



หน่วยการเรียนรู้ที่ 7 การใช้โปรแกรมประยุกต์

1. ความหมายของโปรแกรมประยุกต์

โปรแกรมประยุกต์ หมายถึง โปรแกรมที่พัฒนาขึ้นเพื่อให้เครื่องคอมพิวเตอร์ทำงานตามความต้องการของผู้ใช้ ที่เป็นงานทั่วไป และงานเฉพาะด้าน ขึ้นอยู่กับลักษณะงานและจุดมุ่งหมาย

นำโปรแกรมประยุกต์ไปใช้งานนอกจากเป็นการเพิ่มประสิทธิภาพในการทำงานแล้วยังเป็นการอำนวยความสะดวกแก่ผู้ปฏิบัติงานอีกด้วย เช่น โปรแกรมเพื่องานด้านการฝากถอนเงินโดยเครื่องรับจ่ายเงินอัตโนมัติจะเกี่ยวข้องกับการฝากหรือถอนเงิน รวมทั้งการควบคุมยอดเงินคงเหลือในบัญชีเงินฝากของลูกค้าธนาคาร ตัวอย่างของโปรแกรมประยุกต์เพื่อใช้งานในด้านต่าง ๆ ได้แก่

- โปรแกรมการคำนวณน้ำประปา ค่าไฟฟ้า ค่าโทรศัพท์
- โปรแกรมเพื่อใช้บริหารบุคคลของหน่วยงาน
- โปรแกรมเพื่อการลงทะเบียนเรียนของนักศึกษา
- โปรแกรมเพื่อแสดงยอดขายสินค้าของบริษัท
- โปรแกรมประยุกต์เงินเดือนพนักงาน
- โปรแกรมประยุกต์เพื่อจัดซื้อสินค้าหรือพัสดุ

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

ก่อนหน้านี้เว็บเบราว์เซอร์จะมีหน้าที่สำหรับใช้ดูข้อมูลต่าง ๆ ผ่านเครื่องแม่ข่ายให้บริการเว็บ (Web Server) ที่ให้บริการผ่าน World Wide Web (WWW) หรือเทียบง่าย ๆ เหมือนเป็นโทรศัพท์เป็นห้องสมุดให้เราเข้าไปดูข้อมูล แต่เป็นสถานีโทรศัพท์ที่มีนับล้าน ๆ ช่อง ผู้ใช้ส่วนใหญ่จะไม่ค่อยสนใจรายละเอียดในการใช้งานเว็บเบราว์เซอร์หรือเลือกโปรแกรมเว็บเบราว์เซอร์มากนัก ผู้ใช้มักจะใช้โปรแกรมที่ติดตั้งมากับระบบปฏิบัติการ เช่น IE หรือ Internet Explorer ที่ติดตั้งมากับระบบปฏิบัติการ Windows หรือ Safari ที่มาพร้อมกับ Mac OS ต่อมาเมื่อมีโปรแกรมงานเว็บ

เบราว์เซอร์ฟรีจาก Mozilla ชื่อ Firefox เข้ามาให้ใช้โดยข้อดีของ
เว็บเบราว์เซอร์



ผลิตโปรแกรม
ให้เราได้ใช้มา
เบราว์เซอร์ของตน

เองที่ใช้ชื่อว่า Google Chrome ทำให้เกิดการแข่งขันเรื่องความ
สามารถของโปรแกรมเว็บเบราว์เซอร์มากขึ้นตามลำดับ



MacOS, iOS



MacOS, MS Windows,
Linux OS, Android OS



MacOS, MS Windows,
Linux OS
Android OS, Chrome OS



MS Windows, MacOS,
iOS, Android OS



MacOS, MS Windows,
Linux OS, Android OS



ภาพโปรแกรมเว็บเบราว์เซอร์ที่ได้รับความนิยม

สาเหตุที่ทำให้เราให้ความสำคัญกับโปรแกรมเว็บ
เบราว์เซอร์มากขึ้น เพราะว่าเทคโนโลยีการสื่อสารในปัจจุบันมีค
ความก้าวหน้าอย่างรวดเร็ว ทำให้เกิดบริการใหม่ ๆ บนเครือข่ายอิน
เทอร์เน็ต นอกเหนือจากการดูข้อมูล ไม่ว่าจะเป็นความบันเทิง การ
ช้อปปิ้งออนไลน์ จนถึงการทำธุรกรรมการเงิน หรือแม้แต่การ
เข้าไปดูข้อมูลต่าง ๆ จากอินเทอร์เน็ตเองก็ตาม เพราะเว็บ
เบราว์เซอร์เป็นเหมือนประตูสู่โลกภายนอกของคอมพิวเตอร์ส่วน
บุคคลหรือระบบเครือข่ายในองค์กร ในขณะเดียวกันก็เป็นช่องทาง
ให้เกิดการเข้ามาของผู้ไม่ประสงค์ดีทั้งแบบที่โจมตีโดยตรง (แฮ็ก
ข้อมูล) หรือการผ่านมัลแวร์ที่แนบมากับข้อมูลที่ผู้ใช้เข้าไปดู
ทำให้ผู้ใช้ต้องเข้าใจกลไกการทำงานหรือความสามารถต่าง ๆ
ของโปรแกรมเว็บเบราว์เซอร์เพื่อความสะดวกปลอดภัยในการใช้
งานอินเทอร์เน็ต

ความสามารถและบริการของเว็บเบราว์เซอร์ที่เพิ่มขึ้นผ่านระบบ World Wide Web บวกกับความเร็วในการใช้งานอินเทอร์เน็ตในปัจจุบันที่มีมากขึ้น จนกระทั่งเราสามารถทำงานต่าง ๆ ผ่านเว็บเบราว์เซอร์ได้โดยไม่ต้องใช้โปรแกรมเสริมอื่น เช่น กรณีโน้ตบุ๊กของ Google ที่ชื่อว่า Chrome Book เมื่อเปิดเครื่องผู้ใช้จะเข้าไปใช้โปรแกรมพื้นฐาน เช่น ผ่านทางเว็บเบราว์เซอร์โดยมีโปรแกรมให้ใช้งานผ่าน Google Docs

ตัวอย่างโปรแกรมเว็บเบราว์เซอร์ ได้แก่ Opera, Avast Secure Browser, Google Chrome, Mozilla Firefox, Safari และ Microsoft Edge โดยเว็บเบราว์เซอร์ชั้นนำที่เป็นที่นิยมจะมีคุณสมบัติที่ใกล้เคียงกันโดยเฉพาะเรื่องความมั่นคงปลอดภัย แต่จะแตกต่างกันในรายละเอียดปลีกย่อยที่จะช่วย



ใน Google Chrome

หัวใจสำคัญของการใช้เว็บเบราว์เซอร์นอกจากเรื่องความเร็ว

ค่ามาตรฐานระดับความมั่นคงปลอดภัยในระดับปานกลางและให้ผู้ใช้ปรับเปลี่ยนเองได้ภายในเมนูการตั้งค่าของโปรแกรม โดยจะขอยกตัวอย่างการปรับตั้งค่าจากโปรแกรม Google Chrome เนื่องจากมีผู้นิยมใช้มาก (โปรแกรมอื่นจะปรับแต่งใกล้เคียงกัน)

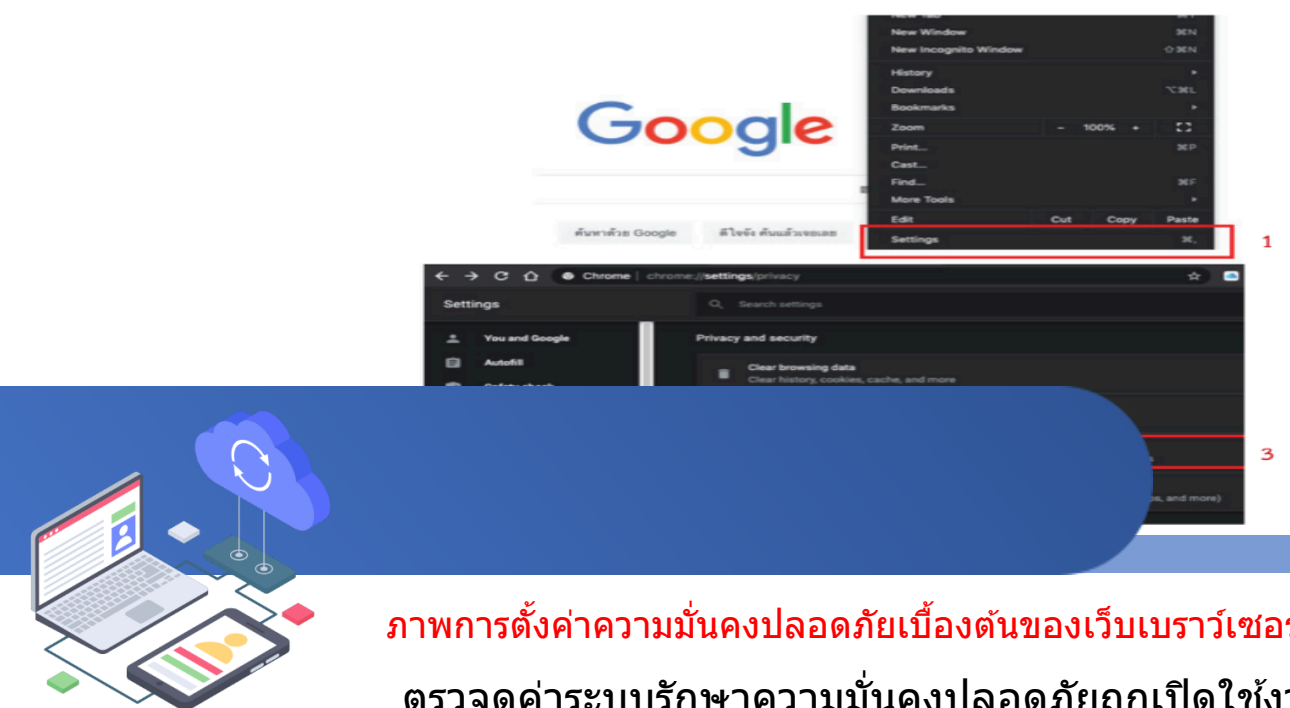
2.1 การท่องเว็บให้ปลอดภัยด้วย HTTPS

ปกติแล้วมักจะคุ้นเคยกับโพรโทคอล HTTP ซึ่งเมื่อพิมพ์ชื่อเว็บไซต์ในเว็บเบราว์เซอร์ โปรแกรมจะเติมโพรโทคอลให้เอง เช่น ถ้าเราพิมพ์ www.kmutnb.ac.th ระบบจะเติม <http://www.kmutnb.ac.th/> และถ้าตรวจพบว่าเว็บไซต์มีบริการ

ด้านความมั่นคงปลอดภัยที่เรียกว่า HTTPS ระบบจะปรับที่อยู่ของเว็บไซต์เป็น <https://www.kmutnb.ac.th/> โดยอัตโนมัติ HTTPS (Hypertext Transfer Protocol Secure) คือ โพรโทคอลการสื่อสารอินเทอร์เน็ตที่ช่วยรักษาความสมบูรณ์ถูกต้องของข้อมูลผู้ใช้และเก็บข้อมูลไว้เป็นความลับระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์ ผู้ใช้คาดหวังประสบการณ์ออนไลน์ที่มีความมั่นคงปลอดภัยและเป็นส่วนตัวระหว่างที่ใช้เว็บไซต์ผู้ใช้ควรหลีกเลี่ยงเว็บไซต์ที่ไม่ใช้โพรโทคอล HTTPS เนื่องจากการรับส่งข้อมูลต่าง ๆ ระหว่างการท่องเว็บไซต์จะสามารถถูกดักข้อมูลไปได้ง่าย

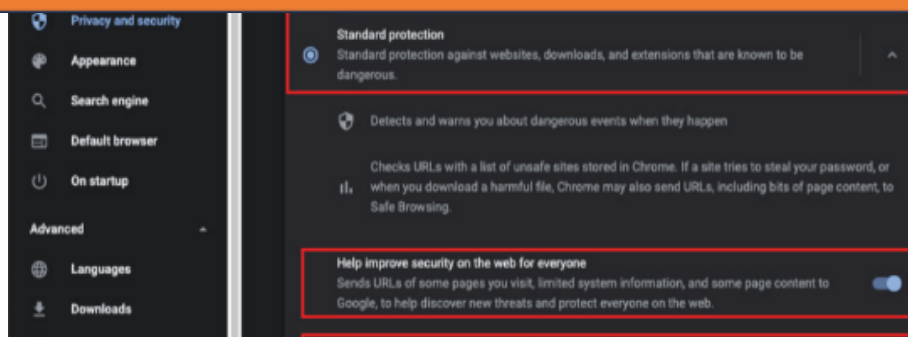
2.2 การตรวจสอบและตั้งค่าความมั่นคงปลอดภัยเบื้องต้นของเว็บเบราว์เซอร์

ไปที่ Settings -> Privacy & Security -> Security



ภาพการตั้งค่าความมั่นคงปลอดภัยเบื้องต้นของเว็บเบราว์เซอร์

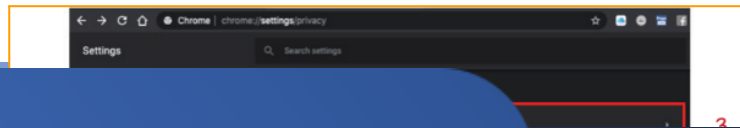
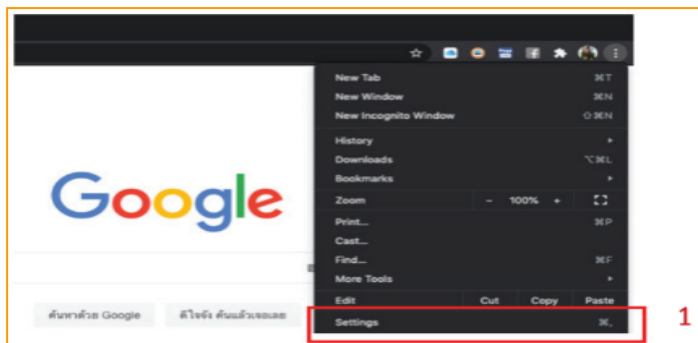
ตรวจสอบดูค่าระบบรักษาความมั่นคงปลอดภัยถูกเปิดใช้งานใน
เมนู Standard และเลือกให้ใช้งานความมั่นคงปลอดภัย



ภาพการลบประวัติการท่องเว็บไซต์

2.3 การลบประวัติการท่องเว็บไซต์

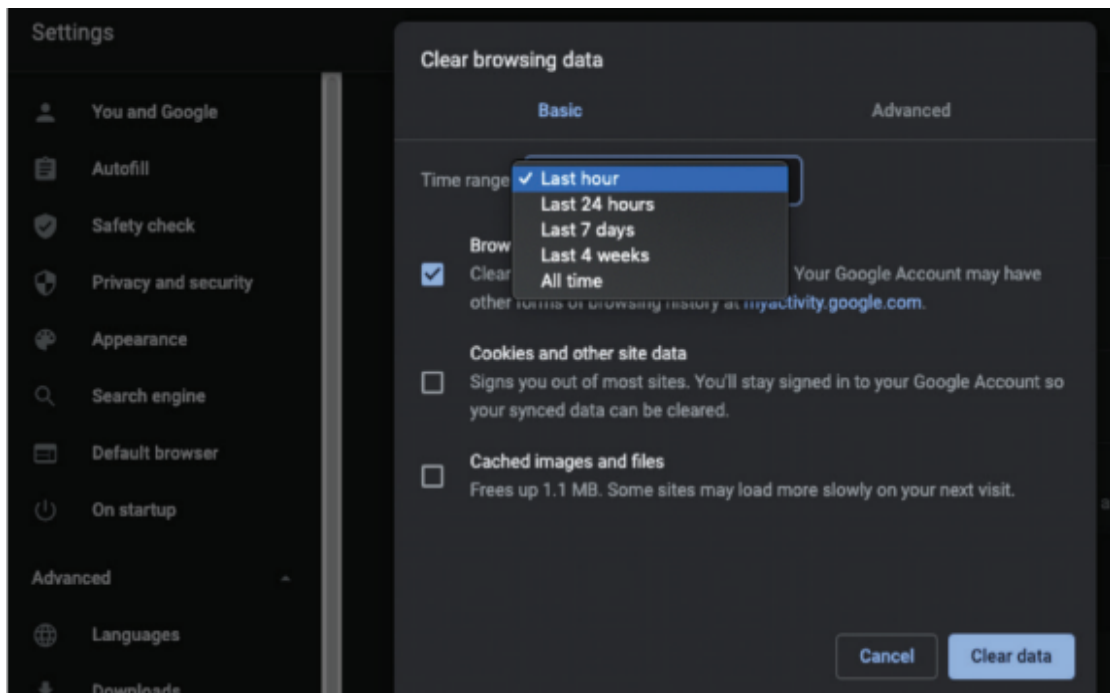
ทั้งในกรณีที่ เป็นเครื่องของตนเองหรือการไปใช้เครื่องคอมพิวเตอร์ของผู้อื่นแล้วต้องการจะลบประวัติการใช้งาน เพื่อป้องกันข้อมูลที่ใช้งานรั่วไหลไปยังบุคคลอื่นทำได้ ดังนี้
Settings -> Privacy and Security -> Clear browsing data



◆ ภาพ Settings -> Privacy and Security -> Clear browsing data

ผู้ใช้สามารถกำหนดระยะเวลาที่ต้องการลบประวัติการเข้าใช้งานในระบบได้





ภาพการกำหนดระยะเวลาที่ต้องการลบประวัติการเข้าใช้งาน

2.4 การใช้งานร่วมกันของเว็บเบราว์เซอร์ในหลายอุปกรณ์

เว็บเบราว์เซอร์ในหลายอุปกรณ์สมัยใหม่จะมีความสามารถที่เรียกว่าการ Synchronize ข้อมูลของผู้ใช้ ไปยังอุปกรณ์อื่นเพื่ออำนวยความสะดวกให้กับผู้ใช้ที่มีอุปกรณ์คอมพิวเตอร์หลายเครื่อง เช่น โน้ตบุ๊ก เครื่องตั้งโต๊ะและสมาร์ทโฟน ถ้าผู้ใช้ลงชื่อเข้าใช้เว็บเบราว์เซอร์ด้วยบัญชีเดียว (สามารถสมัครได้ฟรี) เช่น การลงชื่อด้วย Gmail ใน Google Chrome ข้อมูลของผู้ใช้ทั้งประวัติการเข้าชม บุกมาร์ก จนถึงรหัสผ่านต่าง ๆ จะถูกส่งผ่านไปปรากฏในทุกอุปกรณ์ที่ผู้ใช้ลงชื่อเข้าไปใช้งาน อย่างไรก็ตามสิ่งที่ต้องระมัดระวังคืออุปกรณ์ที่ลงชื่อเข้าใช้ด้วยบัญชีของเว็บเบราว์เซอร์ จะต้องมั่นใจว่ามีความมั่นคงปลอดภัยในแง่กายภาพ คือไม่มีบุคคลอื่นสามารถเข้าไปใช้งานได้ เพราะอาจจะทำให้ข้อมูลรั่วไหลหรือมีการเข้าถึงข้อมูลส่วนบุคคลต่าง ๆ ได้ หากเป็นอุปกรณ์คอมพิวเตอร์ส่วนบุคคลขอแนะนำให้อย่าใช้การ Synchronize ข้อมูลผ่านเว็บเบราว์เซอร์



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

งานผ่านระบบเครือข่ายนับได้ว่าแทบจะครอบคลุมการทำงานแทบทุกด้าน ได้แก่

3.1 โปรแกรมประยุกต์ด้านการทำธุรกิจ

ในการใช้งานระบบคอมพิวเตอร์ตั้งแต่เริ่มแรกจนถึงปัจจุบัน การใช้งานโปรแกรมประยุกต์ด้านธุรกิจจะเป็นวัตถุประสงค์หลัก โดยโปรแกรมที่นิยมใช้งาน ได้แก่ Word Processing โปรแกรมสำหรับคำนวณหรือ Spread Sheet โปรแกรมนำเสนองาน หรือ Presentation เช่น PowerPoint, Keynote

โปรแกรมประยุกต์เหล่านี้เรามักจะคุ้นเคยการทำงานในแบบที่ต้องติดตั้งบนเครื่องคอมพิวเตอร์แต่ในปัจจุบันผู้ใช้สามารถที่จะใช้งานโปรแกรมเหล่านี้ผ่านเว็บเบราว์เซอร์ได้ ซึ่งมีทั้งแบบฟรีและแบบที่ต้องเสียเงินค่าบริการรายปี

1. โปรแกรม Google Docs หรือ Google Documents “ฟรี” บริการออนไลน์ในการทำงานโปรแกรมประเภท Office จากค่าย Google เพียงแคมีอีเมลของ Google ก็สามารถใช้บริการได้ฟรีผ่านทางเครือข่าย อินเทอร์เน็ต แถมยังมีพื้นที่ในการจัดเก็บข้อมูลอย่าง “Google Drive” ฟรีอีกด้วย

เปรียบเทียบ Microsoft Office กับ Google Docs

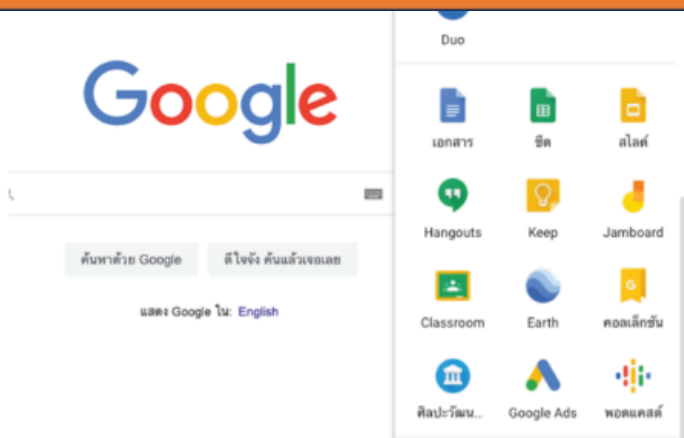
Program	Microsoft Office	Google Docs
งานจดหมาย	Microsoft Word	Docs
งานตาราง คำนวณ	Microsoft Excel	Sheets
งานนำเสนอ	Microsoft PowerPoint	Slides

วิธีใช้งาน Google Docs

1. เปิดโปรแกรม “เว็บเบราว์เซอร์” แนะนำให้ใช้ Google Chrome



โปรแกรมที่ต้องการใช้งาน Google Docs หรือ Slides เป็นโปรแกรมที่สามารถนำมาประยุกต์ใช้งานได้อย่างหลากหลาย เช่น การทำฟอร์มรับสมัคร เก็บข้อมูล หรือแม้แต่การทำแบบทดสอบออนไลน์อีกด้วย



2. โปรแกรม Office 365 เป็นการให้บริการโปรแกรมชุด Microsoft Office ที่สามารถใช้งานได้ทุกที่ผ่านเว็บเบราว์เซอร์และระบบอินเทอร์เน็ต โดยผู้ใช้เพียงแคมีบัญชี

Microsoft ซึ่งลงทะเบียนโดยใช้ E-mail และสมัคร
การใช้บริการ Office 365 ก็สามารถโปรแกรม Microsoft
Office ได้โดยไม่ต้องติดตั้งโปรแกรมชุด Office ในเครื่อง
คอมพิวเตอร์หรือสมาร์ทโฟนและยังมีพื้นที่เก็บข้อมูลบนคลาวด์ให้
สูงถึง 1 TB ทำให้ผู้ใช้สามารถเก็บเอกสารของตนไว้ได้อย่าง
มากมายทั้งสำหรับใช้งานจริงหรือใช้สำหรับสำรองข้อมูล
อย่างไรก็ตาม Office 365 เป็นโปรแกรมที่ผู้ใช้จะต้องเสียค่า
บริการรายปี โดยค่าใช้จ่ายเริ่มต้นเพียงปีละ 300 บาทต่อคน (แบบ
Family) หากผู้ใช้มีความคุ้นเคยกับการใช้โปรแกรมตระกูล
Microsoft Office ก็เป็นตัวเลือกที่น่าสนใจเพราะหนึ่งบัญชี
(E-mail) สามารถลงชื่อใช้งานอุปกรณ์พร้อมกันได้ถึง 5 อุปกรณ์

3.2 โปรแกรมประยุกต์ด้านการสื่อสาร

อินเทอร์เน็ตถูกออกแบบมาสำหรับการทำงานระยะไกล ซึ่ง
ในปัจจุบันด้วยความเร็วในการสื่อสารที่เพิ่มมากขึ้นทำให้สามารถ
บริการการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตเต็มรูปแบบ
ทั้งภาพ เสียงการประชุม หรือการนำเสนอต่าง ๆ โดยเฉพาะ
เมื่อเกิดวิกฤตการณ์โรคโควิด-19 ระบาดทำให้ความจำเป็นในการ

เป็นปัจจัย

เช่น การ
โดยโปรแกรม

ประยุกต์ที่ได้รับความนิยมในการสื่อสารระยะไกลแบบกลุ่ม ได้แก่

1. โปรแกรม Zoom

เป็นโปรแกรมประชุมทางไกลผ่านระบบคลาวด์ เป็นซอฟต์แวร์
สำหรับสื่อสารกันในลักษณะของ Video Conference เหมาะ
สำหรับใช้ประชุมหรือห้องเรียนผ่านเครือข่ายคอมพิวเตอร์ที่มีระบบ
อินเทอร์เน็ตเพื่ออำนวยความสะดวกในการประชุมหรือการเรียนการสอน

งานได้หลายแพลตฟอร์ม

ทั้งบนคอมพิวเตอร์

แท็บเล็ต และสมาร์ทโฟนซึ่งมีคุณสมบัติในการใช้งาน Video



Conference, Chat Room, Schedule และ Share Screen

อีกทั้งยังสามารถเชิญผู้เข้าร่วมประชุมได้โดยไม่ต้องสมัครเป็นสมาชิก เพียงแค่ผู้เข้าร่วมจะต้องมี PM (Personal Meeting ID) และ Password หรือ URL จากผู้ที่เป็นเจ้าภาพการประชุมหรือเรียกว่า โฮสต์ (Host) และติดตั้งแอปพลิเคชันของ Zoom ก็สามารถเข้าร่วมประชุมได้ ทำให้ Zoom เหมาะสำหรับการใช้งานประชุมหรือสร้างห้องเรียนผ่านเครือข่ายคอมพิวเตอร์เป็นอย่างมาก

โปรแกรม Zoom มีบัญชีฟรีสำหรับผู้เริ่มต้น สามารถจัดการประชุมทางไกลได้มากถึง 100 คน โดยจำกัดระยะเวลาไม่เกินครั้งละ 40 นาที ซึ่งเพียงพอที่จะใช้ในการประชุมหรือการเรียนการสอนทั่วไป (สามารถต่อกลับมาได้) และหากต้องการใช้ Zoom เพื่อการประชุมระยะเวลานาน ๆ ผู้ที่เป็นเจ้าภาพการประชุม (Host) สามารถที่จะสมัครสมาชิกเพื่อใช้งานแบบโปร (Professional) ซึ่งมีราคาเริ่มต้นที่ประมาณเดือนละ 400 บาท

2. โปรแกรม Google Meet

เป็นโปรแกรมที่ใช้สำหรับการประชุมเช่นกัน โดยการให้บริการจาก Google ซึ่งพัฒนามาจากโปรแกรม Google Duo โดยเน้นการใช้งานในภาคธุรกิจคือมีความสามารถในการแชร์หน้าจอและแชร์เอกสารระหว่างการประชุม เป็นต้น

Google ไม่ได้บังคับให้ผู้ร่วมประชุมทุกคนจะต้องเป็นผู้ใช้ผลิตภัณฑ์ Gmail ของ Google แต่หากเป็นสมาชิกของ Google อยู่แล้วจะใช้งาน Feature ต่าง ๆ ได้มากกว่า โดยทาง Google ได้ออกแบบไว้สำหรับกลุ่มผู้ใช้งาน 3 ประเภท ดังนี้

1. ระดับธุรกิจ : สำหรับบริษัท องค์กร ทั้งขนาดเล็กและขนาดใหญ่
2. สถาบันการศึกษา : โรงเรียน มหาวิทยาลัย และสถาบันการศึกษาอื่น ๆ
3. ผู้ใช้งานทั่วไป : สำหรับติดต่อสื่อสารกับเพื่อน ญาติ และผู้นัดหมายอื่น ๆ

หากต้องการใช้งาน Google Meet ให้เต็มประสิทธิภาพ ผู้ใช้จะ
ต้องสมัครใช้บริการ G Suite ของ Google เช่นเดียวกันกับ



เลือกรุ่นที่เหมาะสมกับคุณ ทดลองใช้ฟรี 14 วัน

ทุกแพ็คเกจประกอบด้วย

฿113.50 THB ฿227*	฿272.40 THB ฿454*	฿681 THB	คิดต่อฝ่ายขายเพื่อขอข้อมูลราคา
ทดลองใช้/เดือน โดยมีระยะเวลาทดลองใช้ 1 ปี	ทดลองใช้/เดือน โดยมีระยะเวลาทดลองใช้ 1 ปี	ทดลองใช้/เดือน โดยมีระยะเวลาทดลองใช้ 1 ปี	ติดต่อฝ่ายขาย
เริ่มต้นทดลองใช้ฟรี	เริ่มต้นทดลองใช้ฟรี	เริ่มต้นทดลองใช้ฟรี	
- มีแอดมินที่กำหนดเองและปลอดภัย - การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ 100 คน - พื้นที่เก็บข้อมูลขนาด 30 GB ต่อผู้ใช้ - การควบคุมความปลอดภัยและการจัดการ - การสนับสนุนระดับมาตรฐาน (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนขั้นสูง)	- มีแอดมินที่กำหนดเองและปลอดภัย - การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ + มีผู้เข้าร่วมได้ 150 คน - พื้นที่เก็บข้อมูลขนาด 2 TB ต่อผู้ใช้** - การควบคุมความปลอดภัยและการจัดการ - การสนับสนุนระดับมาตรฐาน (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนขั้นสูง)	- มีแอดมินที่กำหนดเองและปลอดภัย + eDiscovery, การเก็บรักษาข้อมูล, การเข้ารหัส S/MIME - การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ + มีผู้เข้าร่วมได้ 500 คน การติดตามการเข้าร่วม การลดเสียงรบกวน สติ๊กเกอร์แบบสติกเกอร์ในโดเมน - พื้นที่เก็บข้อมูลตามต้องการ** - การควบคุมความปลอดภัย การจัดการและการใช้ข้อมูลที่กำหนดขึ้นสูง รวมถึงการเข้ารหัส, DLP, เซลล์ข้อมูล และการจัดการปลายทางระดับองค์กร - การสนับสนุนขั้นสูง (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนระดับพรีเมียม)	

คุณจะได้รับแพ็คเกจ Business Starter, Business Standard และ Business Plus 100 คน ส่วนแพ็คเกจ Enterprise จะไม่มีจำนวนผู้ใช้ขึ้นสำหรับสูงสุด
ลูกค้า Google Workspace อาจเข้าถึงฟีเจอร์เพิ่มเติมได้ในช่วงเวลาจำกัด

ภาพราคาค่าใช้บริการของ Google Workspace ที่มีการรวม Google Meet
เป็นส่วนหนึ่งของบริการ

3. Microsoft Team

เป็นแอปพลิเคชันสื่อสารระดับองค์กรที่มีข้อดีในด้านการทำงาน
ร่วมกับ Office 365 โดยมีคุณสมบัติใกล้เคียงกับ
โปรแกรมประชุมทางไกลอื่น เช่น การแชร์หน้าจอ การทำงาน



สามารถที่จะใช้งาน Microsoft Team ได้ทันที

4. Line Meeting

เป็นแอปพลิเคชันด้านการสื่อสารอื่น ๆ นอกจากโปรแกรมสื่อสารและการประชุมเฉพาะทางที่มีอยู่ในตลาดแล้ว ผู้ให้บริการการสื่อสารข้อมูลส่วนบุคคล เช่น Line Facebook Messenger ก็พัฒนาการให้บริการประชุมกลุ่มขึ้นมาเช่นกัน Line จะใช้ชื่อว่า Line Meeting ซึ่งปรากฏอยู่ในโปรแกรม Line โดยผู้ใช้สามารถเชิญเพื่อนเข้าประชุมได้ทันทีโดยไม่ต้องสร้างกลุ่มและไม่จำเป็นต้องเป็นเพื่อนกันใน Line เพียงแต่มีลิงก์หรือ QR Code ที่เชิญ

เช่น การควบคุมเสียงผู้เข้าประชุมโดยแฮนด์ เบนตัน

5. Messenger Rooms

เป็นความสามารถที่เพิ่มขึ้นมาใน Facebook Messenger ให้สามารถสร้างห้องประชุมออนไลน์ ซึ่งรองรับการประชุมได้พร้อมกันถึง 50 คน ไม่จำกัดเวลา โดยมีความสามารถพิเศษคือการมีสติ๊กเกอร์สนุก ๆ พร้อมด้วยระบบ AR ซึ่งผู้ใช้งานสามารถแชร์ข้อมูลของการประชุมผ่าน Room ได้ผ่าน News Feed ของ Facebook โดยตรง หรือจะเข้าไปแชร์ที่ Group หรือ Event ของ Facebook

จากการที่มีโปรแกรมประยุกต์ด้านการสื่อสารให้เลือกหลากหลายโดยแต่ละโปรแกรมจะมีข้อดีข้อเสียที่แตกต่างกัน ดังนั้นผู้ใช้งานหรือองค์กรจะต้องพิจารณาเลือกโปรแกรมที่เหมาะสมกับตนเองมากที่สุดโดยข้อพิจารณาหลักจะประกอบไปด้วย

1. ผู้เข้าร่วมประชุมมีความพร้อมที่จะใช้โปรแกรมใด เช่น การประชุมที่จัดขึ้นเป็นประจำภายในองค์กร ผู้ใช้น่าจะมีความพร้อม

สามารถเรียนรู้การใช้โปรแกรมสำหรับการประชุมมาตรฐาน เช่น Zoom หรือถ้าหน่วยงานที่มีการใช้งาน office 365 อยู่แล้วก็ควรจะใช้ Microsoft Team เพื่อให้เกิดประโยชน์สูงสุดแต่ถ้าเป็นการประชุมกับบุคคลภายนอกเป็นครั้งคราวอาจจะเลือกใช้ระบบง่ายที่บุคคลทั่วไปมีใช้อยู่แล้วเช่น การประชุมผ่าน Line เป็นต้น

2. รูปแบบและระยะเวลาการประชุม เป็นการประชุมที่ต้องการความร่วมมือหรือเป็นทางการและสำคัญในการนำเสนอ หน่วยงานจำเป็นจะต้องใช้โปรแกรมที่สามารถควบคุมการประชุมได้เป็นอย่างดี เช่นการปิดเสียงของผู้เข้าร่วมประชุมเพื่อให้ผู้เข้าประชุมได้รับฟังเสียงจากผู้นำการประชุมอย่างชัดเจน เป็นต้น

3. ปัจจัยอีกอย่างหนึ่งที่จะต้องคำนึงถึง คือ ระบบอินเทอร์เน็ตของผู้จัดการประชุมหรือโฮสต์โดย สำหรับการประชุมผ่านระบบคลาวด์ ผู้ที่เป็นโฮสต์ไม่จำเป็นจะต้องมีความเร็วอินเทอร์เน็ตสูงมากนักแต่ระบบจะต้องมีเสถียรภาพที่ดี มีความเร็วคงที่ โดยความเร็วที่เหมาะสมเริ่มที่ประมาณ 4 Mbps ขึ้นไป

4. ควรเตรียมตัวก่อนการประชุม เช่น หาที่ไม่มีเสียงรบกวน มีแสงสว่างพอเหมาะ และมีความเป็นส่วนตัวพอสมควร

5. เพื่อประสิทธิภาพในการสื่อสาร ผู้เข้าร่วมประชุมทุกคนควรใช้หูฟังและ Microphone หรือหากใช้ลำโพงภายนอกต้องปิดเสียงก้องหรือ



4. หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่อง

อินเทอร์เน็ตจะต้องมีความตระหนักรู้ เพื่อสามารถป้องกันข้อมูลส่วนตัวและลดความเสี่ยงในการใช้งาน โดยได้ประยุกต์

แนวทางจากที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(องค์การมหาชน) (สพธอ.) และคำแนะนำและแนวทางปฏิบัติด้าน
Password จากเอกสาร NIST Special Publication
800-63B Rev3 ของสถาบันมาตรฐานและเทคโนโลยีแห่ง
ชาติสหรัฐฯ (National Institute of Standards and
Technology: NIST) โดยมีข้อแนะนำ ดังนี้

4.1 การตั้งรหัสผ่านที่คาดเดาได้ยาก

โดยทั่วไปเพื่อความมั่นคงปลอดภัยควรตั้งรหัสผ่านอย่างน้อย 8 ตัวอักษร รหัสผ่านยิ่งยาวยิ่งเดายากหลีกเลี่ยงการตั้งรหัสผ่านด้วยหมายเลขโทรศัพท์ ชื่อเล่น ชื่อสัตว์เลี้ยง หรือคำพูดใดก็ตามที่สามารถระบุตัวตนของเราได้ วิธีการตั้งรหัสผ่านที่เดายาก

1. ในการตั้งรหัสผ่านควรมีตัวเลขประกอบด้วย การตั้งรหัสผ่านที่ดีควรประกอบไปด้วย

1) ตัวอักษรพิมพ์เล็ก

3) ตัวเลข

2) ตัวอักษรพิมพ์ใหญ่

4) ตัวอักษรพิเศษ

ผสมกัน

โดยมีความยาวอย่างน้อย 8 ตัวอักษรขึ้นไป ยกตัวอย่างเช่น การนำประโยคในเนื้อเพลงมาเปลี่ยนแปลงรูปแบบตามหลักการทั้ง 4 รูปแบบ จะทำให้รหัสผ่านนั้นมีความยากในการคาดเดาจากผู้ไม่ประสงค์ดี ตัวอย่างเช่น ประโยคเดิม คือ all my Yesterday เรียบเรียงใหม่เป็น A11mYe47erd@y หรือประโยคเดิม ผมรักคุณมากนะครับ เรียบเรียงใหม่เป็น z,iyd86l,kdot8iy[เป็นต้น

โปรดจำไว้

ความยาวของรหัสผ่านสำคัญกว่าความยาก เนื่องจากยิ่งรหัสผ่านยาวยิ่งเดารหัสผ่านได้ยาก การบังคับให้รหัสผ่านใหม่มีความยากกลับยิ่งทำให้ความมั่นคงปลอดภัยลดลง เพราะผู้ใช้อาจเพิ่มตัวอักษรบางตัวลงไป หรืออาจทำการจดบันทึกไว้เนื่องจากจำไม่ได้และใช้รหัสผ่านซ้ำกันกับระบบอื่น

2. ไม่จำเป็นต้องรีเซตรหัสผ่านใหม่ทุก 3 เดือนหรือ 6 เดือน เนื่องจากการจดจำรหัสผ่านดี ๆ ถือเป็นเรื่องยากอยู่แล้ว เมื่อต้องมี

หลาย ๆ รหัสผ่านที่ต้องจำ อาจทำให้ผู้ใช้เพิ่มตัวอักษรบางตัวลง และใช้รหัสผ่าน



อย่างไรก็ตาม อาจยังคงมีนโยบายการรักษาความมั่นคงปลอดภัยของบางองค์กรที่

อนุญาตตาม แต่ยังคงมีการพิจารณาและแนะนำที่ไม่บังคับให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านบ่อย ๆ แต่ให้เปลี่ยนเฉพาะในกรณีที่จำเป็น เช่น พบว่าข้อมูลรั่วไหล หรือพบการล็อกอินที่ผิดปกติ

3. ะมัดระวังการใส่รหัสผ่านบนเครื่องคอมพิวเตอร์สาธารณะหรือเครื่องคอมพิวเตอร์ของบุคคลอื่น

4. ควรตั้งรหัสผ่านสำหรับการทำงานกับบัญชีธนาคารออนไลน์ ไม่ซ้ำกับบัญชีเว็บ อีเมล เว็บเกมหรือแม้กระทั่งเว็บเครือข่ายสังคมออนไลน์

4.2 คำแนะนำในการพิสูจน์ตัวตนด้วยรหัสผ่าน

NIST ได้ให้คำแนะนำการใช้พิสูจน์ตัวตนด้วยรหัสผ่านเมื่อผู้ใช้ทำการล็อกอิน ดังนี้

1. เปิดใช้งาน “แสดงรหัสผ่านขณะพิมพ์” ควรเปิดให้มีฟีเจอร์ “แสดงรหัสผ่านขณะพิมพ์” เพื่อเพิ่มโอกาสให้ผู้ใช้พิมพ์รหัสผ่านยาว ๆ ได้ถูกต้องในทีเดียว

2. เปิดให้ “วาง” รหัสผ่านในช่องที่ต้องกรอกได้ ยิ่งการใส่รหัสผ่านทำได้ง่าย ผู้ใช้ยิ่งมีแนวโน้มที่จะตั้งรหัสผ่านยาวและยากมากยิ่งขึ้น การเปิดให้ “คัดลอก” และ “วาง” รหัสผ่านในช่องที่ต้องกรอกได้จึงเป็นผลดีมากกว่า

3. ใช้การป้องกันรหัสผ่านรั่วไหล ต้องมีการตรวจสอบรหัสผ่านใหม่กับรายการแบล็กลิสต์ เช่นคำในพจนานุกรม คำที่ใช้ตัว

อักษรเรียงกัน คำที่ใช้เป็นชื่อต่าง ๆ ข้อความที่มักใช้บ่อย หรือรหัสผ่านที่เคยหลุดออกมาสู่สาธารณะ การใช้เครื่องมือตรวจสอบรหัสผ่านที่เคยรั่วไหลก็เป็นทางเลือกที่ช่วยให้การตั้งรหัสผ่านใหม่มีความมั่นคงปลอดภัยมากยิ่งขึ้น

4. ใช้การพิสูจน์ตัวตนแบบ 2 ปัจจัย (2-Factor Authentication: 2FA) หรือตรวจสอบสิทธิ์แบบหลายปัจจัยได้ (Multi-factor authentication: MFA) ใช้การยืนยันตัวตน 2 จาก 3 ปัจจัยต่อไปนี้เพื่อทำการพิสูจน์ตัวตน

1) สิ่งที่คุณรู้ (Something you know) เช่น รหัสผ่าน หรือพิน

2) สิ่งที่คุณมี (Something you have) เช่น มือถือ หรือโทเค็น

3) สิ่งที่คุณเป็น (Something you are) เช่น ลายนิ้วมือ หรือสแกนใบหน้า

เช่น ใช้รหัสผ่าน (สิ่งที่คุณรู้) และใช้รหัสผ่านครั้งเดียว (One



... (สิ่งที่คุณมี) หรือลายนิ้วมือ (สิ่งที่คุณเป็น) ปัจจัยยังมีความปลอดภัยสูงมาก โดยต้องใช้ 8 ตัวอักษร

... MFA ... ควรกำหนดให้ตั้งรหัสผ่านที่มีความยาวไม่ต่ำกว่า 14 ตัวอักษร

เป็นการหลอกลวงในรูปแบบการปลอมแปลง อีเมล หรือข้อความที่สร้างขึ้นหลอกให้ผู้ใช้งานเปิดเผยข้อมูลทางการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น บัญชีใช้งานและรหัสผ่าน (Username/Password), ข้อมูลบัตรเครดิต หรือหมายเลขบัตรประจำตัวอื่น ๆ โดยอ้างว่าที่ผู้ใช้งานอาจเคยติดต่อ เช่น เว็บไซต์ธนาคารเว็บไซต์ที่เคยซื้อขายสินค้าบริการยืนยันข้อมูลส่วนตัวให้เป็นปัจจุบัน โดยอ้างให้เข้าใจผิดว่าหากไม่ดำเนินการอาจก่อให้เกิดความเสียหายต่าง ๆ โดยคนร้ายมักใส่ hyperlink ให้ดูเหมือน

URL ขององค์กรนั้น ๆ โดยเป็นเว็บไซต์ปลอม (Spoofed Website) เพื่อหลอกให้กรอกข้อมูลลงไป

วิธีป้องกัน ไม่ควรใช้ลิงก์ในอีเมลเพื่อเข้าใช้งานยังเว็บไซต์ และหากผู้ใช้งานสงสัยควรติดต่อทางโทรศัพท์ไปยังองค์กรนั้น ๆ โดยตรงและควรใช้งานผ่านการพิมพ์ URL ขององค์กรนั้นใหม่ ทุกครั้งที่ใช้งาน

4.4 วิธีป้องกันการถูกขโมยข้อมูลส่วนบุคคล

1. ตรวจสอบรายการใช้งานอยู่เสมอในการใช้งานเว็บไซต์ต่าง ๆ ที่ต้องกรอกข้อมูลและรหัสผ่านก่อนใช้งานทุกครั้งจะมีข้อมูลประวัติการใช้งานของเรา จึงควรตรวจสอบประวัติข้อมูลการใช้งานเพื่อสังเกตความผิดปกติ

2. หลีกเลี่ยงการใช้ข้อมูลส่วนตัวที่มากเกินไปในการทำธุรกรรมทางเว็บไซต์ควรหลีกเลี่ยงการให้ข้อมูลส่วนตัวเกินจำเป็น เนื่องจากหากให้ข้อมูลส่วนตัวของเรามากก็就会有ความเสี่ยงมากขึ้น

3. ระมัดระวังอีเมลที่สอบถามข้อมูลส่วนบุคคล หากได้รับอีเมลจากบุคคลที่ไม่รู้จัก สอบถามเกี่ยวกับข้อมูลส่วนบุคคลไม่ควรตอบข้อมูลส่วนบุคคลกลับทางอีเมลและหากอีเมลดังกล่าวมาจากธนาคารหรือองค์กรที่เราเคยใช้บริการ ก็ควรติดต่อสอบถามทางโทรศัพท์เพื่อให้มั่นใจว่าไม่ถูกหลอกสอบถามข้อมูลส่วนบุคคลทางอีเมล

4. ควรระมัดระวัง Wi-Fi Hotspot ปลอม ซึ่งเป็นภัยคุกคาม



ที่สร้างขึ้นโดยแฮกเกอร์เพื่อล่อลวงผู้ใช้ให้เชื่อมต่อและขโมยข้อมูลส่วนตัวของผู้ใช้ ในที่สาธารณะหรือที่ทำงาน ควรระวังการเชื่อมต่ออินเทอร์เน็ตโดยไม่ทราบแหล่งที่มาของเครือข่าย Wi-Fi หรือใช้เครือข่าย Wi-Fi ที่ไม่ปลอดภัย เช่น ร้านกาแฟ หรือที่สาธารณะ หากจำเป็นต้องเชื่อมต่อ ควรตรวจสอบชื่อเครือข่าย Wi-Fi และรหัสผ่านก่อนเชื่อมต่อ และควรใช้ VPN เพื่อเพิ่มความปลอดภัย

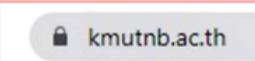
5. ทำลายเอกสารที่มีข้อมูลส่วนบุคคล ควรระมัดระวังเอกสารหรือจดหมายส่วนตัวที่ระบุข้อมูลส่วนบุคคล เช่น หมายเลขบัตรเครดิต บัญชีผู้ใช้งาน หรือแม้แต่การแจ้งรหัสผ่านทางจดหมาย ควรเก็บรักษาในที่ปลอดภัยจากบุคคลภายนอก และหาก

ไม่มีความจำเป็นต้องเก็บไว้เป็นหลักฐานหรือช่วยเตือนความจำเป็นควรทำลายในลักษณะไม่สามารถนำกลับมาอ่านใหม่ได้ เช่น การย่อยทำลายเอกสารให้เป็นชิ้นเล็ก เป็นต้น

4.5 วิธีป้องกันการถูกฉ้อโกงทางเว็บไซต์

1. ศึกษาข้อมูล ความน่าเชื่อถือในสินค้าและผู้ขาย อาจใช้วิธีการส่งอีเมล หรือโทรศัพท์ไปสอบถามรายละเอียดสินค้าหรือบริการ เพื่อสังเกตความรวดเร็วในการตอบกลับและการมีตัวตนเองของธุรกิจนั้น ๆ และทำการค้นหารีวิวเพิ่มเติมเกี่ยวกับสินค้า บริการ หรือผู้ขายรายนั้น ๆ ในอินเทอร์เน็ต

2. การจ่ายชำระเงินผ่านระบบควรสังเกตว่าระบบดังกล่าวมีความมั่นคงปลอดภัยหรือเข้ารหัสเสมอหรือไม่ เช่น อาจสังเกตจาก https หรือเครื่องหมายแม่กุญแจที่ปรากฏบนเว็บไซต์ที่ใช้งานอยู่

สัญลักษณ์ https เมื่อเปิดจากเว็บเบราว์เซอร์ที่แตกต่างกัน	เว็บเบราว์เซอร์ที่ใช้งาน
	Google Chrome
	Mozilla Firefox
	Microsoft Edge

ภาพสัญลักษณ์ https เมื่อเปิดจากเว็บเบราว์เซอร์ที่แตกต่างกัน

3. หากสามารถเลือกชำระเงินแบบบัตรเดบิต (Debit Card) หรือบัตรเครดิต (Credit Card) ก็ควรเลือกชำระใช้บัตรเครดิตเสมอ เนื่องจากหากมีปัญหาในตัวสินค้าที่สั่งซื้อ เจ้าของบัตรอาจจะสามารถปฏิเสธการชำระเงินได้ ในขณะที่กรณีบัตรเดบิตมีความเสี่ยงกว่าเนื่องจากจะถูกหักเงินจากบัญชีเงินฝากธนาคารทันทีที่ชำระผ่านบัตรเดบิต รวมทั้งควรตรวจสอบใบแจ้งหนี้ทุกรอบบัญชี เพื่อตรวจสอบรายการที่อาจผิดปกติ

4. ศึกษาว่าเว็บไซต์ที่กำลังจะซื้อสินค้าหรือบริการดังกล่าวมีกฎระเบียบเกี่ยวกับการรับประกันความพึงพอใจในสินค้าหรือไม่ มีนโยบายการรับคืนและคืนเงินทันทีเมื่อลูกค้าแจ้งความไม่พอใจในสินค้าหรือไม่

5. ใช้ความระมัดระวังอย่างสูงหากพบการเสนอขายสินค้า



สรุปท้ายหน่วย

การที่เราจะใช้ประโยชน์จากคอมพิวเตอร์ได้ นอกจากจะมี

ที่ต้องคำนึงถึงโดยเฉพาะการใช้งานโปรแกรมประยุกต์บนระบบ
เครือข่ายก็คือ ความมั่นคงปลอดภัยของระบบงานและข้อมูลที่ถูก
รับส่งหรือถูกบันทึกไว้บนระบบเครือข่าย เพราะข้อมูลเหล่านี้อาจ
จะเป็นความลับทางการค้า รหัสผ่านการทำ
ธุรกรรมการเงิน ซึ่งหากหลุดไปยังบุคคลที่ไม่ประสงค์ดีก็จะสร้าง
ความเสียหายแก่ผู้ใช้ และองค์กรอย่างมหาศาล