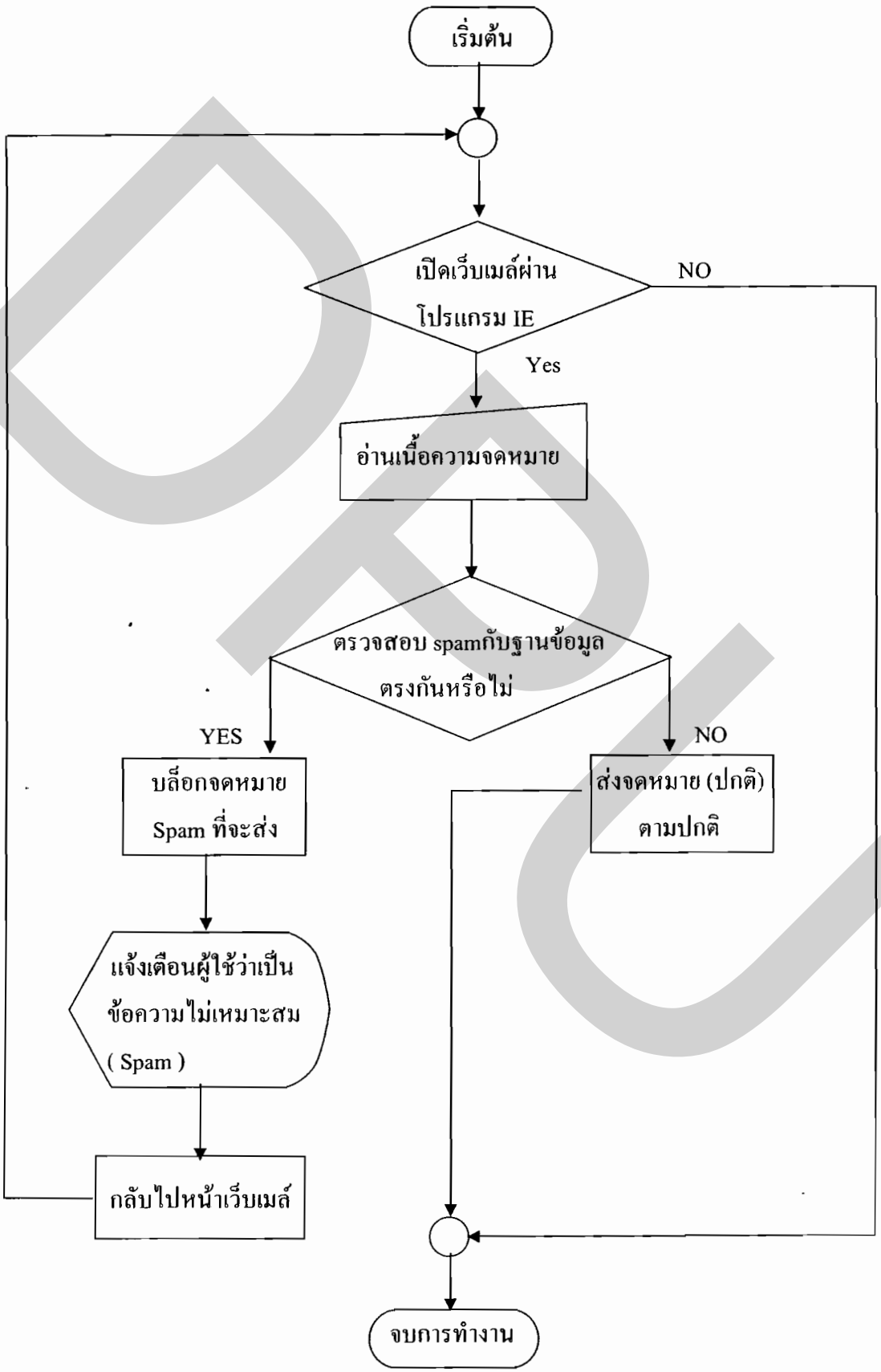

ภาพที่ 3.2 ผังงานระบบกรองข้อความไม่เหมาะสม ( Spam )

### 3.2.4 ผังงานโปรแกรมการปรับปรุงฐานข้อมูลข้อความไม่เหมาะสม ( Spam )




ภาพที่ 3.3 ผังงานการปรับปรุงฐานข้อมูลข้อความไม่เหมาะสม ( Spam )

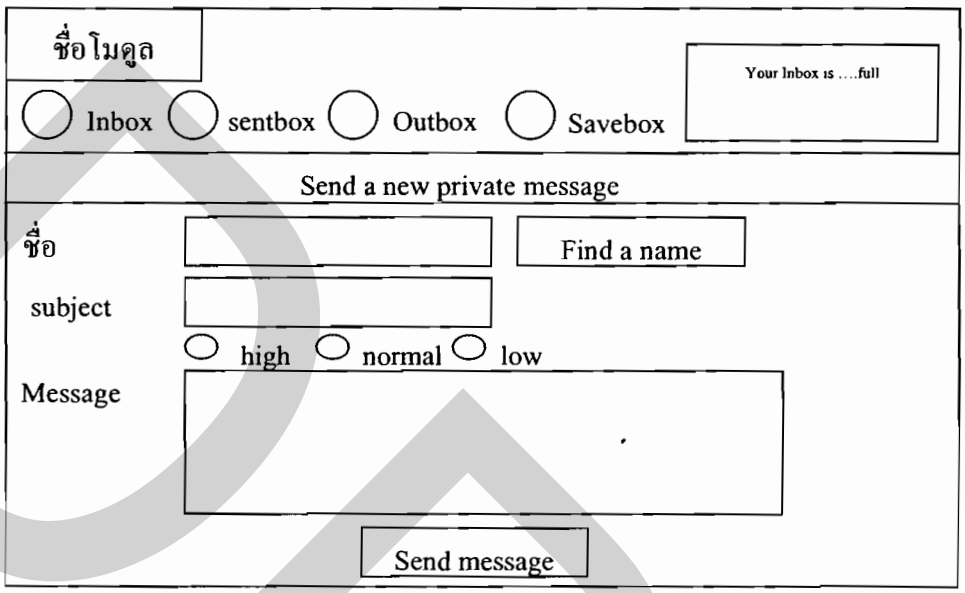
3.2.5 ผังงานโปรแกรมตรวจสอบข้อความไม่เหมาะสม ( Spam )




ภาพที่ 3.4 ผังงานโปรแกรมตรวจสอบข้อความไม่เหมาะสม ( Spam )

3.2.6 การออกแบบหน้าจอ ( Design Interface )

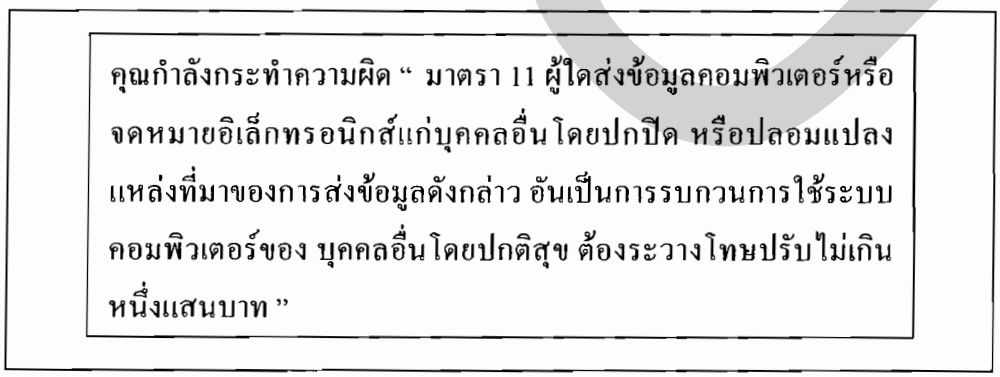
1) หน้าจอโปรแกรมส่งข้อความ




ภาพที่ 3.5 หน้าจอการทำงานของโปรแกรมส่งข้อความ

2) เมื่อ User กรอกข้อความจดหมาย ระบบจะนำ Subject และ Message มาทำการตรวจสอบกับฐานข้อมูลสแปมและข้อความไม่สุภาพ ในฐานข้อมูลลักษณะการตรวจไวยากรณ์หรือการสะกดคำ ซึ่งหากตรวจพบว่าข้อมูลที่ผู้ใช้กรอกตรงกันจะทำการบล็อกข้อความดังกล่าว

3) เมื่อตรวจพบระบบจะทำการบล็อกข้อความดังกล่าว และแจ้งเตือนการกระทำความผิดให้ผู้ใช้ทราบทันที เพื่อปรับปรุงแก้ไขการกระทำดังกล่าว




ภาพที่ 3.6 หน้าจอการแจ้งเตือนเมื่อตรวจพบข้อความไม่เหมาะสม ( spam )

**3.3 การพัฒนาโปรแกรม ( Development )**

การพัฒนาโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมลสำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์ โดยใช้โปรแกรมภาษา PHP, JAVA และใช้ฐานข้อมูล MySql โดยมีขั้นตอนการพัฒนาโปรแกรม ดังนี้

3.3.1 สำรวจและรวบรวมข้อมูลสแปม เพื่อจัดทำเป็นฐานข้อมูล

3.3.2 ศึกษาทฤษฎีที่เกี่ยวข้อง เพื่อใช้ประกอบการพัฒนาโปรแกรมให้เกิดประสิทธิภาพสูงสุด ได้แก่

1) หลักการทำงานของโปรแกรมรับ – ส่งจดหมายอิเล็กทรอนิกส์

2) หลักการทำงานของเมล์เซิร์ฟเวอร์

3) หลักการทำงานของระบบเครือข่ายและโปรโตคอล

4) หลักการทำงานของฐานข้อมูลเชิงสัมพันธ์ (Relational Database)

5) หลักการทำงานของโปรแกรมอินเทอร์เน็ต เอ็กซ์พลอเรอร์ เบราว์เซอร์

6) หลักการทำงานของโปรแกรมซอฟต์แวร์ที่ใช้ในการพัฒนาระบบ

7) ศึกษา Filter สำหรับกรอง Spam ที่มีใช้อยู่ในปัจจุบัน

3.3.3 วิเคราะห์และออกแบบระบบฐานข้อมูล

3.3.4 พัฒนาโปรแกรม

1) ด้านระบบเครือข่ายและโปรโตคอล

1.1) ติดตั้งโปรแกรม VMware Workstation สำหรับสร้าง Vitrual Machine (VM) หรือเครื่องคอมพิวเตอร์เสมือน

1.2) ติดตั้งเครื่อง server บน VM (Web Server , Mail Server)

1.3) ติดตั้งเครื่องลูกข่ายบน VM (ระบบปฏิบัติการวินโดว์ XP)

1.4) ติดตั้งเครื่องลูกข่ายบนระบบปฏิบัติการหลัก (ระบบปฏิบัติการวินโดว์ 7)

1.5) ติดตั้งระบบ Network

2) ด้านเว็บเซิร์ฟเวอร์ และเมล์เซิร์ฟเวอร์

2.1) ด้านเว็บเซิร์ฟเวอร์

ติดตั้งโปรแกรม Web Server สำหรับให้บริการเว็บเมล์ ได้แก่ โปรแกรม IIS และAppserv Program

2.2) ด้านเมล์เซิร์ฟเวอร์

ติดตั้งโปรแกรมเมล์เซิร์ฟเวอร์ (ArGoSoft Mail Server) สำหรับระบบรับ – ส่งจดหมาย ของ Microsoft Outlook 2003

3) ด้านโปรแกรมรับ – ส่งจดหมายอิเล็กทรอนิกส์ (e-mail)

3.1) โปรแกรม Microsoft Outlook 2003

3.2) เว็บเมล์ Smail.com

3.2.1) พัฒนาเว็บเมล์ด้วยภาษา Personal Home Pages (PHP) และ Java script

3.2.2) เทคโนโลยี Server-side scripting สำหรับสร้าง dynamic และ Interactive Web Applications

3.2.3) การเขียน PHP script จะทำโดยการฝังหรือ embedded ส่วนที่เป็น script ลงไปในเว็บเพจ

3.2.4) PHP จะแสดงหน้าการทำงานแบบ HTML ที่ประกอบด้วย Server-side scripts ที่ถูกประมวลผลโดย Web server ก่อนที่จะส่งไปยัง Browser ของผู้ใช้งาน

4) ด้านโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam)

4.1) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานระบบรับ - ส่งจดหมายอิเล็กทรอนิกส์ (อีเมล) ส่วนนี้จะเป็นการตรวจสอบข้อความต่างๆ ที่ผู้ใช้ทำการกรอกข้อมูลในส่วนของเนื้อความจดหมาย เมื่อผู้ส่งกด Send เพื่อทำการส่งโปรแกรมจะทำการตรวจสอบและดักจับข้อความดังกล่าว โดยเปรียบเทียบกับรายชื่อของข้อความที่ไม่เหมาะสมที่ได้เก็บรวบรวมไว้ในฐานข้อมูลของโปรแกรม หากพบว่าตรงกันให้ทำการป้องกันไม่ให้ส่งข้อความดังกล่าว และแจ้งเตือนให้ผู้ใช้งานทราบว่าข้อความนี้มีเนื้อหาไม่เหมาะสมระบบไม่สามารถทำการส่งข้อความดังกล่าวได้ โดยมีหลักการทำงานดังนี้

4.1.1) โปรแกรมจะถูกเรียกขึ้นมาพร้อมกับตอนที่เปิดการใช้งานระบบรับ – ส่งเมล์

4.1.2) เมื่อมีการเรียกใช้งานโปรแกรมรับ – ส่งเมล์โปรแกรมตรวจสอบข้อความที่ไม่เหมาะสมจะทำงานแบบอัตโนมัติ

4.1.3) นำข้อความที่ User ทำการ Send มาทำการตรวจสอบกับฐานข้อมูลข้อความที่ไม่เหมาะสมหากตรงกันให้ทำการ Block Data ดังกล่าวทันที

4.1.4) เมื่อทำการ Block Data ดังกล่าวเรียบร้อยแล้ว จะแสดงข้อความแจ้งให้ผู้ใช้งานทราบถึงการกระทำความผิด และแนวทางการปฏิบัติ

4.1.5) หากตรวจสอบแล้วข้อความดังกล่าวเป็นข้อความปกติ ไม่มีการละเมิดหรือการกระทำความผิดข้อความ (จดหมาย) นั้นจะถูกส่งไปยัง Mail Server และส่งไปยังผู้รับ

4.2 ส่วนของโปรแกรมปรับปรุงฐานข้อมูลข้อความไม่เหมาะสม ส่วนนี้จะใช้ในการเก็บรายชื่อข้อความที่ไม่เหมาะสมของโปรแกรม เนื่องจากโปรแกรมตรวจสอบข้อความที่ไม่

เหมาะสมสำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้อินเทอร์เน็ตระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์ (อีเมล) เป็นโปรแกรมขนาดเล็กและยังไม่ได้ผนวกในส่วนของการปรับปรุงฐานข้อมูลแบบออนไลน์ จึงให้ Admin เป็นผู้ปรับปรุง แก้ไข ลบ เพิ่ม ฐานข้อมูลรายชื่อข้อความที่ไม่เหมาะสมเองได้ตลอดเวลา โดยเขียนข้อมูลเพิ่มเติมในส่วนของฐานข้อมูลดังกล่าว

3.3.5 ทดสอบและปรับปรุงแก้ไขโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam)

**3.4 การทดสอบโปรแกรม ( Test )**

3.4.1 ทดสอบการทำงานของระบบขั้นต้น โดยหลังจากมีการพัฒนาระบบตรวจสอบข้อความไม่เหมาะสม (Spam) และแจ้งเตือนการกระทำความผิดทางเครือข่ายคอมพิวเตอร์ผ่านไประยะหนึ่ง จะเริ่มทำการทดสอบหาข้อผิดพลาด เพื่อพัฒนาและแก้ไขให้ระบบทำงานได้อย่างสมบูรณ์

หลังจากมีการพัฒนาระบบการกรองผ่านไประยะหนึ่ง จะเริ่มทำการทดสอบย่อย เพื่อหาข้อผิดพลาดต่างๆ ภายใน Application แล้วทำการแก้ไข

3.4.2 ทดสอบประสิทธิภาพจริงของระบบตรวจสอบข้อความไม่เหมาะสมและแจ้งเตือนการกระทำความผิดทางเครือข่ายคอมพิวเตอร์ที่พัฒนาขึ้น และทำการประเมินประสิทธิภาพของระบบพร้อมทำการสรุปผล

ทำการทดสอบระบบด้วยการ นำข้อมูลจดหมายขยะและจดหมายปกติที่ได้จาก hotmail นำมาเป็นข้อมูลชุดตัวอย่าง เพื่อใช้ในการทดสอบระบบ วิธีการทดสอบระบบคือนำชุดข้อมูลตัวอย่างทำการส่งเมล์ไปยังผู้รับผ่านเว็บเมล์และตัวกรองที่สร้างขึ้น กรณีที่เป็นจดหมายขยะระบบจะต้องทำการบล็อกจดหมายดังกล่าวโดยไม่ยินยอมให้ทำการส่ง แต่หากจดหมายที่ต้องการส่งเป็นจดหมายที่มีสถานะปกติ (ไม่มีข้อความที่ไม่เหมาะสม) ระบบจะทำการส่งจดหมายดังกล่าวไปยังเมล์เซิร์ฟเวอร์ เพื่อจัดส่งถึงผู้รับปลายทาง โดยเปรียบเทียบประสิทธิภาพด้วยการใช้ข้อมูลชุดเดียวกันในการทดสอบผ่านโปรแกรม Microsoft Outlook 2003, hotmail, gmail, yahoo ซึ่งไม่ว่าผู้ส่งจะทำการส่งจดหมายที่มีสถานะปกติ หรือผู้ส่งมีความประสงค์ที่จะส่งจดหมายขยะ โปรแกรม Microsoft Outlook 2003, hotmail, gmail, yahoo จะต้องยินยอมให้ส่งจดหมายดังกล่าวได้ในทุกกรณี

หลังจากได้ทำการพัฒนาโปรแกรมเสร็จเรียบร้อยแล้ว การทดสอบโปรแกรมจะทำการทดลองใช้งานระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์ (อีเมล) ภายในองค์กรกรมพลาธิการทหารบก โดยขั้นต้นจะทำการทดสอบระบบที่กองยุทธการและการข่าว เพื่อเป็นหน่วยนำร่องเนื่องจากเป็นหน่วยงานที่ทำหน้าที่ด้านการรักษาความปลอดภัยแก่หน่วยในเรื่องของบุคคล ข้อมูลข่าวสาร และสถานที่ จากภารกิจดังกล่าว จึงถือได้ว่าเป็นหน่วยงานที่มีความเหมาะสม ผู้วิจัยจึงเลือกหน่วยงานนี้

เป็นกรณีศึกษาเพื่อทดสอบการใช้งานว่ามีความเหมาะสมหรือต้องปรับปรุงโปรแกรมส่วนใด เพื่อให้เกิดความสมบูรณ์และมีประสิทธิภาพในการทำงานเมื่อนำไปใช้จริง

สรุปผลการเปรียบเทียบและประโยชน์ นำผลการทำงานในการจำลองสถานการณ์มาสร้างกราฟ เพื่อใช้ในการวิเคราะห์การทำงานและประเมินประสิทธิภาพของระบบ

### 3.5 การประเมินผลการวิจัย ( Conclusions of the Research Evaluation )

การประเมินผลการทำงานของโปรแกรมการตรวจสอบการส่งผ่านข้อมูลสแปมเมล สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์ งานวิจัยนี้ได้มีการประเมินประสิทธิภาพของตัวกรองสแปมบนเว็บเมล์ที่พัฒนาขึ้นในมิติต่างๆ ดังต่อไปนี้

1) การประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่างๆ ได้แก่ Hotmail Yahoo และ Gmail

2) การวัดความแม่นยำและถูกต้องของตัวกรองข้อความสแปมที่พัฒนาขึ้น

3) เปรียบเทียบผลการกรองจากการติดตั้งตัวกรองข้อความสแปมต่างสถานที่ และ

4) วิเคราะห์ผลการทดลอง

# บทที่ 4
# ผลการวิจัย

เมื่อทำการวิเคราะห์และออกแบบ ตลอดจนพัฒนาโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมลสำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์เสร็จสมบูรณ์เรียบร้อยแล้ว จึงได้นำโปรแกรมดังกล่าวมาประเมินหาประสิทธิภาพในการทำงานของโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam) ผลการดำเนินงานและการประเมินโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมล สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์มีดังต่อไปนี้

## 4.1 ผลการพัฒนาโปรแกรม

ผลจากการพัฒนาโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมล สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์ สามารถจำแนกเป็นการทำงานในด้านต่างๆ ได้ดังรายละเอียดต่อไปนี้

4.1.1 ด้านระบบเครือข่ายและโปรโตคอล

1) ติดตั้ง VMware Workstation 6.0

ผู้วิจัยจึงเลือกใช้ VMware ในการทดสอบระบบเมล์เซิร์ฟเวอร์ในการทำวิจัยครั้งนี้ เนื่องจากทำให้ผู้วิจัยสามารถทดลองใช้งาน OS หรือโปรแกรมอื่นๆ ที่สนใจได้โดยไม่ต้องทำการ format เครื่อง

2) การติดตั้งระบบ Network

การติดตั้งและการทดลองใช้งานระบบอีเมลที่พัฒนาขึ้น ได้นำไปทดลองใช้งานจริงในขั้นต้น ณ กองยุทธการและการข่าว กรมพลาธิการทหารบก เนื่องจากเป็นหน่วยงานที่มีภารกิจในเรื่องของการดำเนินการเกี่ยวกับการข่าวกรองทางเทคนิคของเหล่าทหารพลาธิการ งานกิจการพลเรือน และการรักษาความปลอดภัยต่อบุคคล สถานที่ และเอกสารของกรมพลาธิการทหารบก จึงเป็นหน่วยงานที่มีความเหมาะสมในการทดลองการใช้งานในระบบที่ถูกพัฒนาขึ้น

การทดลองใช้งานระบบอีเมลที่พัฒนาขึ้นนั้น ผู้วิจัยได้ดำเนินการเพิ่มบัญชีรายชื่อผู้ใช้จากบัญชีรายชื่อกำลังพลสังกัดกองยุทธการและการข่าว กรมพลาธิการทหารบก จำนวนทั้งสิ้น 28 คน (อัตรากำลังพลทั้งสิ้น 40 คน บรรจุจริง 28 คน) ประกอบด้วยเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้ในระบบ จำนวนทั้งสิ้น 16 เครื่อง

4.1.2 ด้านเว็บเซิร์ฟเวอร์ และเมล์เซิร์ฟเวอร์

1) Web Server

IIS เป็นโปรแกรมที่ใช้สำหรับทำเว็บเซิร์ฟเวอร์จากค่ายไมโครซอฟต์ ใช้สำหรับทดสอบเขียนภาษาสคริปต์ต่างๆ ที่ต้องการประมวลผลที่เซิร์ฟเวอร์สำหรับงานวิจัยนี้ใช้ IIS5 บนระบบปฏิบัติการ Windows XP Professional

2) Mail Server

งานวิจัยนี้ได้นำโปรแกรม Argosoft Mail Server มาใช้ในการจำลองระบบรับ – ส่งจดหมายอิเล็กทรอนิกส์เมล์

4.1.3 ด้านโปรแกรมรับ – ส่งจดหมายอิเล็กทรอนิกส์ (e-Mail)

1) Microsoft Outlook 2003

การใช้จดหมายอิเล็กทรอนิกส์ (e-Mail) ด้วย Microsoft Outlook และสร้าง Username ของแต่ละคนเพื่อ Login เข้าใช้ Microsoft Outlook 2003 ซึ่งการทำเช่นนี้เราเรียกว่าการกำหนด User Profile

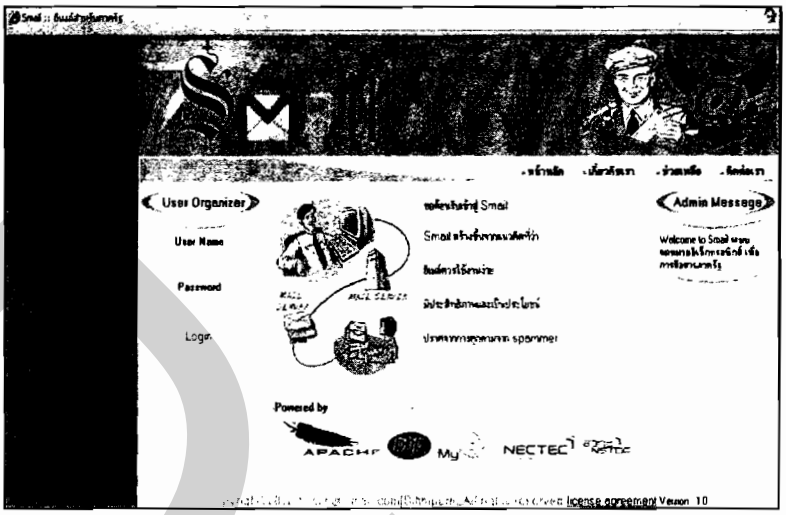
2) Web Mail [Smail.com]

2.1) การทำงานของเว็บเมล์ที่พัฒนาขึ้น

· Smail ถูกสร้างขึ้นเพื่อการสื่อสารภาครัฐ แบ่งกลุ่มผู้ใช้ออกเป็น 2 กลุ่ม คือ ผู้ดูแลระบบ และผู้ใช้งาน

ผู้ดูแลระบบ ทำหน้าที่เพิ่มบัญชีรายชื่อผู้ใช้ จัดการตั้งค่าและรูปแบบต่างๆ ของระบบ

ผู้ใช้งาน มีหน้าที่ในการใช้งานโดยรับส่งจดหมายอิเล็กทรอนิกส์




ภาพที่ 4.1 รูปเว็บเมล์ที่พัฒนาขึ้น

2.2) เว็บเมล์ประกอบด้วย

2.2.1) หน้าหลัก

ใช้สำหรับ login เข้าระบบ ซึ่งแบ่งผู้ใช้เป็น 2 ส่วนคือ

1. ผู้ดูแลระบบ (admin)
2. ผู้ใช้งาน (User)

2.2.2) เกี่ยวกับเรา

เพื่อให้ทราบถึงความเป็นมา ประกอบด้วย

1. ความเป็นมาและแนวเหตุผล
2. วัตถุประสงค์
3. ขอบเขตของการวิจัย
4. ขั้นตอนและวิธีการดำเนินงาน
5. ประโยชน์ที่ได้รับ

2.2.3) ช่วยเหลือ

1. การยอมรับในข้อกำหนดและเงื่อนไขการใช้บริการ
2. ข้อกำหนดการสมัครสมาชิก
3. ความต้องการของระบบ
4. การใช้งาน (การส่งข้อความ)

2.2.4) ติดต่อเรา

2.3) ระบบส่งข้อความ

ระบบจดหมายอิเล็กทรอนิกส์นี้ อนุญาตให้ผู้ใช้สามารถติดต่อกันได้ภายในระบบผ่านทาง e-Mail (ผู้ใช้ไม่สามารถรับหรือส่งข้อความนอกระบบได้)

เมื่อผู้ใช้เข้าสู่หน้า " ส่งข้อความ " ในการส่งข้อความจะมีขั้นตอนการใช้งาน ดังนี้

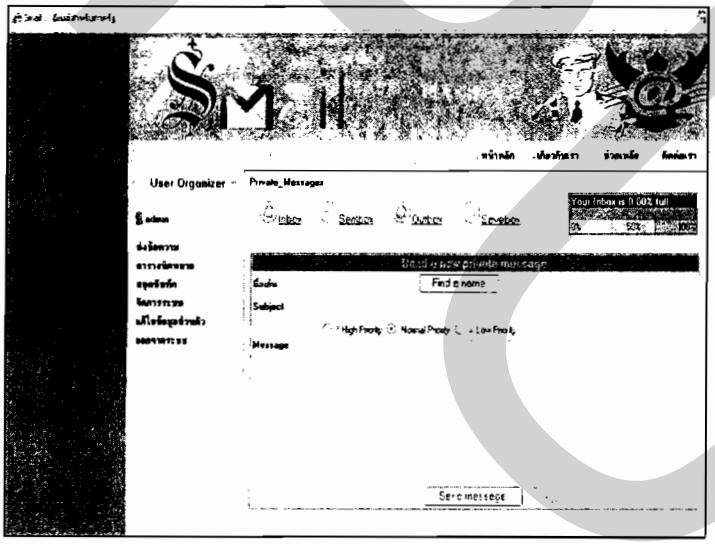
1. ช่อง " ชื่อ " สำหรับใส่ชื่อผู้รับจะต้องเป็นชื่อในระบบเท่านั้น ซึ่งสามารถตรวจสอบและค้นหาได้โดยการคลิกที่ปุ่ม Find a name

2. ช่อง " Subject " สำหรับใส่หัวข้อของข้อความ

3. ปุ่มเลือกระดับความสำคัญ มี 3 ระดับ คือ high, normal และ low เมื่อผู้ใช้เลือกระดับความสำคัญ รูปภาพแสดงระดับความสำคัญที่อยู่ตรงหน้าของปุ่มกำหนดระดับ จะไปปรากฏในตู้รับจดหมายของผู้รับ

4. ช่อง " Message" สำหรับกรอกข้อความที่ต้องการส่ง

5. เมื่อผู้ใช้กรอกข้อมูลทุกอย่างและกดปุ่ม Send message ด้านล่าง ข้อความจะถูกส่งไปยังผู้รับและถูกนำไปเก็บอยู่ใน Outbox

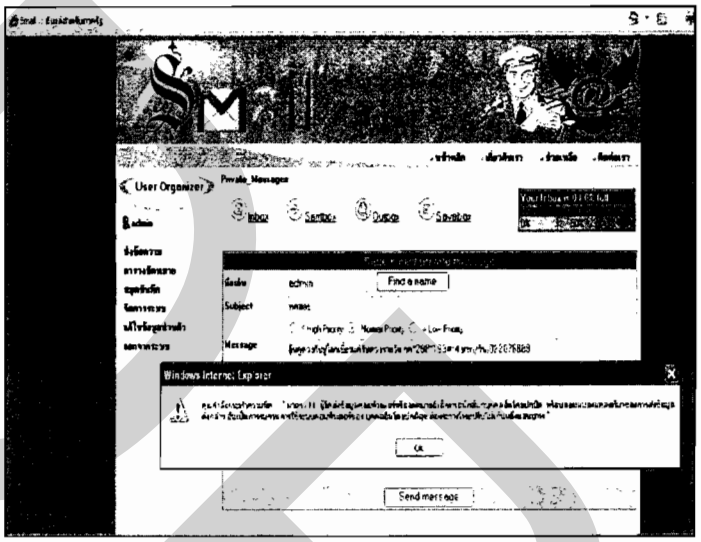



ภาพที่ 4.2 ฟอร์มส่งเมล์

4.1.4 ด้านโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam)

การทำงานในการตรวจสอบข้อความไม่เหมาะสม (Spam) ของโปรแกรมทางฝั่งเครื่องลูกข่ายนั้น เป็นแบบอัตโนมัติ เมื่อผู้ใช้ทำการกรอกข้อความครบถ้วน ระบบจะทำการประมวลผล

ข้อมูล หากตรวจพบว่าเนื้อความจดหมายดังกล่าว เข้าข่ายการกระทำความผิดกฎหมาย มาตรา 11 การส่งข้อความ Spam ระบบจะทำการบล็อกข้อความทันกล่าว พร้อมแจ้งเตือนผู้ใช้ในการกระทำความผิดนั้นทันที




ภาพที่ 4.3 ข้อความแจ้งเตือนผู้ใช้ที่กระทำความผิด

**4.2 ผลการทดสอบด้านประสิทธิภาพการทำงานของโปรแกรม**

หลังจากได้พัฒนาโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์ ได้แบ่งแนวทางในการประเมินประสิทธิภาพในมิติต่างๆ ดังนี้

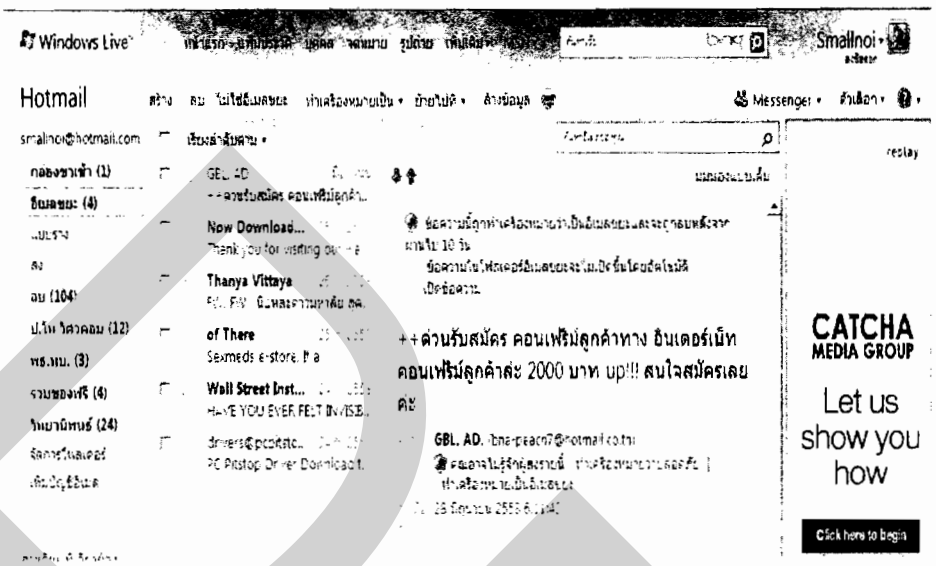
4.2.1 ทดสอบประสิทธิภาพของโปรแกรม ด้วยการเปรียบเทียบการกรองข้อความ จากเว็บเมล์ที่สร้างขึ้น กับ hotmail, gmail, yahoo และ Outlook โดยส่งข้อความจากกลุ่มตัวอย่าง จำนวน 2,000 ข้อความ ดังนี้

1) ตัวอย่างข้อมูลที่นำมาใช้เป็นกลุ่มตัวอย่าง

ข้อมูลที่นำมาเป็นกลุ่มตัวอย่างได้จากการสนับสนุนข้อมูลจากบริษัท กสท.[1] และจากอีเมลขยะของ hotmail

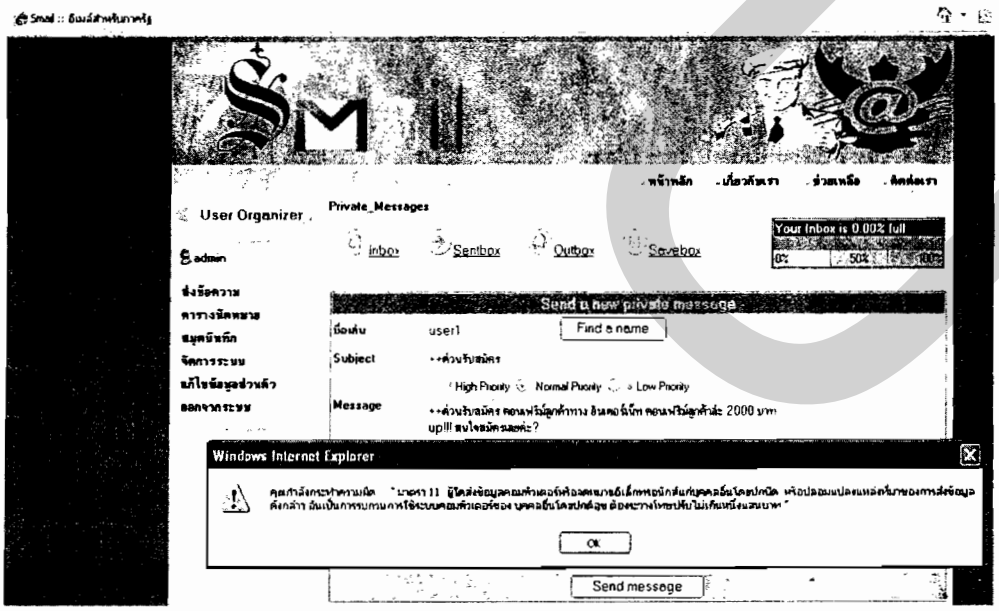
---

นนท์ บุญนิธิประเสริฐ, ชัยพร เขมะภาตะพันธ์ .(2552) **การกรองข้อความภาษาไทย และภาษาอังกฤษของบริการส่งข้อความสั้นบนเครือข่ายโทรศัพท์เคลื่อนที่**. หน้า 35




ภาพที่ 4.4 แสดงอีเมลขยะใน hotmail ที่ใช้ในการทดสอบเบื้องต้น

2) ตัวอย่างการกรองข้อความจากเว็บเมล์ที่พัฒนาขึ้น นำชุดข้อมูลตัวอย่างมาทำการทดสอบ

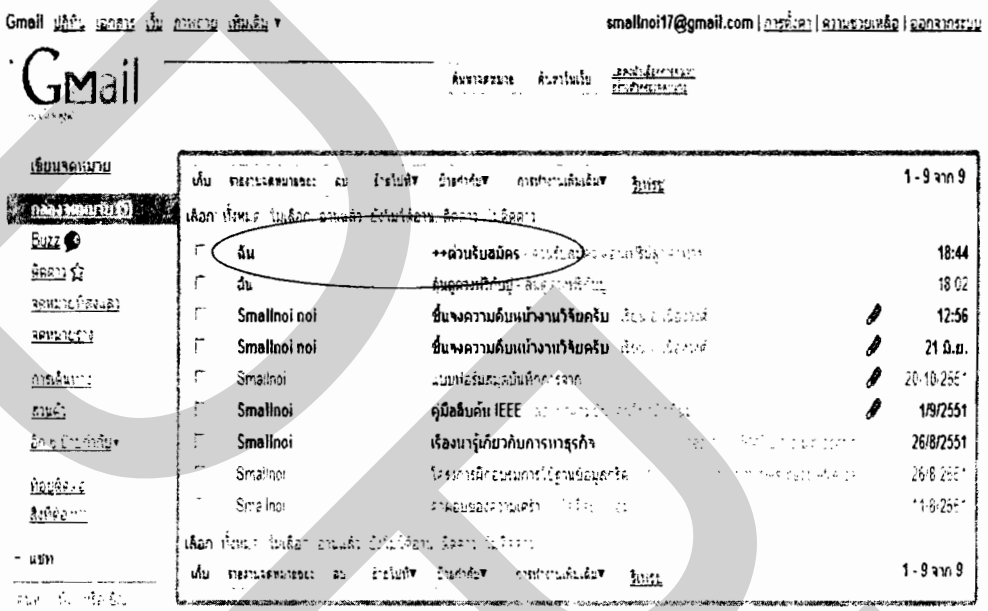



ภาพที่ 4.5 แสดงอีเมลขยะระบบ Smail ที่ใช้ในการทดสอบเบื้องต้น

ระบบสามารถกรองข้อความ Spam และทำการบล็อกข้อความดังกล่าวได้

3) ตัวอย่างการกรองข้อความจากเว็บเมล์ gmail[1]

นำชุดข้อมูลตัวอย่างมาทำการทดสอบ




ภาพที่ 4.6 แสดงอีเมลขยะใน Gmail ที่ใช้ในการทดสอบเบื้องต้น

. ระบบไม่สามารถกรองข้อความ Spam ได้

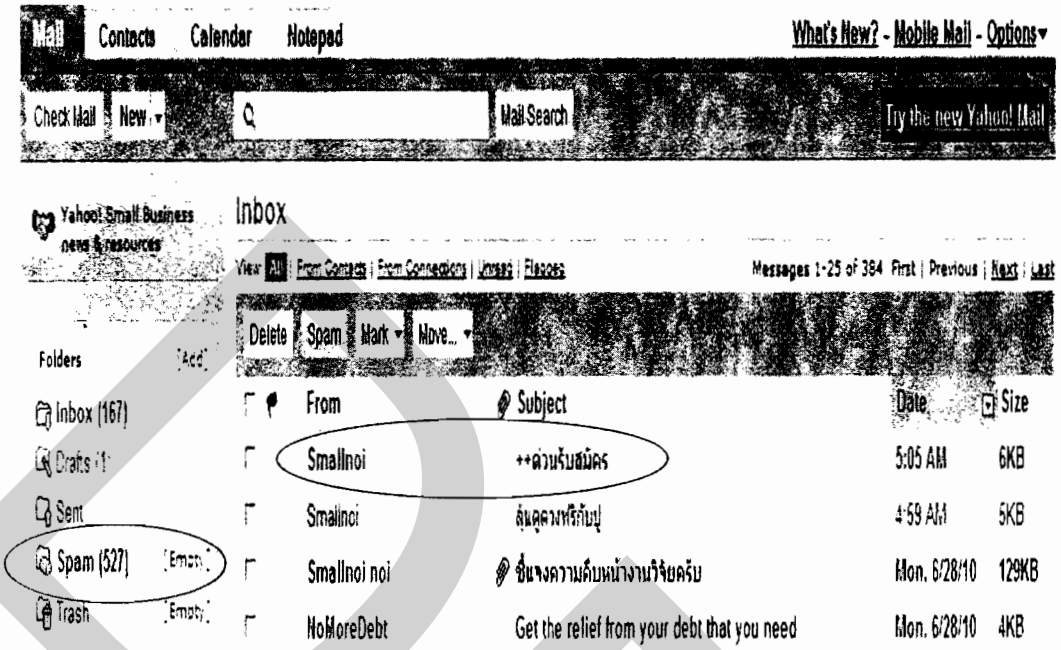
4) ตัวอย่างการกรองข้อความจากเว็บเมล์ yahoo[2]

นำชุดข้อมูลตัวอย่างมาทำการทดสอบ

---

ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ gmail.**ระบบรับ – ส่งจดหมาย.**

ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ yahoo .**ระบบรับ – ส่งจดหมาย.**



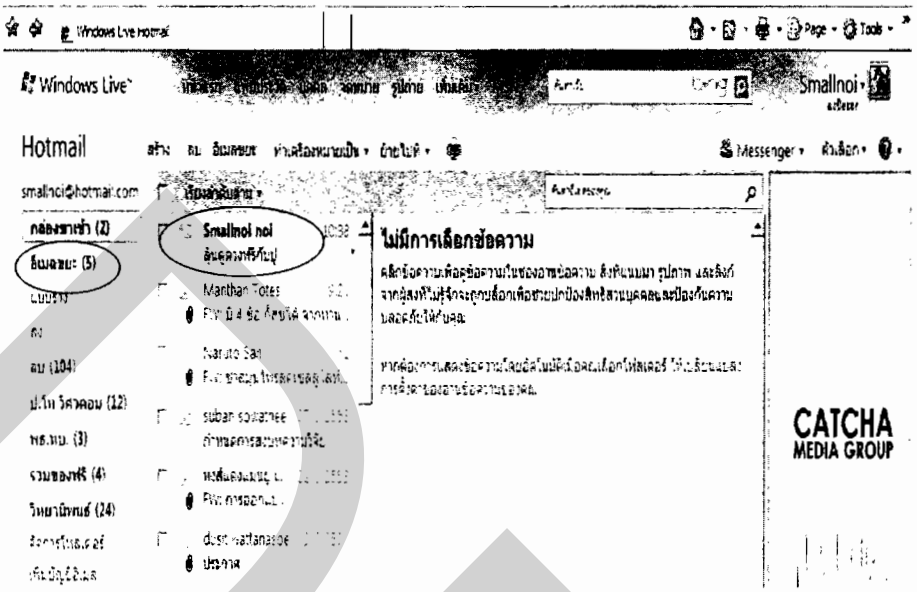

ภาพที่ 4.7 แสดงอีเมลขยะใน yahoo ที่ใช้ในการทดสอบเบื้องต้น

ระบบไม่สามารถกรองข้อความ Spam ได้

5) ตัวอย่างการกรองข้อความจากเว็บเมล์ hotmail[1]

นำชุดข้อมูลตัวอย่างมาทำการทดสอบ

[1] ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ hotmail. **ระบบรับ – ส่งจดหมาย.**




ภาพที่ 4.8 แสดงอีเมลขยะใน hotmail ที่ใช้ในการทดสอบเบื้องต้น

ระบบไม่สามารถกรองข้อความ Spam ได้

6) ผลการประเมินประสิทธิภาพของโปรแกรม ผู้วิจัยได้ทำการทดลองโดยใช้ข้อความสแปม[1] จำนวน 1,000 ข้อความและข้อความอีเมลปกติจำนวน 1,000 ข้อความ ส่งไปยังผู้ให้บริการทั้ง 5 ได้แก่ เว็บเมล์ที่ผู้วิจัยพัฒนาขึ้น(หรือ smail), hotmail, gmail, yahoo และ outlook สามารถสรุปผลได้ ดังนี้

ตารางที่ 4.2 ผลการประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่างๆ

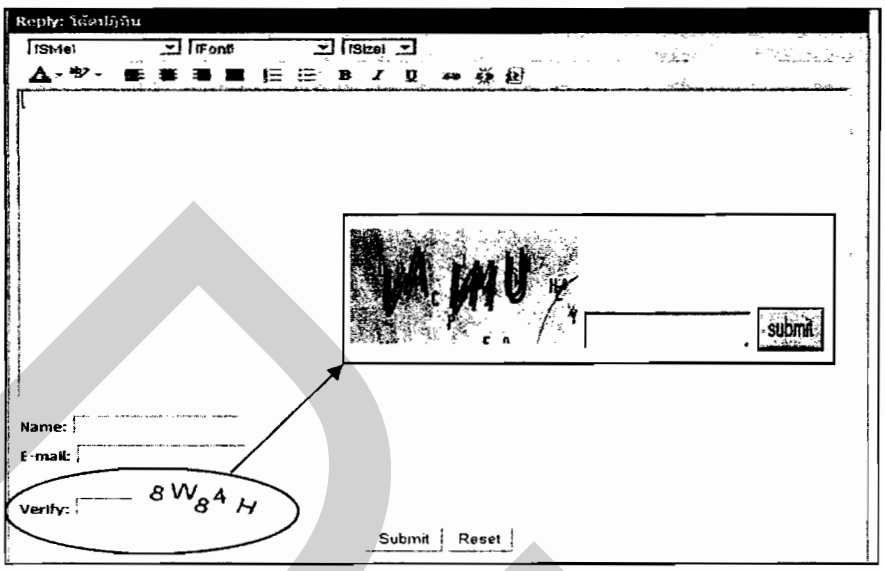
| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | จำนวนชุดข้อมูล | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) | | | | |
|---|---|---|---|---|---|---|
| | | เว็บเมล์ | hotmail | gmail | yahoo | outlook |
| ข้อความปกติ | 1000 | 1000 | 1000 | 1000 | 1000 | 1000 |
| ข้อความ Spam | 1000 | 956 | 0 | 0 | 0 | 0 |

[1] นนท์ บุญนิธิประเสริฐ, ชัยพร เขมะภาตะพันธ์.(2552) **การกรองข้อความภาษาไทย และภาษาอังกฤษของบริการส่งข้อความสั้นบนเครือข่ายโทรศัพท์เคลื่อนที่.** หน้า 35

จากผลการประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่างๆ พบว่า ผลการทดสอบสมมติฐานจากเว็บที่สร้างขึ้น กรณีที่เป็นจดหมายขยะระบบจะต้องทำการบล็อกจดหมายดังกล่าวโดยไม่ยินยอมให้ทำการส่ง แต่หากจดหมายที่ต้องการส่งเป็นจดหมายที่มีสถานะปกติ (ไม่มีข้อความที่ไม่เหมาะสม) ระบบจะทำการส่งจดหมายดังกล่าวไปยังเมล์เซิร์ฟเวอร์ เพื่อจัดส่งถึงผู้รับปลายทาง โดยเปรียบเทียบประสิทธิภาพด้วยการใช้ข้อมูลชุดเดียวกันในการทดสอบผ่านโปรแกรม Microsoft Outlook 2003, hotmail, gmail, yahoo ซึ่งไม่ว่าผู้ส่งจะทำการส่งจดหมายที่มีสถานะปกติ หรือผู้ส่งมีความประสงค์ที่จะส่งจดหมายขยะ โปรแกรม Microsoft Outlook 2003, hotmail, gmail, yahoo จะต้องยินยอมให้ส่งจดหมายดังกล่าวได้ในทุกกรณี

จากตารางพบว่า การส่งข้อความจากลุ่มตัวอย่างจำนวน 2,000 ข้อความ แบ่งเป็นข้อความปกติ จำนวน 1,000 ข้อความ และข้อความ Spam จำนวน 1,000 ข้อความ ปรากฏว่าเว็บเมล์ที่พัฒนาขึ้นสามารถส่งข้อความปกติได้ จำนวน 1,000 ข้อความ และกรองข้อความ Spam ได้จำนวน 956 ข้อความ ในขณะที่ Microsoft Outlook 2003, hotmail, gmail, yahoo นั้นทำการส่งข้อความทั้ง 2,000 ข้อความ โดยไม่สามารถบล็อกข้อความที่เป็น Spam ได้

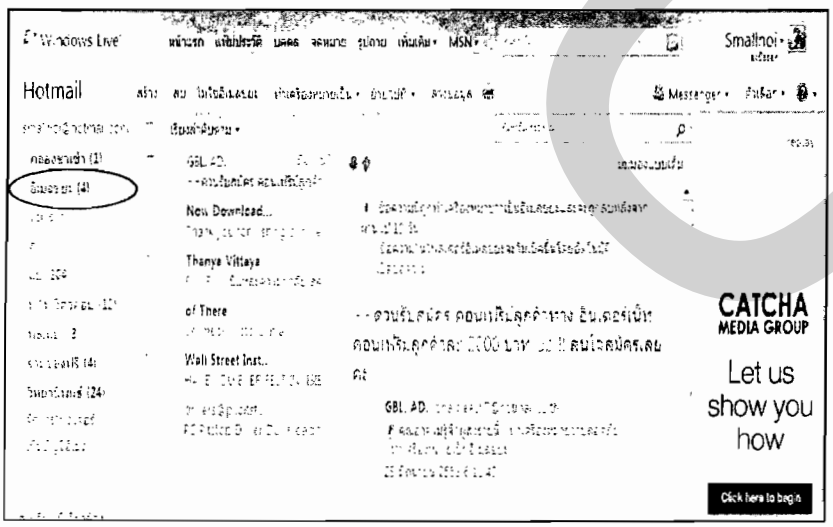
สาเหตุที่เป็นเช่นนั้นเพราะผู้ให้บริการอีเมลเหล่านั้นเน้นการป้องกันสแปมอีเมลจาก Spam Bot เท่านั้น โดยไม่สามารถป้องกันการส่งสแปมจากมนุษย์ได้ ซึ่งผู้ให้บริการอีเมลเหล่านี้เลือกใช้ลักษณะการยืนยันตัวตน คือ CAPTCHA (Completely Automated Public Turing Computer and Humans Apart)ซึ่งทำหน้าที่ตรวจสอบว่าคุณเป็นมนุษย์หรือไม่ขณะที่กำลังโพส ข้อความอยู่เพื่อป้องกัน Spam Bot เท่านั้น ดังภาพที่ 4.9




ภาพที่ 4.9 เว็บมาสเตอร์ใช้ป้องกัน Spam Bot

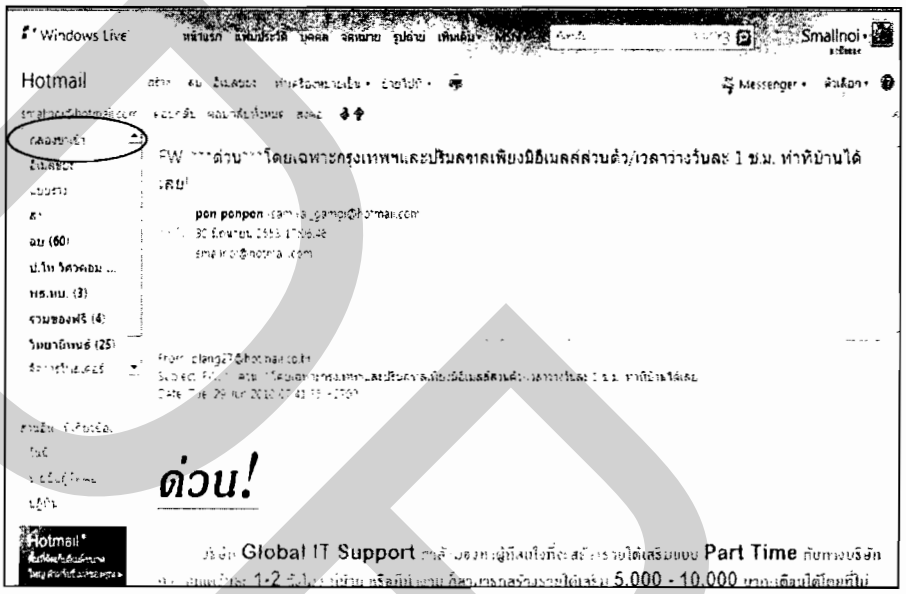
ดังนั้น งานวิจัยนี้จึงเสนอการกรอง Spam แบบอัตโนมัติที่สามารถป้องกันการส่งข้อความ Spam จากมนุษย์ได้ ซึ่งหากผู้ใช้ที่เป็นมนุษย์ทำการส่งข้อความที่เป็น Spam ระบบจะทำการบล็อกข้อความดังกล่าวทันที พร้อมแจ้งเตือนการกระทำความผิดให้ผู้ใช้รับทราบ

รูปแบบการกรอง Spam ของ Hotmail เมื่อ Hotmail ตรวจพบจดหมาย Spam จะทำการเก็บข้อมูลจดหมายดังกล่าวไว้ใน อีเมลขยะ ดังภาพที่ 4.10



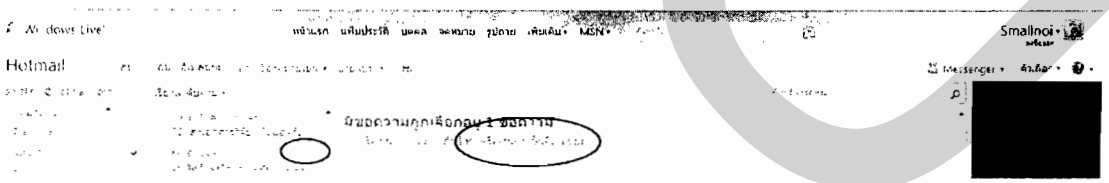

ภาพที่ 4.10 อีเมลขยะ hotmail

แม้ hotmail จะมีตัวกรอง Spam ที่มีประสิทธิภาพ แต่จดหมาย Spam บางฉบับ ตัวกรองยังคงตีความว่าเป็นจดหมายปกติ และส่งจดหมาย Spam ดังกล่าว มายังกล่องขาเข้า ดังภาพที่ 4.11




ภาพที่ 4.11 อีเมลขยะที่ hotmail กรองไม่พบ

หากตัวกรองแบบอัตโนมัติของ hotmail ไม่สามารถกรอง Spam ดังกล่าวได้ hotmail ยังมีเมนูให้ User พิจารณาและทำเครื่องหมายว่าจดหมายฉบับนั้นเป็นอีเมลขยะ ดังภาพที่ 4.12

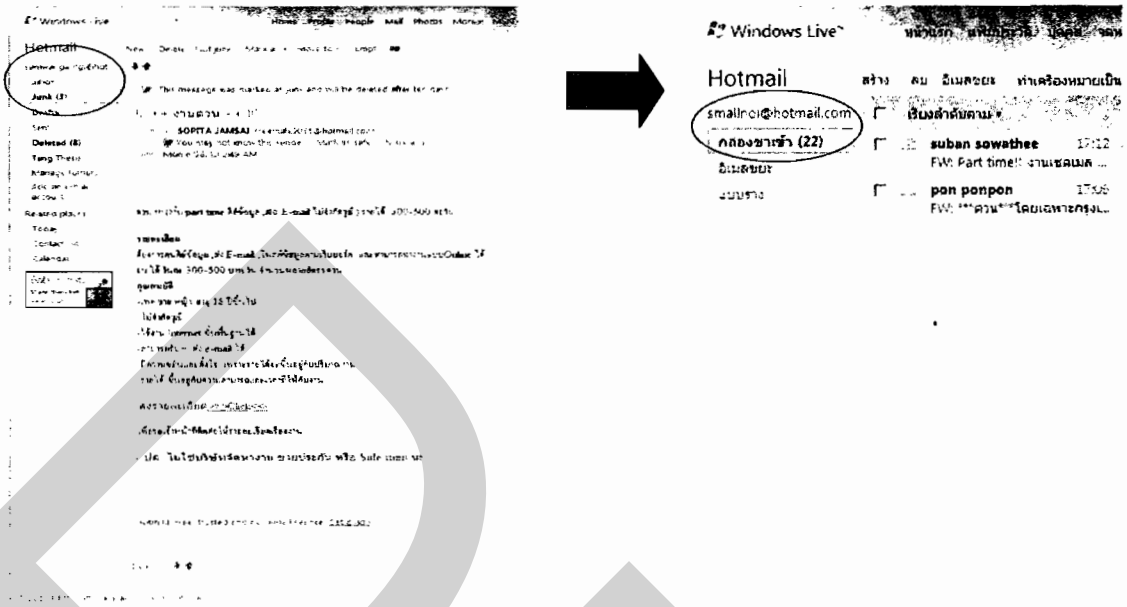



ภาพที่ 4.12 การทำเครื่องหมายอีเมลขยะ

ทำการทดสอบโดยทำเครื่องหมายอีเมลขยะของจดหมายฉบับหนึ่งที่ส่งเข้ามาเมื่อเวลา 3:55 ระบบจะนำจดหมายดังกล่าวไปไว้ยัง " อีเมลขยะ" เมื่อเวลาผ่านไป 8:59 ดังภาพที่ 4.13 ปรากฏว่าจดหมายจากผู้ส่งรายเดิมที่ทำการทำเครื่องหมายอีเมลขยะไว้ ยังคงส่งมาเป็นจดหมายปกติ

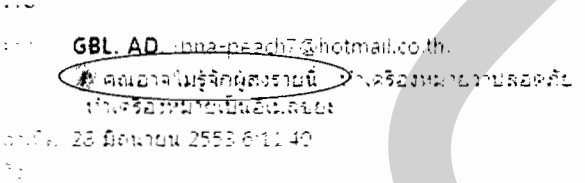

ภาพที่ 4.13 ผลจากการทำเครื่องหมายอีเมลขยะ

ทำการทดสอบสมมติฐานต่อด้วยการส่งจดหมายจากข้อความกลุ่มตัวอย่าง ได้ผลตามตารางที่ 4.2 จากนั้น ให้ผู้ช่วยวิจัยทำการส่งข้อความจากอีเมลขยะของตนมายังผู้วิจัยพบว่า จดหมายที่ส่งมาจากผู้ช่วยวิจัยถูกกรองเป็นจดหมายที่มีสถานะปกติ จดหมายที่ส่งมาถูกเก็บไว้ในจดหมายกล่องขาเข้าดังภาพที่ 4.14




ภาพที่ 4.14 การส่งข้อความขยะ hotmail ไป hotmail

จากรูปพบว่า เมื่อนำจดหมายขยะของ hotmail กลับมาส่งอีกครั้ง hotmail ไม่สามารถคัดกรองจดหมายขยะของตนได้ เนื่องจาก hotmail และเว็บในปัจจุบัน มิได้กรองที่เนื้อหาหรือข้อความของจดหมายแต่กรองที่ที่อยู่ของผู้ส่ง ดังภาพที่ 4.15




ภาพที่ 4.15 Spamfilter ของ hotmail

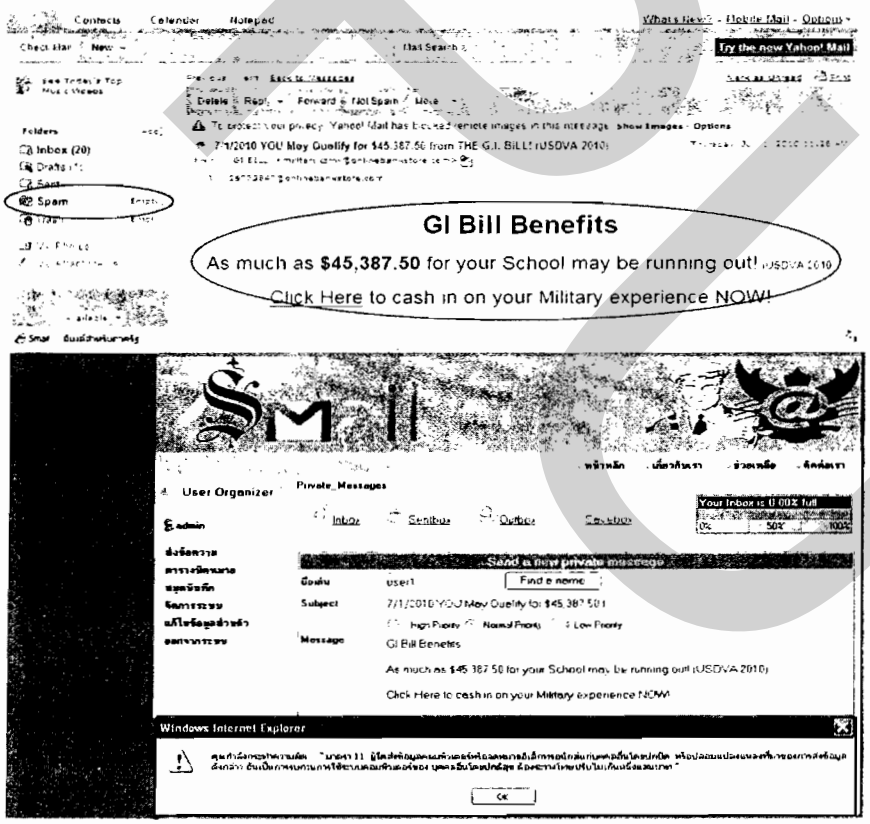
จากรูปจะเห็นได้ว่า hotmail กรอง Spam จากการตรวจสอบแหล่งที่มาของผู้ส่ง มิใช่เนื้อหาหรือข้อความในจดหมาย ผลลัพธ์ที่ได้จากการกรอง Spam ของ hotmail ดังภาพที่ 4.16

ข้อความนี้ถูกทำเครื่องหมายว่าเป็นอีเมลขยะและจะถูกลบหลังจากผ่านไป 10 วัน
ข้อความในโฟลเดอร์อีเมลขยะจะไม่เปิดขึ้นโดยอัตโนมัติ
เปิดข้อความ

ภาพที่ 4.16 ผลลัพธ์ตัวกรองสแปมของ hotmail

ทำการทดสอบสมมติฐานต่อด้วยการนำข้อมูลจากกลุ่มตัวอย่าง จำนวน 2,000 ข้อความ ทำการส่งผ่านเว็บเมล์ที่พัฒนาขึ้น พบว่าสามารถส่งจดหมายปกติได้ 1,000 ฉบับ และกรองสแปมได้ 956 ฉบับ ผลตามตารางที่ 4.2

จากนั้นทำการทดสอบด้วยการนำจดหมายขยะจาก hotmail, yahoo มาทำการทดสอบผ่านเว็บเมล์ที่พัฒนาขึ้น พบว่า สามารถกรองข้อความดังกล่าวได้ ดังภาพที่ 4.17




ภาพที่ 4.17 นำ spam จาก yahoo มากรองด้วยเว็บที่พัฒนาขึ้น

ดังนั้น จึงสรุปได้ว่า hotmail, yahoo, gmail ใช้รูปแบบการกรองแบบตรวจสอบแหล่งที่มาหรือรายชื่อผู้ส่งว่ารู้จักกับผู้รับหรือไม่ มิได้ตรวจสอบที่เนื้อหาหรือข้อความของจดหมาย ดังนั้น ถ้าผู้ช่วยวิจัยและผู้วิจัยส่งจดหมายที่มีข้อความเนื้อหาที่เป็นสแปม นั้นหมายความว่าสามารถส่งได้ดังที่กล่าวมาแล้วข้างต้น ด้วยเหตุนี้การติดตั้งระบบตรวจสอบและบล็อกข้อความสแปมที่เครื่องลูกข่ายตามที่เสนอในงานวิจัยฉบับนี้จึงสามารถช่วยลดปริมาณจดหมาย spam ปริมาณมากกว่าผู้ให้บริการจดหมายอิเล็กทรอนิกส์ทั่วไปทำได้ เพราะเนื่องจาก spammer ไม่สามารถส่งข้อความดังกล่าวได้ ดังนั้น จดหมายขยะหรือ Spam จึงไม่เกิดขึ้นในระบบ รายละเอียดผลการทดสอบตามผนวก ก ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูลที่แนบ

4.2.2 การวัดความแม่นยำและถูกต้องของตัวกรองสแปมที่พัฒนาขึ้น

ทำการวัดประสิทธิภาพด้านความแม่นยำและถูกต้องของ Spam Filter ที่พัฒนาขึ้นด้วยการทดสอบการส่งผ่านข้อมูล Spam ในระบบ จำนวน 1,000 ข้อความ สรุปผลการประเมินได้ดังแสดงในตารางที่ 4.3

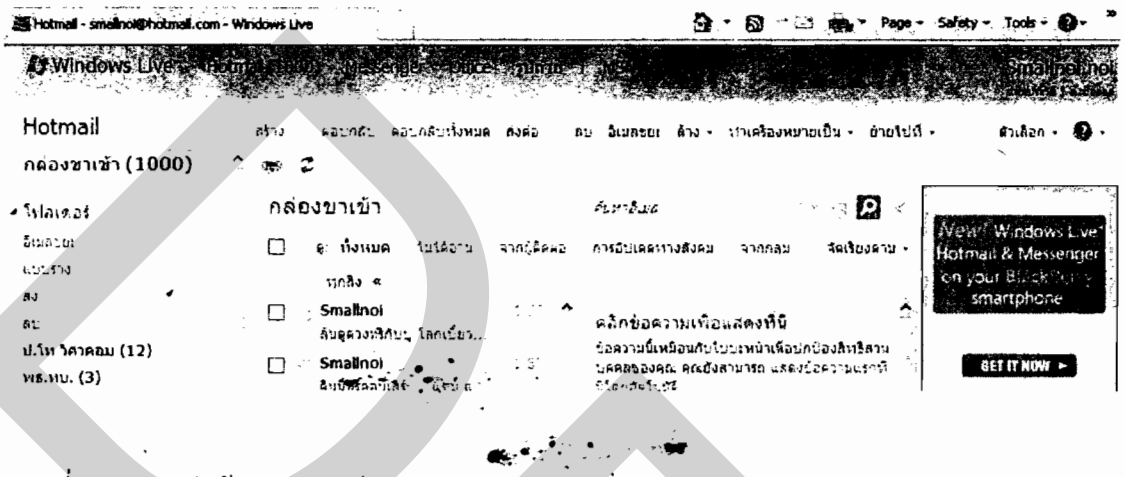
ตารางที่ 4.3 ผลการวัดความแม่นยำและถูกต้องของตัวกรองสแปมที่พัฒนาขึ้น

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | จำนวนชุดข้อมูล | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) | | | | |
|---|---|---|---|---|---|---|
| | | เว็บเมล์ | hotmail | gmail | yahoo | outlook |
| ข้อความปกติ | 1000 | 1000 | 1000 | 1000 | 1000 | 1000 |
| ข้อความ Spam | 1,000 | 956 | 0 | 0 | 0 | 0 |

ผลการทดสอบการกรองข้อความโดยวิธีการกรองข้อความด้วยการใช้ Keywords Matching ด้วยวิธีการเทียบคำในฐานข้อมูล จากตารางที่ 4.3 แสดงให้เห็นว่าระบบตรวจสอบและบล็อกสแปมที่ใช้ในงานวิจัยนี้มีความถูกต้องของการกรองข้อความสแปมเฉลี่ยที่ร้อยละ 95.6 และความถูกต้องในการกรองข้อความปกติ 100%

อย่างไรก็ตามตัวกรองสแปมอย่างง่ายที่ใช้ในงานวิจัยนี้ มีความเหมาะสม เนื่องจากสามารถใช้ได้กับทุกภาษา ใช้งานง่าย รูปแบบการเขียนโปรแกรมไม่ซับซ้อน ทั้งนี้ สิ่งสำคัญอยู่ที่วิธีการนำไปใช้ การกำหนดเงื่อนไขอย่างไร เพื่อให้ได้เงื่อนไขที่เป็นจริง ข้อความที่ต้องการมีลักษณะอย่างไร แต่ท้ายที่สุดแล้วบางครั้งก็จำเป็นที่เราจะต้องตรวจสอบด้วยตนเองอีกครั้ง อย่างไรก็ตามข้อจำกัดของตัวกรองชนิดนี้คือ หากผู้ใช้เดาลักษณะเงื่อนไขได้ ก็สามารถที่จะพิมพ์หรือกำหนด

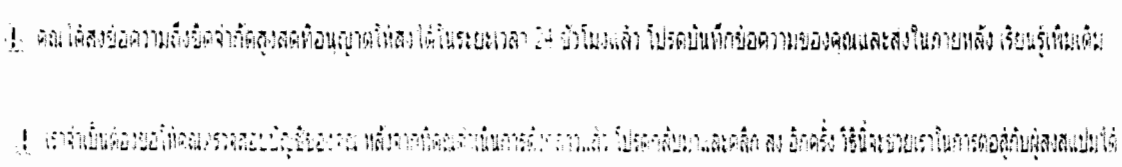
ข้อความให้ผ่านการกรองได้เหมือนกัน ดังนั้น การตรวจสอบจากมนุษย์อีกครั้งจะช่วยให้การกรองมีประสิทธิภาพมากยิ่งขึ้น




ภาพที่ 4.18 การส่งข้อความขยะไป hotmail

จากตารางที่ 4.3 แสดงผลการกรองข้อความเปรียบเทียบเว็บเมล์ที่พัฒนาขึ้นกับ hotmail, yahoo, gmail และ Outlook พบว่าข้อความที่ hotmail; yahoo, gmail กรองผิดพลาดส่วนใหญ่เกิดจากการกรองที่ที่อยู่ของผู้ส่ง มิใช่การกรองที่เนื้อหาของข้อความ ดังข้อพิจารณาที่ได้กล่าวไปในหัวข้อการประเมินประสิทธิภาพระดับผู้ให้บริการ

จากการทดสอบประสิทธิภาพด้านความถูกต้อง Spam Filter ของ hotmail พบข้อสังเกต คือ กรณีส่งข้อความ Spam จาก hotmail พบว่า hotmail ไม่สามารถบล็อกข้อความ Spam ที่กำลังส่งได้ แต่ hotmail จะยุติการส่งข้อความฝั่งเครื่องลูกข่าย กรณี User ใช้งานเกินข้อตกลงที่กำหนดไว้ ดังภาพที่ 4.19 ซึ่งไม่เกี่ยวข้องกับการกรอง Spam เลย หาก User พยายามที่จะส่งข้อความดังกล่าวต่อไป ระบบจะแสดงข้อความแจ้งเตือน User ให้ “ ตรวจสอบบัญชีของคุณ ” เพื่อยืนยันตัวตน ดังภาพที่ 4.19



ภาพที่ 4.19 Spam Filter ของ hotmail

ผลการทดสอบประสิทธิภาพด้านความถูกต้อง Spam Filter ของ gmail พบข้อสังเกตคือ กรณีที่มีจดหมายซึ่งมีแหล่งที่มาและข้อความเดียวกัน ระบบจะทำเครื่องหมายระบุจำนวนหลังหัวข้อของจดหมายฉบับดังกล่าว ดังภาพที่ 4.20 โดยไม่เพิ่มจำนวนของจดหมายกล่องขาเข้า ดังนั้น จึงสรุปได้ว่า hotmail, yahoo, gmail และ Outlook ไม่สามารถบล็อกการส่งข้อความ Spam จากผู้ส่งได้


ภาพที่ 4.20 Spam Filter ของ gmail

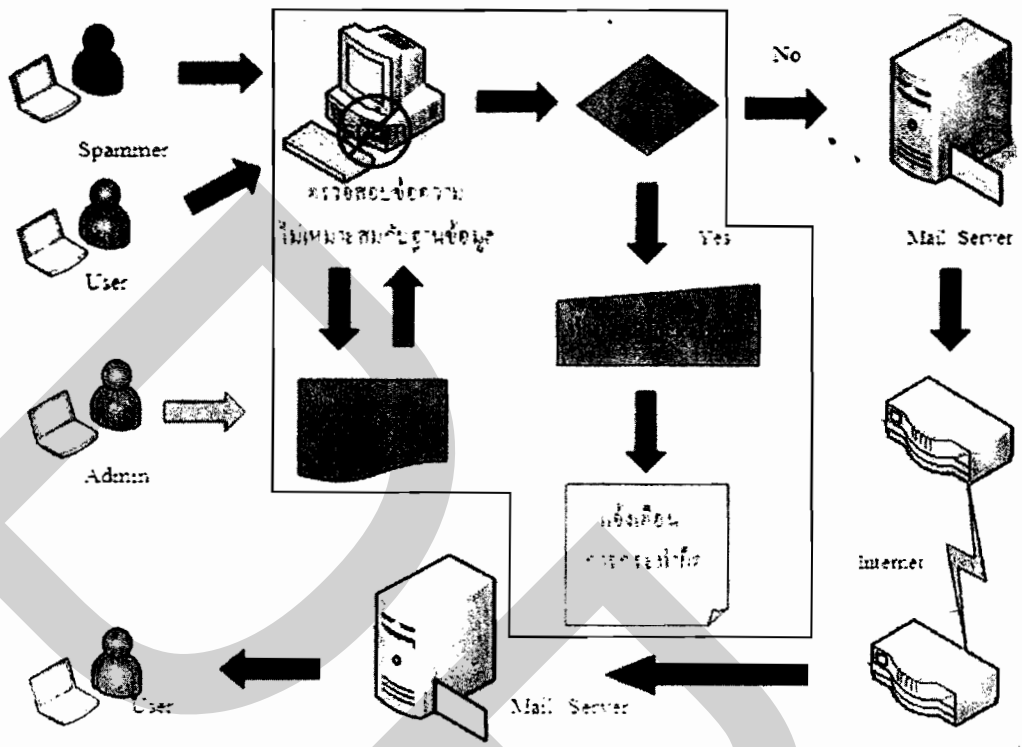
4.2.3 เปรียบเทียบผลการกรองจากการติดตั้งตัวกรองสแปมต่างสถานที่

ทำการทดสอบระบบด้วย การติดตั้งตัวกรองสแปมต่างสถานที่ที่กรมพลาธิการทหารบก จำนวน 2 ที่ด้วยกัน โดยนำตัวกรองสแปมที่พัฒนาขึ้นไปทำการติดตั้งยัง

1) เว็บบราวเซอร์ของเครื่องลูกข่าย (Client) และ

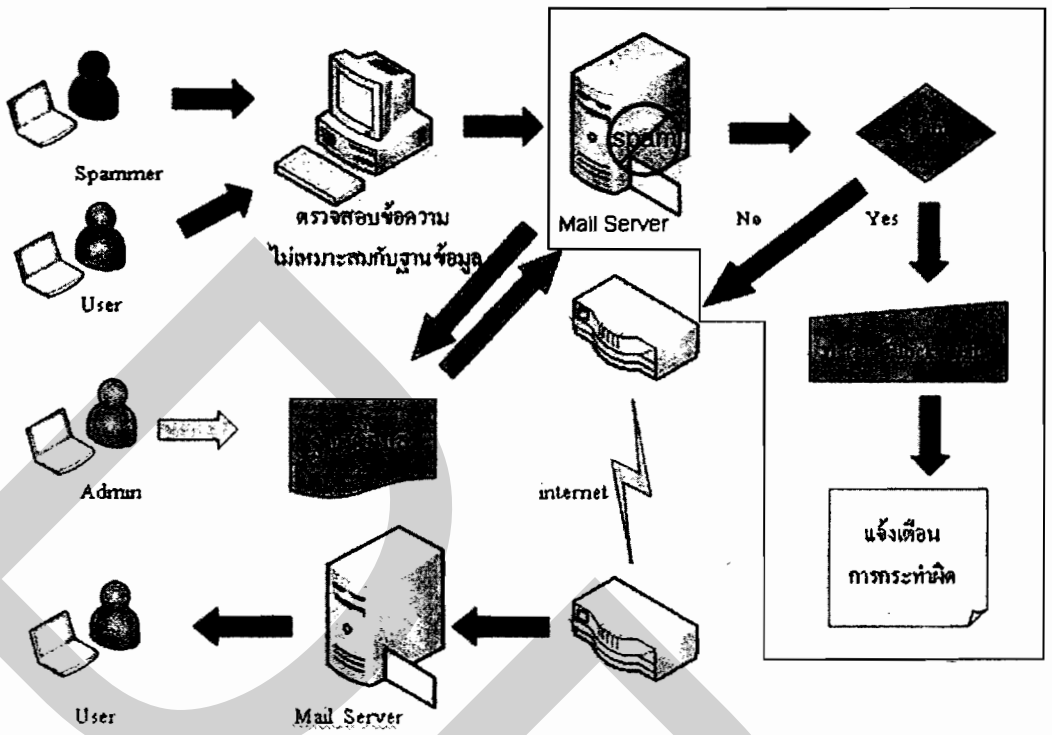
2) เครื่องแม่ข่ายผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (Mail Server)

เพื่อทำการเปรียบเทียบประสิทธิภาพของตัวกรองที่ติดตั้งต่างสถานที่ โดยพิจารณาประสิทธิภาพด้านการลดปริมาณการจราจรบนเครือข่ายเป็นหลัก ซึ่งโดยทั่วไป สามารถวัดได้จากปริมาณการจราจรที่เกิดขึ้นจริงในหน่วยของ packet ซึ่งในการทดสอบระบบนี้เราสนใจเฉพาะข้อมูลอีเมลบนเครือข่ายที่เกิดขึ้นจริง เราได้ทำการเก็บข้อมูลปริมาณการจราจรบนเครือข่ายที่มีการใช้งานจริงเป็นเวลา 4 สัปดาห์ ที่กองยุทธการและการข่าว กรมพลาธิการทหารบก โดยเครื่อง Mail Server เปิดให้บริการตามเวลาราชการ (0900–1200 น. และ 1300-1600 น.) และปิดบริการนอกเวลาราชการ




ภาพที่ 4.21 การติดตั้งตัวกรองสแปมที่ฝั่งเครื่องลูกข่าย

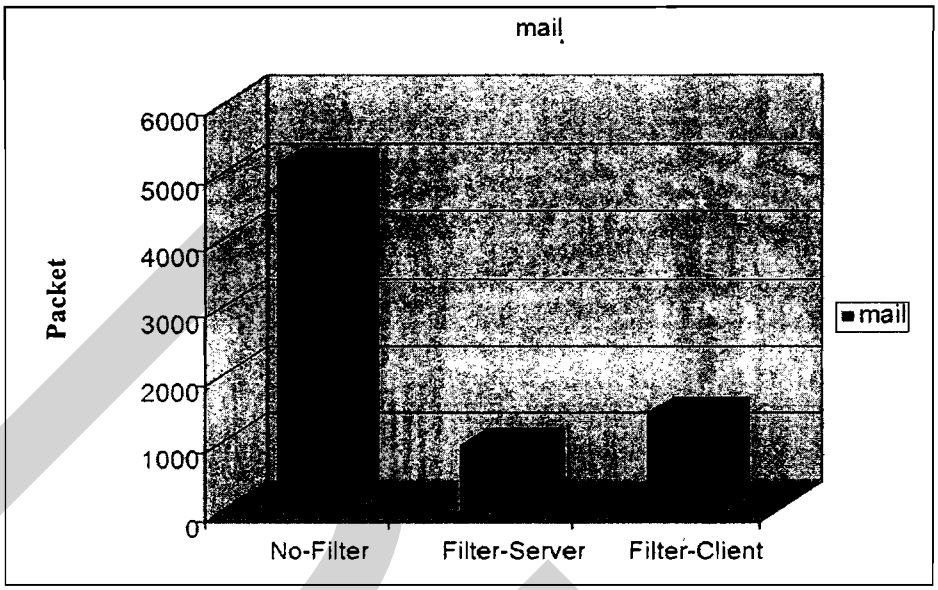
ภาพที่ 4.21 เป็นการติดตั้งตัวกรองสแปมที่ฝั่งเครื่องลูกข่าย (Client) การทำงาน คือ จะทำงานในแบบ Client – side กล่าวคือ เป็นการประมวลผลทางฝั่ง Client หรือเครื่องของ User เอง โดยฐานข้อมูลสแปมและการประมวลผลจะอยู่ที่ฝั่ง Client ซึ่งวิธีการนี้จะทำให้ลดภาระงานของ Server ลงได้อย่างมาก และเพิ่มความเร็วในการทำงานที่ Server ได้มาก แต่ข้อเสียคือ ฐานข้อมูลถูกส่งไปยังเครื่องลูกข่ายโดยการฝัง code ของฐานข้อมูลสแปมยังหน้าเว็บเมล์ ซึ่งจะทำให้ page มีขนาดใหญ่เมื่อมีฐานข้อมูลสแปมเพิ่มขึ้น




ภาพที่ 4.22 การติดตั้งตัวกรองสแปมที่ฝั่ง Server

ภาพที่ 4.22 เป็นการติดตั้งตัวกรองสแปมที่ฝั่ง Server การประมวลผลจะกระทำที่ฝั่งเซิร์ฟเวอร์ การทำงานคือ ระบบจะทำการเช็คค่าที่ส่งมาจากฟอร์มโดยการเปรียบเทียบคำกับฐานข้อมูลสแปมที่ติดตั้งยังฝั่ง Server ซึ่งเป็นการเพิ่มโหลดให้กับ Server ทำให้ Server ทำงานหนัก แต่ข้อดีของวิธีการนี้คือไม่จำกัดฐานข้อมูล และไม่เพิ่มขนาดของหน้า Page

ภาพที่ 4.23 และตาราง 4.2 ถึง 4.6 แสดงผลการทดลองในรูปแบบปริมาณข้อมูลในช่วงเวลาที่ไม่มีการติดตั้งตัวกรองสแปม (No_Filter) ช่วงที่มีการติดตั้งตัวกรองสแปมยังตำแหน่งเครื่องแม่ข่าย (Server)และติดตั้งตัวกรองยังเครื่องลูกข่าย (Client) เพื่อศึกษาถึงผลกระทบของตำแหน่งการติดตั้งตัวกรองสแปมในเครือข่ายต่อประสิทธิภาพของตัวกรองสแปม โดยเก็บปริมาณการจราจรเฉพาะข้อมูลอีเมลในแต่ละวิธี




ภาพที่ 4.23 ปริมาณการจราจรข้อมูลบนเครือข่ายในภาพรวม

จากภาพที่ 4.23 พบว่าปริมาณข้อมูลเฉพาะอีเมลในช่วงเวลาที่ไม่ติดตั้งตัวกรองสแปมมีปริมาณข้อมูลรวม 5,117 packet เมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย (Server) มีปริมาณข้อมูลเฉพาะอีเมลรวม 944 packet (คิดเป็น 18.45%) และเมื่อติดตั้งตัวกรองสแปมยังเครื่องลูกข่าย (Client) มีปริมาณข้อมูลเฉพาะอีเมลรวม 1,413 packet (คิดเป็น 27.61%) ดังนั้นตัวกรองสแปมที่ฝั่ง Client มีประสิทธิภาพต่างจากตัวกรองสแปมที่ฝั่ง Server โดยเฉลี่ยเพียง 9.21% เท่านั้น ดังแสดงในตารางที่ 4.4

ตารางที่ 4.4 ข้อมูลการจราจรเฉพาะอีเมลบนเครือข่ายแยกตามสัปดาห์

| ห้วงเก็บข้อมูล | No-Filter | Filter-Server | | Filter-Client | |
|---|---|---|---|---|---|
| สัปดาห์ที่ 1 | 1208 | 248 | 20.53% | 297 | 24.59% |
| สัปดาห์ที่ 2 | 864 | 163 | 18.87% | 269 | 31.13% |
| สัปดาห์ที่ 3 | 1623 | 291 | 17.93% | 465 | 28.65% |
| สัปดาห์ที่ 4 | 1422 | 242 | 17.02% | 382 | 26.86% |
| รวม | 5,117 | 944 | 18.45% | 1,413 | 27.61% |

จากตารางที่ 4.4 ตัวกรองจะทำการตรวจสอบแพ็คเก็ตที่ผ่านเข้า – ออกเครือข่ายว่ามีความปลอดภัยหรือไม่ หากไม่ปลอดภัยตัวกรองจะทำการตัดทิ้งแพ็คเก็ตนั้นโดยไม่ทำการส่งต่อ การตัดสินใจว่าแพ็คเก็ตใดปลอดภัยหรือไม่จะพิจารณาจากกฎที่ผู้ดูแลเป็นผู้กำหนด ซึ่งเมื่อพิจารณาแพ็คเก็ตที่เกิดขึ้นที่ฝั่ง Server พบว่ามีปริมาณแพ็คเก็ตลดลงเหลือ 944 แพ็คเก็ต โดยเราได้ทำการตรวจสอบความถูกต้องของการกรองว่ามีความผิดพลาดหรือไม่ พบว่า ในปัจจุบันยังไม่เกิดข้อผิดพลาดจากการใช้งานจริง ดังภาพที่ 4.24


ภาพที่ 4.24 ปริมาณอีเมลที่เกิดขึ้นที่ฝั่ง Server

สำหรับฝั่ง Client นั้น หากจะตรวจสอบตัวกรองจากการใช้งานจริง ว่ามีการกรองที่ผิดพลาดหรือไม่ ต้องใช้การเฝ้าดูการทำงาน (Monitor) ของระบบแบบประจำวัน ซึ่งต้องพิจารณาจาก Log Browser เพื่อดูการทำงานของ Packet ที่วิ่งผ่าน ซึ่งจะไม่สามารถมองภาพรวมของระบบได้ ดังนั้น จึงพิจารณาผลการกรองจากผู้ใช้เป็นหลัก โดยในปัจจุบันยังไม่พบข้อร้องเรียนหรือปัญหาจากการใช้งานดังกล่าว

ตารางที่ 4.5 แสดงข้อมูลการจราจรเฉพาะอีเมลบนเครือข่าย โดยแบ่งตามรายชั่วโมงที่เปิดให้บริการ เมื่อเปรียบเทียบปริมาณข้อมูลการจราจรบนเครือข่ายพบว่า ในช่วงเวลาที่มีปริมาณข้อมูลอีเมลจำนวนมาก (14.00 – 16.00 น.) ตัวกรองที่ Client ยิ่งเพิ่มความสามารถในการลดปริมาณข้อมูลที่เกิดจากสแปมลงได้ใกล้เคียงกับตัวกรองที่ติดตั้งที่ Server

ตารางที่ 4.5 ปริมาณข้อมูลอีเมลเฉลี่ยบนเครือข่าย รายชั่วโมง

| Time | no_filter | server | | Client | |
|---|---|---|---|---|---|
| 900 | 140 | 43 | 30.7% | 80 | 57.14% |
| 1000 | 701 | 125 | 17.83% | 187 | 26.68% |
| 1100 | 928 | 386 | 41.59% | 592 | 63.79% |
| 1300 | 611 | 156 | 25.53% | 245 | 40.10% |
| 1400 | 1169 | 197 | 16.85% | 272 | 23.27% |
| 1500 | 1231 | 37 | 3.01% | 37 | 3.01% |
| 1600 | 337 | 0 | | 0 | |

จากตารางที่ 4.6 แสดงข้อมูลการจราจรเฉพาะอีเมลบนเครือข่าย โดยแบ่งตามวัน (จันทร์ – ศุกร์) เมื่อเปรียบเทียบปริมาณข้อมูลการจราจรบนเครือข่ายพบว่า การติดตั้งตัวกรองสแปมที่ Client สามารถลดปริมาณข้อมูลที่เกิดจากสแปมต่อวันลงได้ใกล้เคียงกับตัวกรองที่ Server (~10%)

ตารางที่ 4.6 ปริมาณข้อมูลอีเมลเฉลี่ยบนเครือข่ายแยกตามวัน

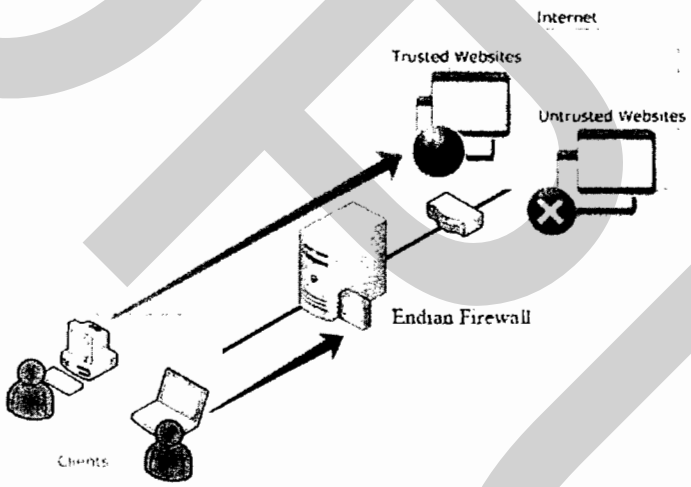
| Day | จันทร์ | อังคาร | พุธ | พฤหัส | ศุกร์ |
|---|---|---|---|---|---|
| no_filter | 1145 | 1397 | 522 | 1196 | 857 |
| Server | 203 (17.7%) | 297 (21.3%) | 38 (7.3%) | 216 (18.1%) | 190 (22.2%) |
| Client | 327 (28.6%) | 446 (31.9%) | 75 (14.4%) | 349 (29.2%) | 216 (25.2%) |

จากผลการเปรียบเทียบปริมาณข้อมูลข้างต้นแสดงให้เห็นว่า แม้ตัวกรองข้อความสแปมที่พัฒนาขึ้น จากการส่งตัวอย่างกลุ่มข้อมูลตามตารางที่ 1 จะให้ค่าความถูกต้องในการกรองเท่ากันที่ 95.6% แต่เมื่อเก็บข้อมูลการใช้งานจริง ด้วยปริมาณ Packet พบว่าการติดตั้งตัวกรองข้อความสแปมต่างสถานที่กลับให้ค่าการกรองที่แตกต่างกัน เมื่อติดตั้งตัวกรองข้อความสแปมยังเครื่องแม่ข่าย (Server) พบว่าสามารถลดปริมาณข้อมูลอีเมลลงได้เฉลี่ย 81.55 % และเมื่อติดตั้งตัว

กรองข้อความสแปมยังเครื่องลูกข่าย (Client) พบว่าสามารถลดปริมาณข้อมูลอีเมลลงได้เฉลี่ย 72.38%

ดังนั้น ตัวกรองข้อความสแปมในฝั่ง Client สามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับฝั่ง Server โดยลดภาระการทำงานที่ Serverอีกด้วย ถึงแม้ว่าในงานวิจัยนี้จะใช้ตัวอย่างตัวกรอง เป็นตัวกรองข้อความสแปมอย่างง่ายก็ตาม ด้วยเหตุนี้การติดตั้งตัวกรองข้อความสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองข้อความสแปมที่น่าสนใจในอนาคต

จากการศึกษาโปรแกรม ENDIAN FIREWALL สำหรับเก็บข้อมูลปริมาณ Traffic ขาเข้า (Incoming)และ Traffic ขาออก (Outgoing) พบว่า ความสามารถหรือคุณลักษณะโดยทั่วไปของ Endian Firewall คือ ออกแบบมาให้ประยุกต์ใช้งานกับ Server โดยมี 4 Network Interface คือ Red, Blue, Green, และ Orange ดังนี้




ภาพที่ 4.25 Network Interface

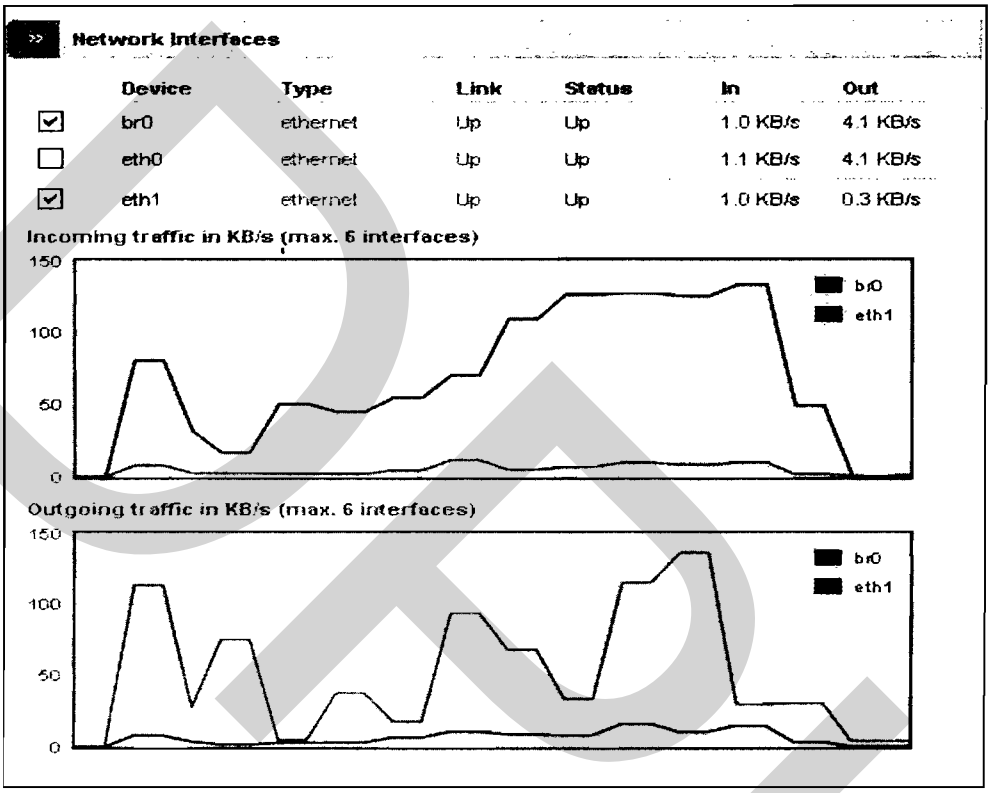
RED Network Interface เครือข่ายส่วนนี้เป็น Internet หรือ Untrusted Network หรือ Block ข้อมูล

GREEN Network Interface อินเตอร์เฟสนี้เชื่อมต่อกับคอมพิวเตอร์ภายใน หรือข้อมูลที่ได้รับอนุญาต

BLUE Network เครือข่ายส่วนนี้ให้ผู้ใช้เชื่อมต่อกับอุปกรณ์ที่เป็น Wireless

ORANGE Network เครือข่ายส่วนนี้เป็นส่วนของ DMZ ซึ่งจะเป็นพื้นที่ของ Server ชนิดต่างๆ

ซึ่งจากการเก็บข้อมูลปริมาณ Traffic ที่เกิดขึ้นจะได้รูปกราฟที่ได้ปรากฏข้อมูล 2 ส่วน คือRED Network Interface และ GREEN Network Interface ดังนี้




ภาพที่ 4.26 Network Interface Incoming-Outgoing Traffic

Incoming Traffic แสดงข้อมูลที่วิ่งเข้ามายังเมล์เซิร์ฟเวอร์ โดยเส้นสีเขียวเป็นข้อมูลที่ได้รับอนุญาตให้เข้ามา ส่วนเส้นสีแดงเป็นข้อมูลที่ไม่ได้รับอนุญาตหรือข้อมูลที่ถูก Block

Outgoing Traffic แสดงข้อมูลที่วิ่งออกจากเมล์เซิร์ฟเวอร์ โดยเส้นสีเขียวเป็นข้อมูลที่ได้รับอนุญาตให้ออกไป ส่วนเส้นสีแดงเป็นข้อมูลที่ไม่ได้รับอนุญาตหรือข้อมูลที่ถูก Block

ตารางที่ 4.7 ข้อมูล Incoming / Outgoing Traffic ครั้งที่ 1

| | เวลา | เขียว | | แดง | | รวม | | |
|---|---|---|---|---|---|---|---|---|
| | | In | Out | In | Out | In | Out | Sum |
| Client | 0900-1000 | 1.9 | 7.7 | 0.4 | 0.0 | 2.3 | 7.7 | 10 |
| | | 82.60% | 100% | 17.39% | 0% | | | |
| | 1100-1200 | 1.6 | 25.4 | 0.0 | 0.0 | 1.6 | 25.4 | 27 |
| | | 100% | 100% | 0% | 0% | | | |
| | 1300-1400 | 16 | 23.2 | 7.2 | 2.6 | 23.2 | 25.8 | 49 |
| | | 68.96% | 89.92% | 31.03% | 10.07% | | | |
| | 1500-1600 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | | 78.57% | 100% | 21.42% | 0% | | | |
| Server | 0900-1000 | 2.2 | 7.2 | 0.6 | 0.0 | 2.8 | 7.2 | 10 |
| | | 78.57% | 100% | 21.42% | 0% | | | |
| | 1100-1200 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1300-1400 | 11.1 | 21.6 | 9.2 | 3.1 | 20.3 | 24.7 | 45 |
| | | 54.67% | 87.44% | 45.32% | 12.55% | | | |
| | 1500-1600 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |

ตารางที่ 4.8 ข้อมูล Incoming / Outgoing Traffic ครั้งที่ 2

| | เวลา | เขียว | | แดง | | รวม | | |
|---|---|---|---|---|---|---|---|---|
| | | In | Out | In | Out | In | Out | Sum |
| Client | 0900-1000 | 2.0 | 25.6 | 0.4 | 0.0 | 2.4 | 25.6 | 28 |
| | | 83.33% | 100% | 16.66% | 0% | | | |
| | 1100-1200 | 6.4 | 18.6 | 0.0 | 0.0 | 6.4 | 18.6 | 25 |
| | | 100% | 100% | 0% | 0% | | | |
| | 1300-1400 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1500-1600 | 6.3 | 9.7 | 18 | 3 | 24.3 | 12.7 | 37 |
| | | 25.92% | 76.37% | 74.07% | 23.62% | | | |
| Server | 0900-1000 | 1.3 | 3.0 | 0.6 | 0.1 | 1.9 | 3.1 | 5 |
| | | 68.42% | 96.77% | 31.57% | 3.22% | | | |
| | 1100-1200 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1300-1400 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1500-1600 | 5.5 | 9.9 | 18.8 | 2.8 | 24.3 | 12.7 | 37 |
| | | 22.63% | 77.95% | 77.36% | 22.04% | | | |

ตารางที่ 4.9 ข้อมูล Incoming / Outgoing Traffic ครั้งที่ 3

| | เวลา | เขียว | | แดง | | รวม | | |
|---|---|---|---|---|---|---|---|---|
| | | In | Out | In | Out | In | Out | Sum |
| Client | 0900-1000 | 4.0 | 0.0 | 15 | 0.0 | 19 | 0.0 | 19 |
| | | 21.05% | 0% | 78.94% | 0% | | | |
| | 1100-1200 | 5.0 | 13.8 | 4.9 | 3.3 | 9.9 | 17.1 | 27 |
| | | 50.50% | 80.70% | 49.49% | 19.29% | | | |
| | 1300-1400 | 5.4 | 30.8 | 17.8 | 2.0 | 23.2 | 32.8 | 56 |
| | | 23.27% | 93.90% | 76.72% | 6.09% | | | |
| | 1500-1600 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| Server | 0900-1000 | 6.3 | 9.7 | 18 | 3 | 24.3 | 12.7 | 37 |
| | | 25.92% | 76.37% | 74.07% | 23.62% | | | |
| | 1100-1200 | 5.0 | 10.6 | 5.4 | 4.0 | 10.4 | 14.6 | 25 |
| | | 48.07% | 72.60% | 51.92% | 27.39% | | | |
| | 1300-1400 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1500-1600 | 6.3 | 9.9 | 18.4 | 2.4 | 24.7 | 12.3 | 37 |
| | | 25.50% | 80.48% | 74.49% | 19.51% | | | |

ตารางที่ 4.10 ข้อมูล Incoming / Outgoing Traffic ครั้งที่ 4

| | เวลา | เขียว | | แดง | | รวม | | |
|---|---|---|---|---|---|---|---|---|
| | | In | Out | In | Out | In | Out | Sum |
| Client | 0900-1000 | 6.0 | 6.0 | 0.3 | 1.7 | 6.3 | 7.7 | 14 |
| | | 95.23% | 77.92% | 4.76% | 22.07% | | | |
| | 1100-1200 | 9.9 | 13.8 | 0.0 | 3.3 | 9.9 | 17.1 | 27 |
| | | 100% | 80.70% | 0% | 19.29% | | | |
| | 1300-1400 | 15.8 | 24.01 | 5.2 | 0.9 | 21.0 | 25.0 | 46 |
| | | 75.23% | 96.04% | 24.76% | 3.6 | | | |
| | 1500-1600 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| Server | 0900-1000 | 4.0 | 2.4 | 0.6 | 2.0 | 4.6 | 4.4 | 9 |
| | | 86.95% | 54.54% | 13.04% | 45.45% | | | |
| | 1100-1200 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |
| | 1300-1400 | 12.0 | 20.0 | 6.4 | 1.6 | 18.4 | 21.6 | 40 |
| | | 65.21% | 92.59% | 34.78% | 7.40% | | | |
| | 1500-1600 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| | | 0% | 0% | 0% | 0% | | | |

# บทที่ 5
# สรุปผลและข้อเสนอแนะ

งานวิจัยนี้ต้องการศึกษาผลกระทบของตำแหน่งการติดตั้งตัวกรองสแปมในเครือข่ายต่อประสิทธิภาพของตัวกรองสแปม โดยมีวัตถุประสงค์เพื่อออกแบบสถาปัตยกรรมการกรองข้อความสแปมที่สามารถลดปริมาณการส่งข้อมูลในเครือข่าย และเพื่อออกแบบสถาปัตยกรรมการกรองข้อความสแปมที่มีความถูกต้องสูง ดังมีรายละเอียดต่อไปนี้

## 5.1 สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ได้ทำการพัฒนาระบบเว็บเมล์สำหรับที่กองยุทธการและการข่าวกรม พลาธิการทหารบก และติดตั้งตัวกรองข้อความสแปมจากการประเมินประสิทธิภาพของตัวอย่างตัวกรองสแปมอย่างง่าย พบว่าเมื่อทำการส่งข้อมูลทดสอบไปยังตัวกรองสแปมอย่างง่าย พบว่ามีความถูกต้องของการกรองข้อความสแปมเฉลี่ยที่ 95.6 % และมีความถูกต้องในการกรองข้อความปกติ 100 % และเมื่อเก็บข้อมูลการใช้งานจริงเป็นเวลา 4 สัปดาห์ด้วยปริมาณการจราจรข้อมูล Packet อีเมลพบว่าเมื่อติดตั้งตัวกรองข้อความสแปมที่เครื่องลูกข่ายสามารถลดปริมาณการจราจรลงได้ถึง 72.38 % ในขณะเดียวกัน เมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย ตัวกรองสแปมสามารถลดปริมาณการจราจรลงได้ถึง 81.55 % ดังนั้น ตัวข้อความกรองสแปมในฝั่งลูกข่ายสามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับฝั่งแม่ข่ายและเป็นการลดการทำงานที่ ฝั่งแม่ข่ายอีกด้วย ซึ่งอาจทำการติดตั้งตัวกรองได้โดยการรวมตัวกรองสแปมในตัวติดตั้งเบราว์เซอร์โดยปริยายเพื่อป้องกันผู้ใช้ถอดตัวกรองสแปมออกเอง และทำให้สามารถแจกจ่ายและติดตั้งโปรแกรมตัวกรองแก่เครื่องคอมพิวเตอร์จำนวนมากในหน่วยงานใหญ่ได้ง่ายด้วยเหตุนี้ การติดตั้งตัวกรองข้อความสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองข้อความสแปมที่น่าสนใจในอนาคต ทั้งนี้ เพื่อให้ระบบเกิดประสิทธิภาพและเกิดประโยชน์สูงสุด ควรมีการพัฒนาต่อดังนี้

5.1.1 โปรแกรมควรมีการเชื่อมโยงกับฐานข้อมูลคำไม่เหมาะสมของสำนักงานตำรวจแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือหน่วยงานอื่นใดที่รับผิดชอบด้านนี้ เพื่อเป็นการใช้ฐานข้อมูลกลางร่วมกัน ลดความซ้ำซ้อน ประหยัดทรัพยากรและงบประมาณ

5.1.2 โปรแกรมควรมีระบบป้องกันรูปภาพ หรือสื่ออนาจาร เช่น การกรองภาพไม่เหมาะสม

5.1.3 โปรแกรมควรมีระบบตรวจสอบคำผิดหรือแสลง[1] ด้วยการแทนที่กลุ่มคำที่ถูกต้อง เพื่อลดปริมาณ Spam ที่อาจเกิดขึ้นในระบบ



---

ราชบัณฑิตยสถาน.ราชบัณฑิต ฯ ค้าน « โปสกวน» เผยคำดิบหวั่นเป็นแฟชั่น. หน้า 1-2

# บรรณานุกรม

# บรรณานุกรม

## ภาษาไทย


### บทความ

ยุทธนา ชื่นจิตร. (2548). "ระบบการส่งอีเมล์ตอบกลับ." **Reply E-mail System (มหาวิทยาลัยรังสิต).** หน้า 56

อติชาต ขานทอง, วัลลภา ตันติประสงค์ชัย และ ชุลีรัตน์ จรัสกุลชัย. (2544). " การจัดกลุ่มเอกสารข้อความภาษาไทยแบบอัตโนมัติโดยใช้เศษของคำ." **Document Summarization**. หน้า 1-3.

อรรยา สิงห์สงบ, (2546). " ความพยายามทางกฎหมายกับการแก้ไขปัญหาจดหมายอิเลคทรอนิกส์ขยะ." **สาร Nectec ฉบับที่ 55 พฤศจิกายน - ธันวาคม 2546.** หน้า 9-10

### วิทยานิพนธ์

กอบเกียรติ สระอุบล และ เบญจพร ลิ้มธรรมาภรณ์ (2552). **การกรองสแปมบอทเน็ต.** วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์. กรุงเทพ ฯ : มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ.

นนท์ บุญนิธิประเสริฐ และ ชัยพร เขมะภาตะพันธ์. (2552). **การกรองข้อความภาษาไทย และภาษาอังกฤษของบริการส่งข้อความสั้นบนเครือข่ายโทรศัพท์เคลื่อนที่.** วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม. กรุงเทพ ฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์

### สารสนเทศจากสื่ออิเล็กทรอนิกส์

บริษัท เวิลด์ ไซเบอร์ เซอร์วิส จำกัด. Anti Spam ระบบป้องกันอีเมล์ขยะ. สืบค้นเมื่อ 22 มกราคม 2554 จาก **http://www.wcs.co.th/antispam.php**

บริษัท Microsoft .Microsoft report . สืบค้นเมื่อ 18 มกราคม 2554 จาก **http://www.microsoft.com/security/sir/**

ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ hotmail.ระบบรับ-ส่งจดหมาย.สืบค้นเมื่อ15 กันยายน 2553 จาก **www.hotmail.com**

ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ yahoo. ระบบรับ-ส่งจดหมาย. สืบค้นเมื่อ 15 กันยายน 2553 จาก **www.yahoo.com**

ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ gmail. ระบบรับ-ส่งจดหมาย. สืบค้นเมื่อ 15 กันยายน 2553 จาก **www.gmail.com**

รัฐบาลไทย. (2550). ผลการประชุมคณะรัฐมนตรีประจำวันที่ 18 ธันวาคม 2550 . สืบค้นเมื่อ 1 กันยายน 2553. จาก **www.thaigov.go.th**

ราชบัณฑิตยสถาน. ราชบัณฑิต ฯ ค้าน " โปสกวน" เผยคำดิบหวั่นเป็นแฟชั่น. สืบค้นเมื่อ 17 กันยายน 2553 จาก **http://news.swu.ac.th/newsclips/doc/200811757.pdf**

สำนักงานปลัดกระทรวง. (2550). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. สืบค้นเมื่อ 1 กันยายน 2553. จาก **http://www.mict.go.th/ewt_news.php?nid=345&filename=index**

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ.(2550).โครงการระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ. สืบค้นเมื่อ 8 ตุลาคม 2553 จาก **http://www.gits.net.th/index.asp**

nectec. Digital Signature.สืบค้นเมื่อ 22 มกราคม 2554 จาก **wiki.nectec.or.th/ngiwiki/pub/Main/digital_signature.doc**

**ภาษาต่างประเทศ**

**ARTICLES**

David E. Sorkin.(2001). "Technical and Legal Approaches to Unsolicited Electronic Mail." **UNIVERSITY OF SAN FRANCISCO LAW REVIEW 35.** U.SF.L.REV.325. p.3

Gary S. Moorefield.(1999). " Note-SPAM It's not Just for breakfast Anymore Anymore: Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-Mail." **Unsolicited Commercial E-Mail.** 5 B.U.J.SCI.&TECH.L.10. p.1

Gordon V. Cormack, Jose Maria Gomez Hidalgo, Enrique Puertas Sanz. (2007). " Spam filtering for short messages." **CIKM'07.** p.1-4.

István Pilászy (2005) "Text Categorization and Support Vector Machines." **Machine Learning.** p.1-9.

James F. Kurose and Keith W.Ross.(2003). " A Top-Down Approach Featuring the Internet. 2nd : Pearson Addison-Wesley." **Computer Networking** p.6

Jennifer M. Kappel.(1999). " Note and Comments -Government Intervention on the Internet: Should the Federal Trade Commission Regulate Unsolicited E-mail Advertising." **ACM.** p.5

S. Dixit, S. Gupta, and C.V. Ravishankar. (2005). "LOHIT: An Online Detection & Control System for Cellular SMS Spam." **IASTED International.** November 14-16. p.2-8.

## ELECTRONIC SOURCES

Fidelis Assis. (2006). OSBF-Lua, Text classification module for the Lua Programming Language and a production class anti-spam in Lua using the module. Retrieved April 14, 2007, from **http://osbf-lua.luaforge.net/**

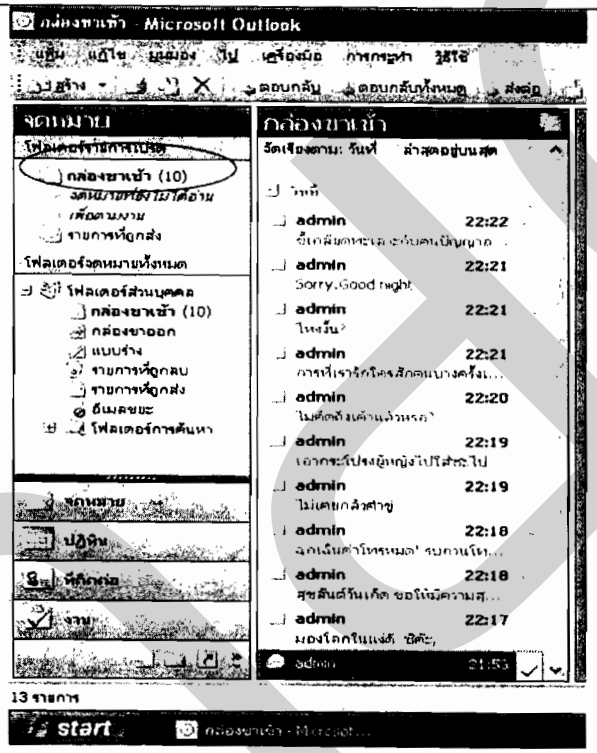
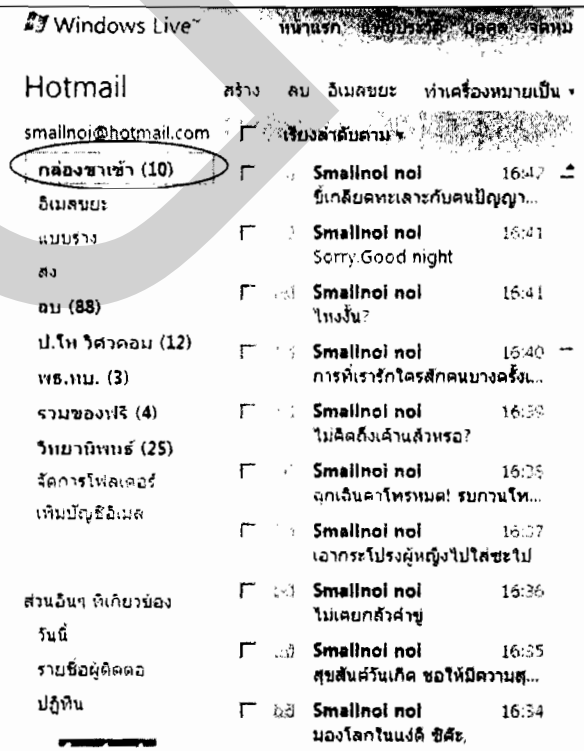
WebGate JSC. (2007). SMS Spam Manager. Retrieved December 18, 2007, from **http://www.webgate.bg/products/ssm/**

# ภาคผนวก

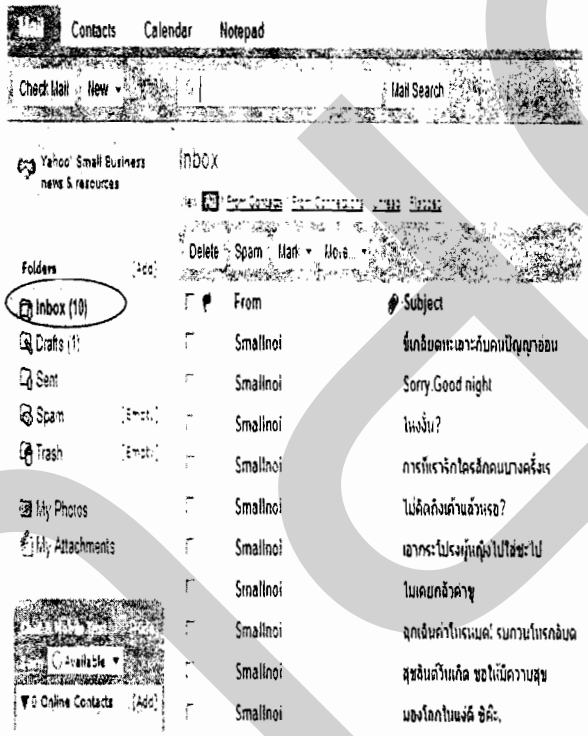
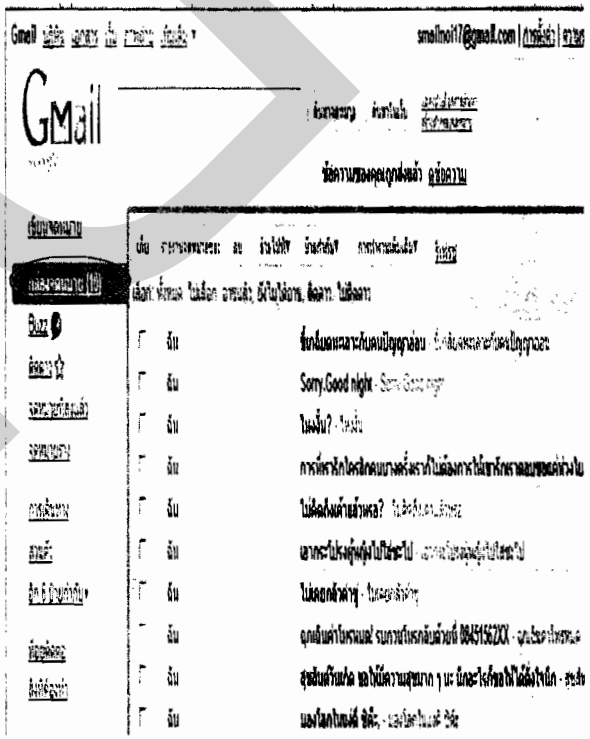
# ภาคผนวก ก

## ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูลโปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมล์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์

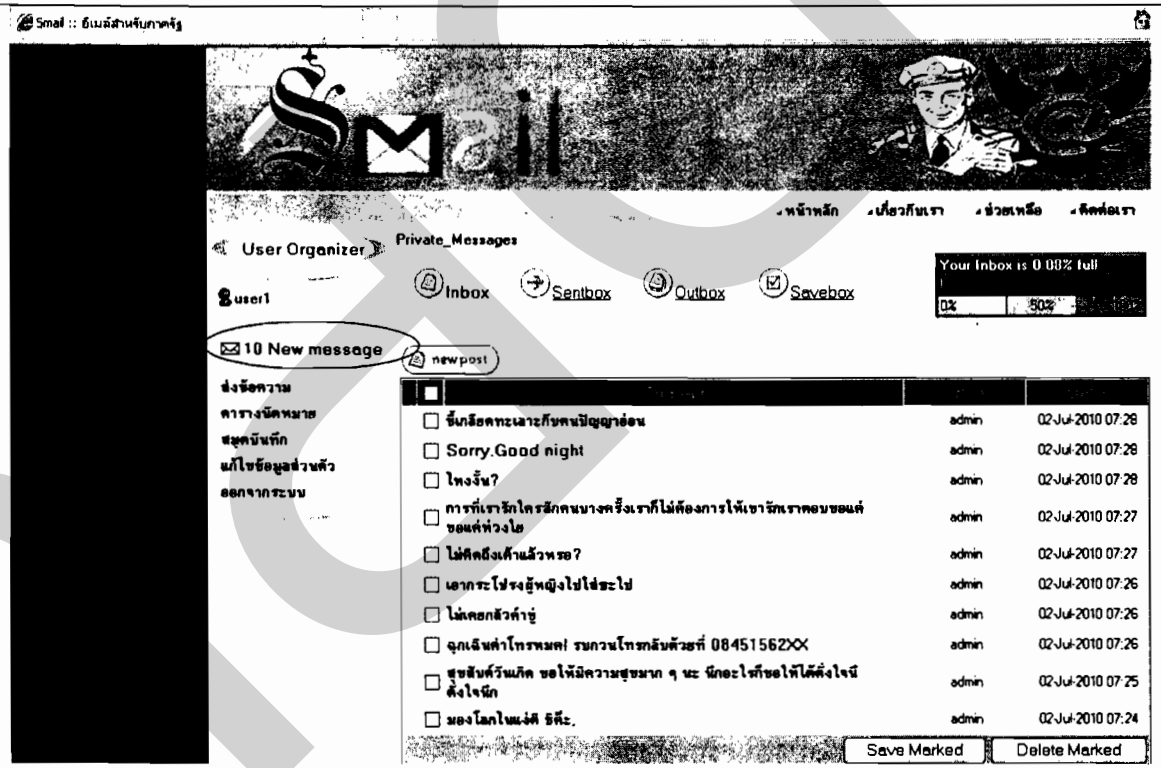
ตารางที่ ก-1 ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (ปกติ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) | |
|---|---|---|---|
| | | Outlook | hotmail |
| มองโลกในแง่ดี ชิคิะ, | ปกติ |  |  |
| สุขสันต์วันเกิด ขอให้มีความสุขมาก ๆ นะ นึกอะไรก็ขอให้ได้ดั่งใจนึก | | | |
| ฉุกเฉินค่าโทรหมด! รบกวนโทรกลับด้วยที่ 08451562XX | | | |
| ไม่เคยกลัวคำขู่ | | | |
| เอากระโปรงผู้หญิงไปใส่ซะไป | | | |
| ไม่คิดถึงเค้าแล้วหรอ? | | | |
| การที่เรารักใครสักคนบางครั้งเราก็ไม่ต้องการให้เขารักเราตอบขอแค่ห่วงใย | | | |
| ไหงงั้น? | | | |
| Sorry.Good night | | | |
| ขี้เกลียดทะเลาะกับคนปัญญาอ่อน | | | |
| สรุปภาพรวม | | ส่งได้ 10 ข้อความ | ส่งได้ 10 ข้อความ |

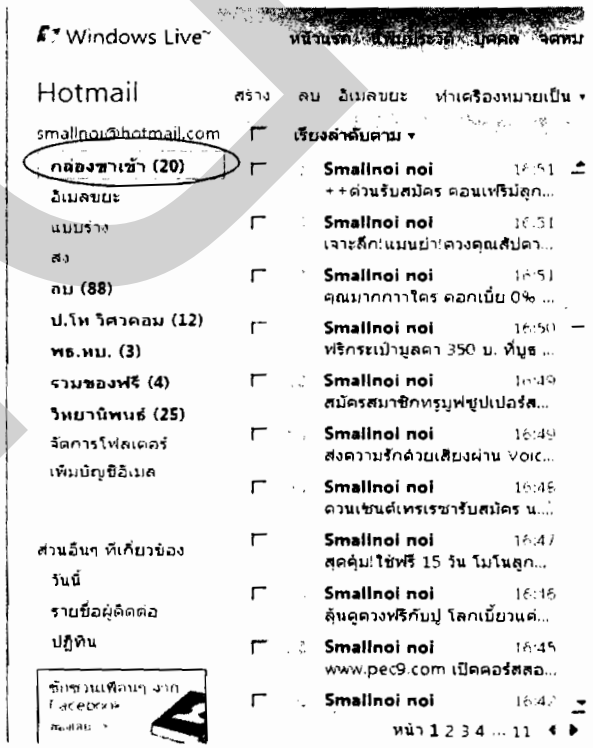
**ตารางที่ ก-1** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (ปกติ) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) | |
|---|---|---|---|
| | | Yahoo | gmail |
| มองโลกในแง่ดี ซิคะ, | ปกติ |  |  |
| สุขสันต์วันเกิด ขอให้มีความสุขมาก ๆ นะ นึกอะไรก็ขอให้ได้ดั่งใจนึก | | | |
| ฉุกเฉินค่าโทรหมด! รบกวนโทรกลับด้วยที่ 08451562XX | | | |
| ไม่เคยกลัวคำขู่ | | | |
| เอากระโปรงผู้หญิงไปใส่ซะไป | | | |
| ไม่คิดถึงเค้าแล้วหรอ? | | | |
| การที่เรารักใครสักคนบางครั้งเราก็ไม่ต้องการให้เขารักเราตอบขอแค่ห่วงใย | | | |
| ไหงงั้น? | | | |
| Sorry.Good night | | | |
| ขี้เกลียดทะเลาะกับคนปัญญาอ่อน | | | |
| สรุปภาพรวม | | ส่งได้ 10 ข้อความ | ส่งได้ 10 ข้อความ |

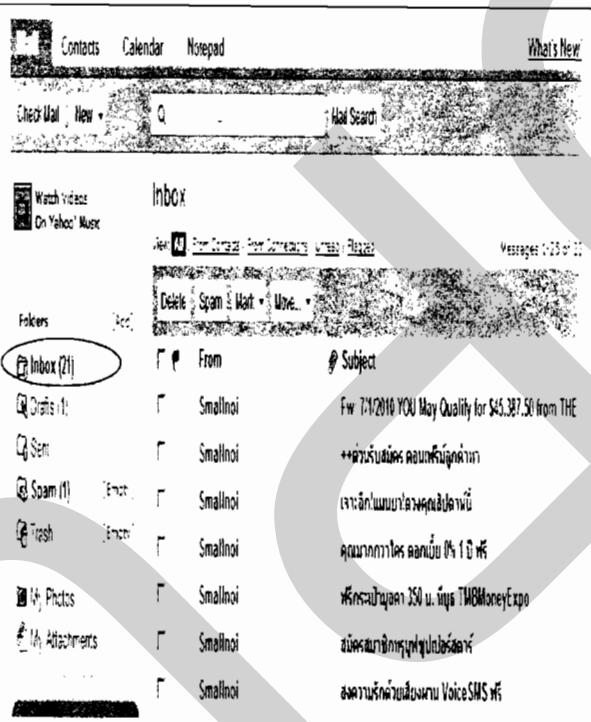
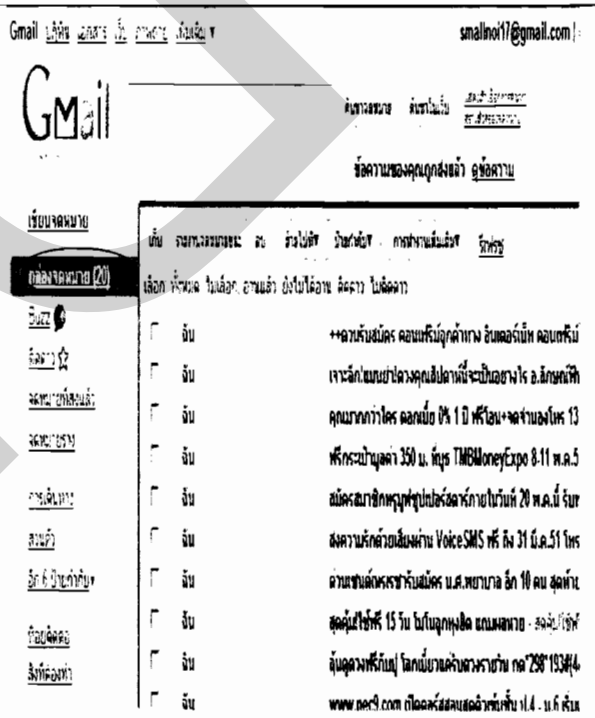
**ตารางที่ ก-1** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (ปกติ) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| มองโลกในแง่ดี ชิคิ๊ะ, | ปกติ |  |
| สุขสันต์วันเกิด ขอให้มีความสุขมาก ๆ นะ นึกอะไรก็ขอให้ได้ดั่งใจนึก | | |
| ฉุกเฉินค่าโทรหมด!รบกวนโทรกลับด้วยที่ 08451562XX | | |
| ไม่เคยกลัวคำขู่ | | |
| เอากระโปรงผู้หญิงไปใส่ซะไป | | |
| ไม่คิดถึงเค้าแล้วหรอ? | | |
| การที่เรารักใครสักคนบางครั้งเราก็ไม่ต้องการให้เขารักเราตอบขอแค่ห่วงใย | | |
| ไหงงั้น? | | |
| Sorry.Good night | | |
| ขี้เกลียดทะเลาะกับคนปัญญาอ่อน | | |
| สรุปภาพรวม | | ส่งได้ 10 ข้อความ |

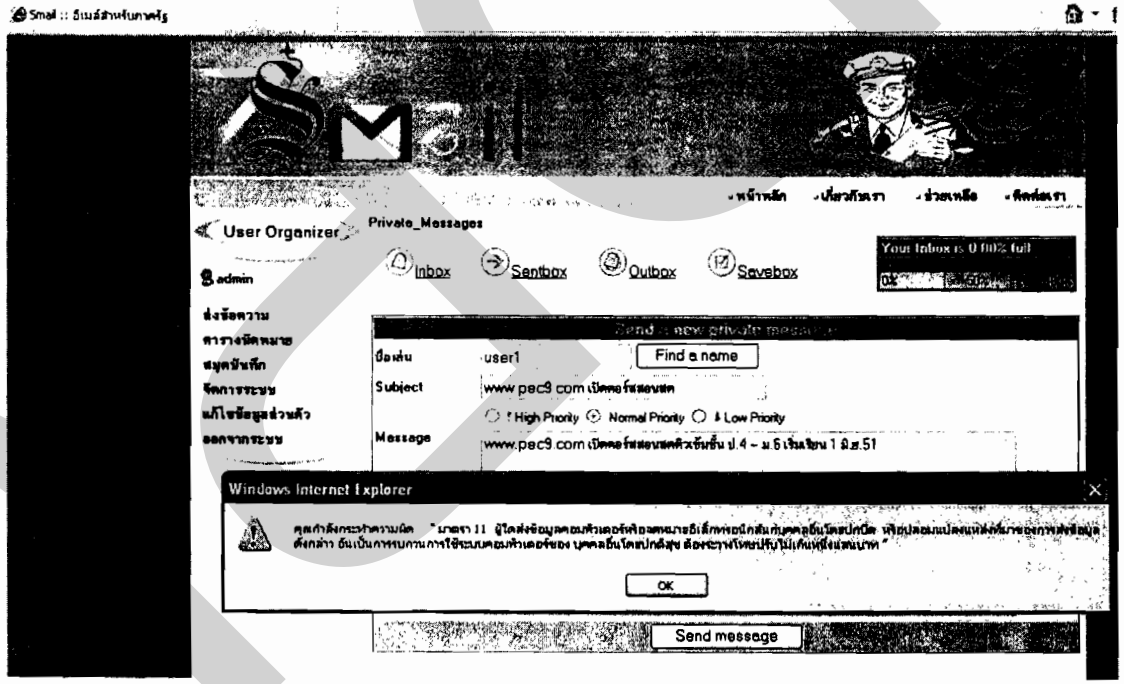
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam)

| รายการประเมิน<br>ประสิทธิภาพการทำงานของโปรแกรม | สถานะ<br>ข้อความ | ระดับประสิทธิภาพของโปรแกรม<br>(จำนวนข้อความที่กรองได้) | |
|---|---|---|---|
| | | Outlook | hotmail |
| www.pec9.com เปิดคอร์สสอนสดติวเข้มชั้น ป.4 – ม.6 เริ่มเรียน 1 มิ.ย.51 | Spam |  |  |
| ลุ้นดูดวงฟรีกับปู โลกเบี้ยวแค่รับดวงรายวัน กด*298*193#(4/)022076888 | | | |
| สุดคุ้ม!ใช้ฟรี 15 วัน โมโนลูกทุ่งฮิต แถมผลหวย โทร*45223111110/027302424 | | | |
| ด่วนเซนต์เทรเรซารับสมัคร น.ศ.พยาบาล อีก 10 ทน สุดท้าย โทร0867227493/037395313 | | | |
| ส่งความรักด้วยเสียงผ่าน VoiceSMS ฟรี ถึง 31 มี.ค.51 โทร 50100 (เฉพาะภูมิภาค) | | | |
| สมัครสมาชิกทรูมูฟซูปเปอร์สตาร์ภายในวันที่ 20 พ.ค.นี้ รับฟรี! | | | |
| ฟรีกระเป๋ามูลค่า 350 บ. ที่บูธ TMBMoney Expo 8-11 พ.ค.51_โชว์บัตร Ready Cash | | | |
| คุณมากกว่าใคร ดอกเบี้ย 0% 1 ปี ฟรีโอน+จด จำนองโทร 1375 | | | |
| เจาะลึก!แม่นยำ!ดวงคุณสัปดาห์นี้จะเป็นอย่างไร อ.ลักษณ์ฟันธง โทร 1900190065 | | | |
| ++ด่วนรับสมัครคอนเฟริม์ลูกค้าทาง อินเตอร์เน็ท คอนเฟริม์ลูกค้าล่ะ 2000 บาท up!!! สนใจสมัครเลยค่ะ? | | | |
| สรุปภาพรวม | | ส่งได้ 10 ข้อความ | ส่งได้ 10 ข้อความ |

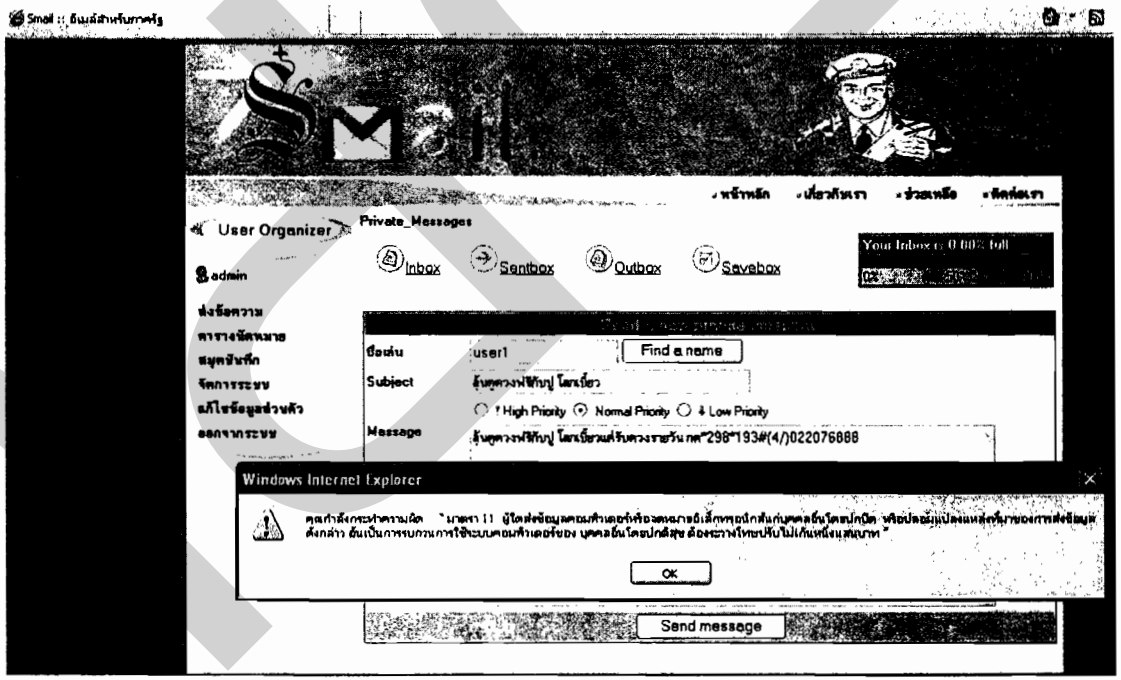
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมิน<br>ประสิทธิภาพการทำงานของโปรแกรม | สถานะ<br>ข้อความ | ระดับประสิทธิภาพของโปรแกรม<br>(จำนวนข้อความที่กรองได้) | |
|---|---|---|---|
| | | Yahoo | gmail |
| www.pec9.com เปิดคอร์สสอนสดติวเข้มชั้น ป.4 - ม.6 เริ่มเรียน 1 มิ.ย.51 | Spam |  |  |
| ลุ้นดูดวงฟรีกับปู โลกเบี้ยวแค่รับดวงรายวัน กด*298*193#(4/)022076888 | | | |
| สุดคุ้ม!ใช้ฟรี 15 วัน โมโนลูกทุ่งฮิต แถมผลหวย โทร*45223111110/027302424 | | | |
| ด่วนเซนต์เทรเรซารับสมัคร น.ศ.พยาบาล อีก 10 คน สุดท้าย โทร0867227493/037395313 | | | |
| ส่งความรักด้วยเสียงผ่าน VoiceSMS ฟรี ถึง 31 มี.ค.51 โทร 50100 (เฉพาะภูมิภาค) | | | |
| สมัครสมาชิกทรูมูฟซูปเปอร์สตาร์ภายในวันที่ 20 พ.ค.นี้ รับฟรี! | | | |
| ฟรีกระเป๋ามูลค่า 350 บ. ที่บูธ TMBMoney Expo 8-11 พ.ค.51_โชว์บัตร Ready Cash | | | |
| คุณมากกว่าใคร ดอกเบี้ย 0% 1 ปี ฟรีโอน+จด จำนองโทร 1375 | | | |
| เจาะลึก!แม่นยำ!ดวงคุณสัปดาห์นี้จะเป็นอย่างไร อ.ลักษณ์ฟันธง โทร 1900190065 | | | |
| ++ด่วนรับสมัคร คอนเฟริม์ลูกค้าทางอินเตอร์เน็ท คอนเฟริม์ลูกค้าล่ะ 2000 บาท up!!! สนใจสมัครเลยค่ะ? | | | |
| สรุปภาพรวม | | ส่งได้ 10 ข้อความ | ส่งได้ 10 ข้อความ |

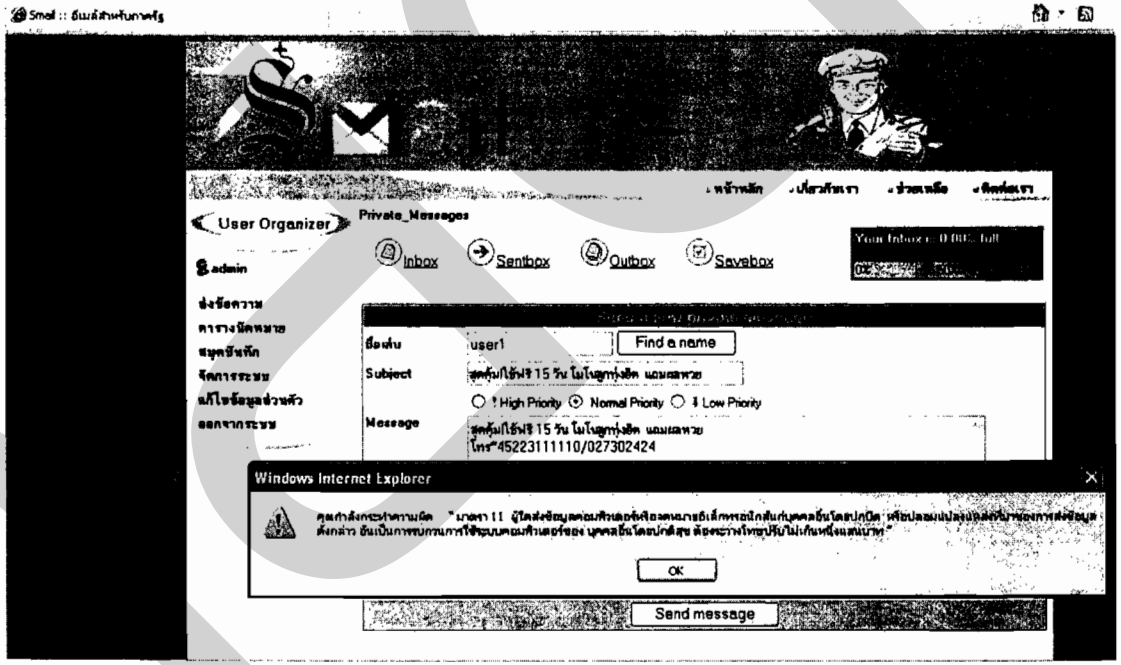
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) เว็บเมล์ที่พัฒนาขึ้น |
|---|---|---|
| www.pec9.com เปิดคอร์สสอนสดติวเข้มชั้น ป.4 – ม.6 เริ่มเรียน 1 มิ.ย. 51 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

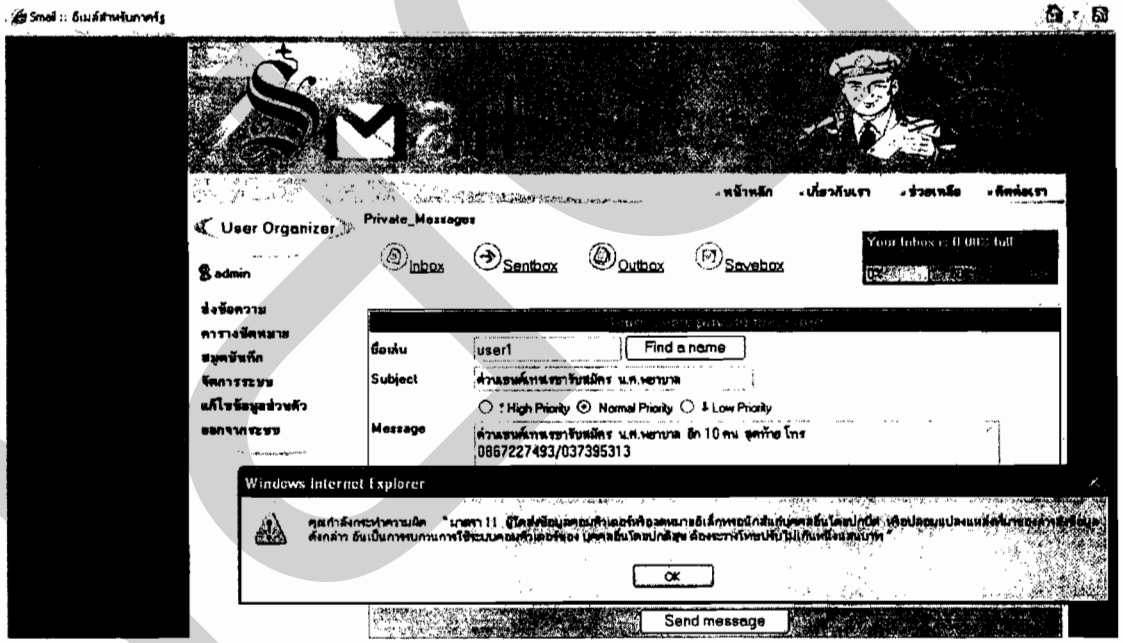
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| ลุ้นดูดวงฟรีกับปู โลกเบี้ยวแค่รับดวงรายวัน กด*298*193#(4/)022076888 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

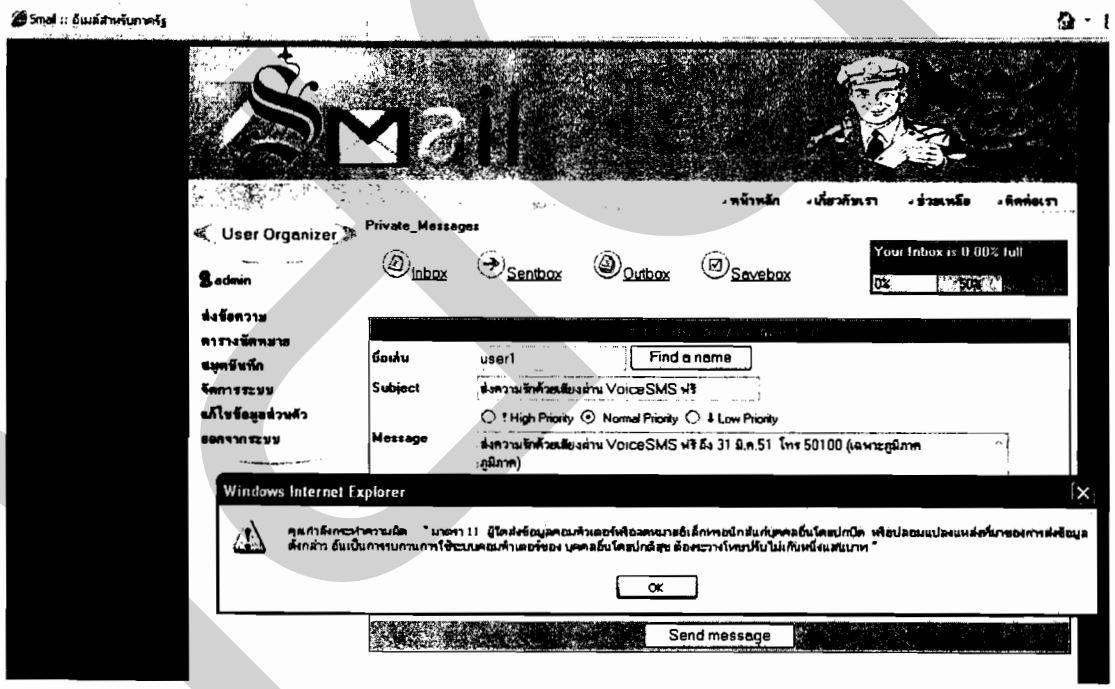
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| สุดคุ้ม!ใช้ฟรี 15 วัน โมโนลูกทุ่งฮิต แถมผลหวยโทร*45223111110/ 027302424 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

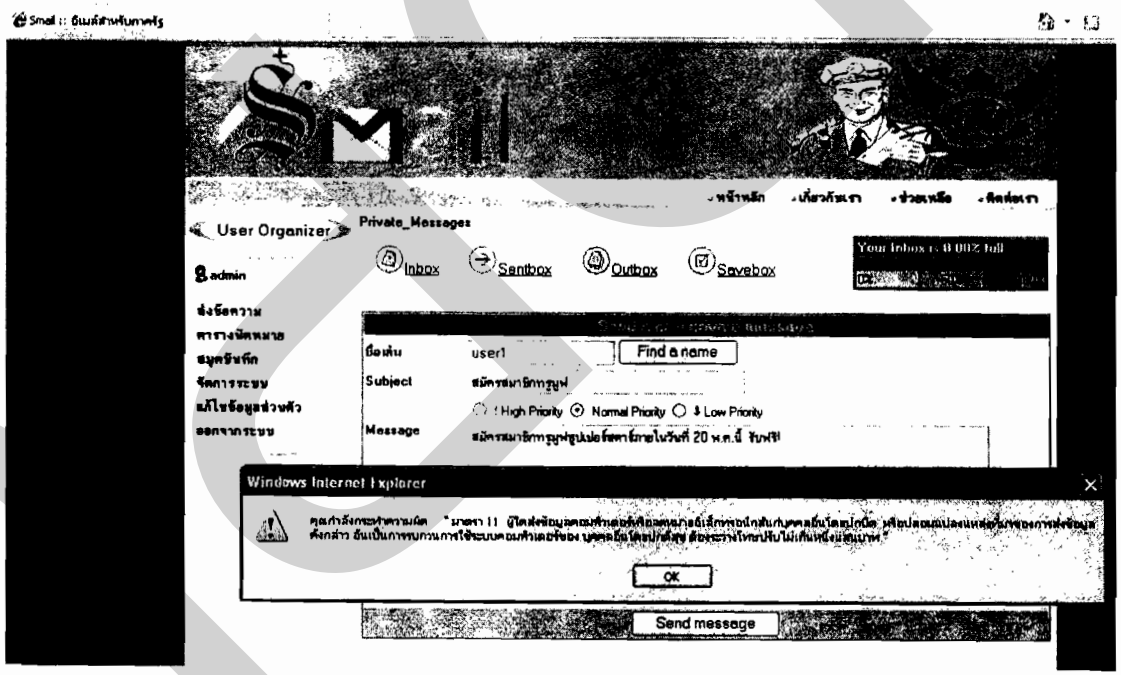
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) เว็บเมล์ที่พัฒนาขึ้น |
|---|---|---|
| ด่วนเซนต์เทรเรซารับสมัคร น.ศ. พยาบาล อีก 10 คน สุดท้าย โทร 0867227493/037395313 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

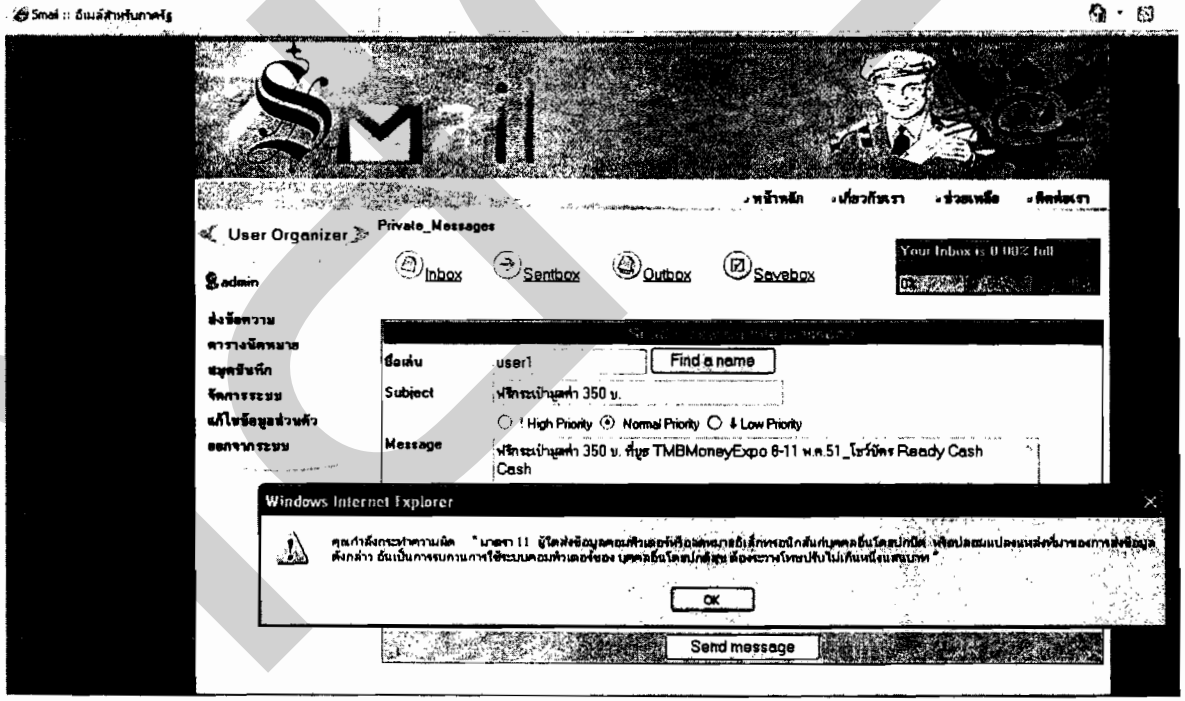
ตารางที่ ก-2 ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| ส่งความรักด้วยเสียงผ่าน VoiceSMS ฟรี ถึง 31 มี.ค.51 โทร 50100 (เฉพาะภูมิภาค) | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

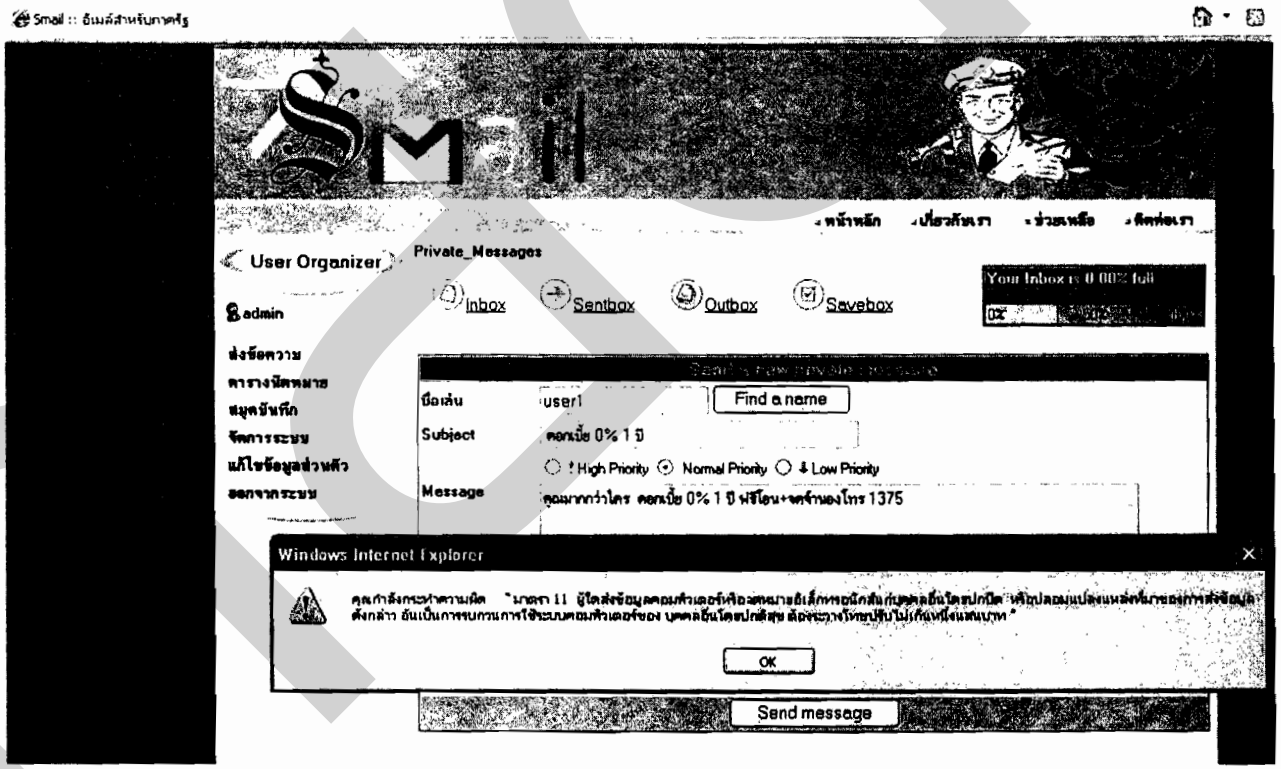
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| สมัครสมาชิกทรูมูฟซูปเปอร์สตาร์ ภายในวันที่ 20 พ.ค.นี้ รับฟรี! | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

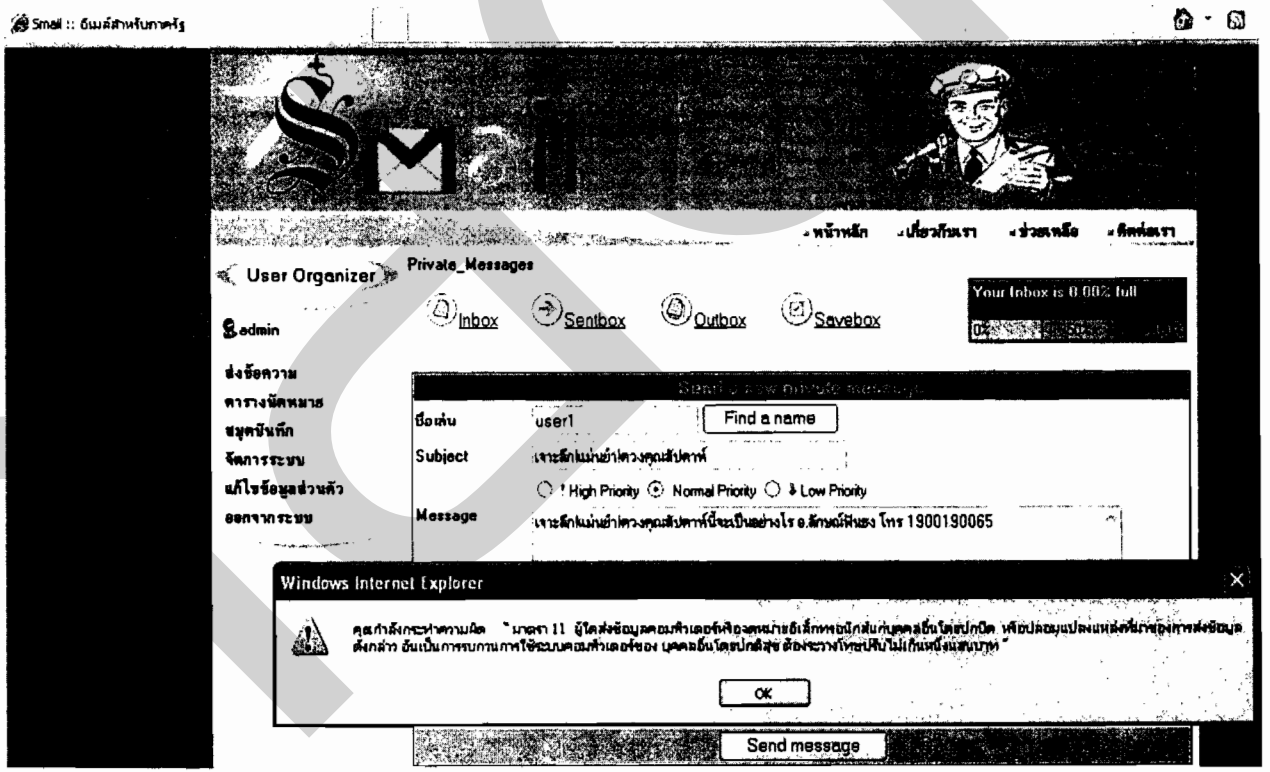
ตารางที่ ก-2 ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) เว็บเมล์ที่พัฒนาขึ้น |
|---|---|---|
| ฟรีกระเป๋ามูลค่า 350 บ. ที่บูธ TMBMoneyExpo 8-11 พ.ค.51_โชว์บัตร Ready Cash | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

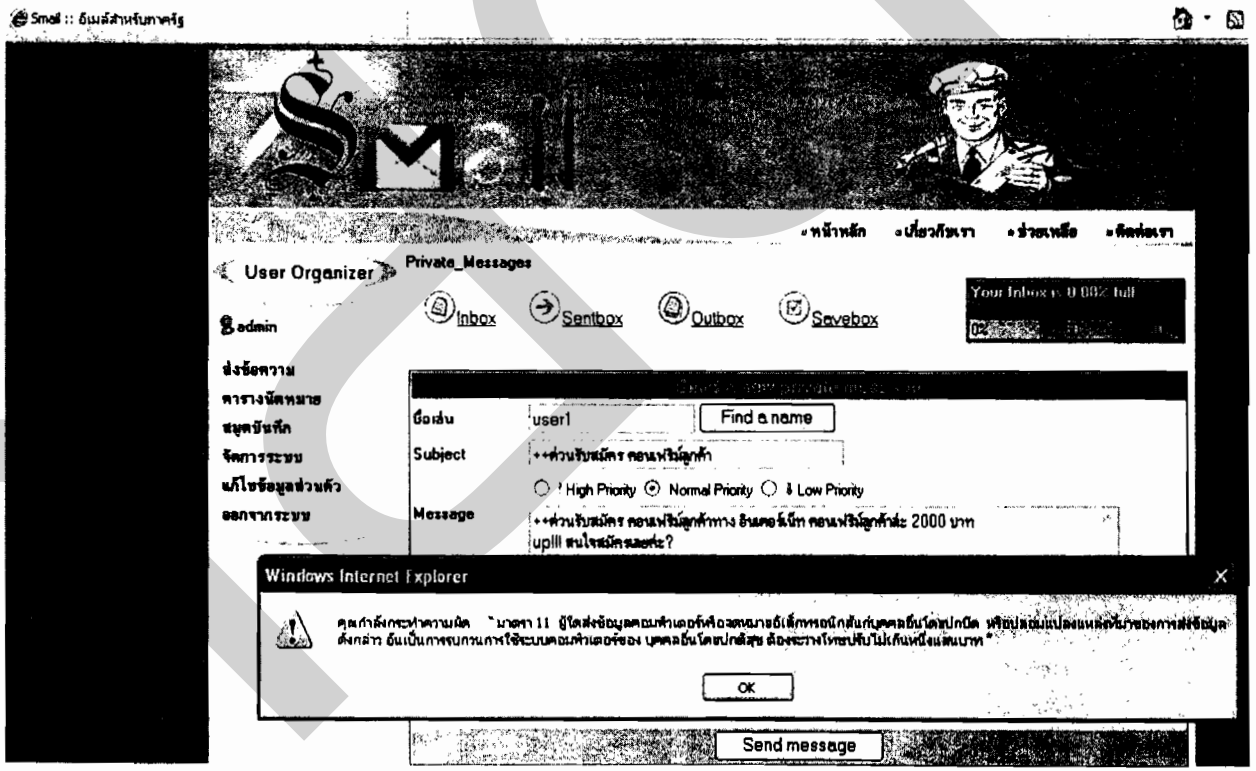
**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| คุณมากกว่าใคร ดอกเบี้ย 0% 1 ปี ฟรีโอน+จดจำนองโทร 1375 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) |
|---|---|---|
| | | เว็บเมล์ที่พัฒนาขึ้น |
| เจาะลึก!แม่นยำ!ดวงคุณสัปดาห์นี้จะเป็นอย่างไร อ.ลักษณ์ฟันธง โทร 1900190065 | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

**ตารางที่ ก-2** ผลการทดสอบการส่งกลุ่มตัวอย่างข้อมูล (Spam) (ต่อ)

| รายการประเมินประสิทธิภาพการทำงานของโปรแกรม | สถานะข้อความ | ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้) เว็บเมล์ที่พัฒนาขึ้น |
|---|---|---|
| ++ด่วนรับสมัคร คอนเฟริม์ลูกค้าทาง อินเตอร์เน็ท คอนเฟริม์ลูกค้าล่ะ 2000 บาท up!!! สนใจสมัครเลยค่ะ? | Spam |  |
| สรุปภาพรวม | | ไม่สามารถส่งข้อความได้ |

# ภาคผนวก ข

## แบบฟอร์มขอใช้บริการอีเมล์โปรแกรมตรวจสอบการส่งผ่านข้อมูลสแปมเมล์ สำหรับเครื่องคอมพิวเตอร์ลูกข่ายก่อนการส่งออกสู่เมล์เซิร์ฟเวอร์

# บันทึกข้อความ

**ส่วนราชการ** .....

**ที่** กห ..... **วันที่** .....

**เรื่อง** ขอรับการสนับสนุน Smail-Mail Address .....

เสนอ กทท.พธ.ทบ.

.....(นามหน่วย).....มีความประสงค์ขอรับการสนับสนุน Smail-Mail Address เพื่อใช้ในการรับ-ส่งเอกสารและประสานงานระหว่างหน่วยจำนวน ..... ชุด รายละเอียดตามที่แนบ

จึงเสนอมาเพื่อกรุณาดำเนินการต่อไป

.....

(.....)

ผบ.หน่วย

# แบบฟอร์มขอใช้บริการ Smail-Mail หน่วยงาน

ชื่อหน่วย (ภาษาไทย) _____

ชื่อหน่วย (ภาษาอังกฤษ) _____

**ผู้รับผิดชอบ :**

ยศ_____ชื่อ_____นามสกุล_____

ตำแหน่ง_____สังกัด_____

ทศท._____โทร.ทหาร_____

---

**หมายเหตุ :**

1. กทท.พธ.ทบ. จะเป็นผู้กำหนด User ID ตามมาตรฐานเดียวกันและกำหนดรหัสผ่านให้ในเบื้องต้น
2. ผู้รับผิดชอบ Smail-Mail Address จะต้องมาขอรับด้วยตนเอง หรือ มอบอำนาจเป็นลายลักษณ์อักษร ในกรณีให้ผู้อื่นมารับแทน เมื่อได้รับการติดต่อจาก กทท.พธ.ทบ.
3. หากมีปัญหาข้อขัดข้อง กรุณาติดต่อที่ กทท.พธ.ทบ.(กองเทคโนโลยีสารสนเทศ กรมพลาธิการทหารบก) โทร.ทหาร 68269 ทศท. โทร.0-2588-3420-1 ต่อ 68269 หรือส่ง User มาที่ *admin@*smail.com หรือ smallnoi@hotmail.com

| |
|---|
| เฉพาะเจ้าหน้าที่ : |
| Create by : _____ Create Date : _____ |

# บันทึกข้อความ

**ส่วนราชการ** .....

**ที่** กห ..... **วันที่** .....

**เรื่อง** ขอรับการสนับสนุน Smail-Mail Address ให้แก่กำลังพล .....

เสนอ กทท.พธ.ทบ.

.....(นามหน่วย).....มีความประสงค์ขอรับการสนับสนุน Smail-Mail Address ส่วนบุคคล ให้แก่กำลังพลจำนวน ..... นาย รายละเอียดตามที่แนบ

จึงเสนอมาเพื่อกรุณาดำเนินการต่อไป

.....

(.....)

ผบ.หน่วย

# แบบขอใช้บริการ Smail-Mail ส่วนบุคคล

ข้าพเจ้า ยศ-ชื่อ-สกุล .....

ชื่อ-นามสกุล (ภาษาอังกฤษ).....

หมายเลขประจำตัว .....

ตำแหน่ง.....สังกัด .....

ทศท. .....โทร.ทหาร .....

ขอใช้บริการ Smail โดยยินดีปฏิบัติตามระเบียบการรักษาความปลอดภัยของ พธ.ทบ. จะเก็บรหัสผ่านอย่างเป็นความลับ และยอมรับผิดชอบทุกประการ หาก Smail-Mail Address ของข้าพเจ้า ถูกนำไปใช้ในทางที่มิชอบ

ลงชื่อ..... ผู้ขอ

(.....)

ตำแหน่ง..... .....

...../...../.....

**หมายเหตุ :**

4. กทท.พธ.ทบ. จะเป็นผู้กำหนด User ID ตามมาตรฐานเดียวกันและกำหนดรหัสผ่านให้ในเบื้องต้น
5. ผู้รับผิดชอบ Smail-Mail Address จะต้องมาขอรับด้วยตนเอง หรือ มอบอำนาจเป็นลายลักษณ์อักษร ในกรณีให้ผู้อื่นมารับแทน เมื่อได้รับการติดต่อจาก กทท.พธ.ทบ.
6. หากมีปัญหาข้อขัดข้อง กรุณาติดต่อที่ กทท.พธ.ทบ.(กองเทคโนโลยีสารสนเทศ กรมพลาธิการทหารบก) โทร.ทหาร 68269 ทศท. โทร.0-2588-3420-1 ต่อ 68269 หรือส่ง User มาที่ *admin@*smail.com หรือ smallnoi@hotmail.com

| Create by : _____ | Create Date : _____ |
|---|---|

# ภาคผนวก ค

## คำสั่งกองเทคโนโลยีสารสนเทศ กรมพลาธิการทหารบก
## เรื่อง ให้นายสิบปฏิบัติหน้าที่เวร (เปิด/ปิด Server)

คำสั่ง กองเทคโนโลยีสารสนเทศ กรมพลาธิการทหารบก
ที่ ๗ / ๒๕๕๔
เรื่องให้นายสิบปฏิบัติหน้าที่เวร ประจำเดือน ก.พ.๕๔

.....

เพื่อให้การปฏิบัติงานของกองเทคโนโลยีสารสนเทศ กรมพลาธิการทหารบก เป็นไปด้วยความเรียบร้อย และเหมาะสมจึงให้ผู้มีรายชื่อท้ายคำสั่งปฏิบัติ ดังนี้

๑. ควบคุมกำกับดูแลการเปิด - ปิด สำนักงานให้เป็นไปด้วยความเรียบร้อย โดยเปิดสำนักงานไม่เกินเวลา ๐๘๐๐ และปิดสำนักงานเวลา ๑๖๓๐ หรือตามที่ผู้บังคับบัญชาสั่งการ เป็นครั้งคราว

๒. ควบคุมกำกับดูแลความสะอาด และเป็นระเบียบเรียบร้อยสำนักงานเป็นส่วนรวม

๓. เปิดเครื่อง Computer Server ( แม่ข่าย ) ทุกวันในเวลา ๐๘๓๐ พร้อมทั้งตรวจสอบความพร้อมในการใช้งานของเครื่อง เช่น ความพร้อมของ Modem ทั้ง ๒ ตัว และปิดเครื่องเวลา ๑๖๓๐

๔. การรับ - ส่ง หน้าที่เวลา ๐๘๐๐ ของทุกวัน และรายงานเหตุการณ์ให้ทราบเป็นประจำทุกวัน

๕. หากไม่มีผู้รับเวรให้เข้าเวรต่ออีกวันหนึ่ง พร้อมทั้งรายงานผู้ที่ขาดการเข้าเวรถัดไปให้ทราบ เพื่อพิจารณาโทษ และผู้ที่เข้าเวรติดต่อกันสองวัน ในคราวเดียวกันตามวรรคแรกให้งดเวรในเดือนถัดไปหนึ่งวัน

๖. การแทนเวรหรือเปลี่ยนเวรกันให้เสนอรายงานขออนุมัติล่วงหน้าก่อน ๑ วันทำการ เมื่อได้รับการอนุมัติแล้วจึงให้ทำการเปลี่ยนเวรกันได้ เว้นผู้ที่ไปราชการตามคำสั่งของทางราชการให้รายงานผ่าน บก.กทท.พธ.ทบ. เพื่อออกคำสั่งจัดเวรแทนเป็นราย ๆ ไป

ทั้งนี้ ตั้งแต่ ๑ กุมภาพันธ์ พ.ศ.๒๕๕๔ เป็นต้นไป

สั่ง ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๕๔

พ.ท.
(วัชราวุธ ยมนา)
รอง หก.กทท.พธ.ทบ. ทำการแทน
หก.กทท.พธ.ทบ.

บัญชีรายชื่อเวรเปิด – ปิดสำนักงาน
กองการไปรษณีย์ทหาร พธ.ทบ.
ประจำเดือน ก.พ.๕๔

| ลำดับ | ยศ – ชื่อ | | วันปฏิบัติหน้าที่ | | | | | | | หมายเหตุ |
|---|---|---|---|---|---|---|---|---|---|---|
| ๑. | จ.ส.อ. จรินทร์ | ทรงบัณฑิต | | ๔ | ๑๐ | ๑๖ | ๒๓ | | | |
| ๒. | จ.ส.อ. ทณิน ปราณี | คณาปัง | ๑ | ๗ | ๑๑ | ๑๗ | ๒๔ | | | |
| ๓. | จ.ส.อ. ไชยกิ | อินทอง | ๒ | ๘ | ๑๔ | ๒๑ | ๒๕ | | | |
| ๔. | ส.อ.สิทธิพร | หุ่นทอง | ๓ | ๙ | ๑๕ | ๒๒ | ๒๘ | | | |

พ.ท.

(วัชราวุธ ยมนา)

รอง หก.กทท.พธ.ทบ. ทำการแทน
หก.กทท.พธ.ทบ.

# ประวัติผู้เขียน

| | |
|---|---|
| ชื่อ-นามสกุล | จ่าสิบตรี สิทธิพร พุ่มพวง |
| ประวัติการศึกษา | สำเร็จการศึกษาระดับปริญญาตรี จากคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏพระนคร ปีการศึกษา 2549 |
| ตำแหน่งและสถานที่ทำงานปัจจุบัน | เจ้าหน้าที่รักษาโปรแกรม กรมพลาธิการทหารบก |