

บริการออนไลน์ไทย ปลอดภัยแค่ไหน?

รายงานผลสำรวจมาตรการรักษาความปลอดภัยและคุ้มครองความเป็นส่วนตัวของเว็บไซต์ไทย ครั้งที่ 1

เมษายน 2557

โครงการวิจัยความเป็นส่วนตัวออนไลน์¹ เครือข่ายพลเมืองเน็ต ทดลองสำรวจมาตรการรักษาความปลอดภัยและการคุ้มครองความเป็นส่วนตัวของผู้ให้บริการออนไลน์ต่างๆ ของประเทศไทย ในระดับ ‘เบื้องต้น’ ครั้งที่ 1² เพื่อเป็นข้อมูลแก่ผู้ใช้ทั่วไปในการตัดสินใจใช้บริการต่างๆ และเพื่อกระตุ้นผู้ให้บริการออนไลน์ให้ตระหนักถึงความสำคัญของการปกป้องความปลอดภัยและความเป็นส่วนตัวของผู้ใช้บริการมากขึ้น

การสำรวจครั้งนี้มุ่งไปที่ผู้ให้บริการสำคัญในด้านต่างๆ จำนวน 50 เว็บไซต์ซึ่งคัดเลือกจากผู้ให้บริการออนไลน์ที่ได้รับความนิยมในประเภทต่างๆ ได้แก่หน่วยงานรัฐ การเงินธนาคาร การศึกษา การคมนาคมขนส่ง ชื้อขายสินค้า และบริการรับสมัครงาน แล้วจึงประเมินว่าบริการเหล่านี้มีความปลอดภัยและคุ้มครองความเป็นส่วนตัวของผู้ใช้ในระดับใด โดยเก็บบันทึกข้อมูลระหว่างเดือนตุลาคม 2556 -มกราคม 2557

เกณฑ์ที่ใช้ในการประเมิน

ในโลกอินเทอร์เน็ตการป้องกันการดักฟังที่พื้นฐานที่สุด คือ การเข้ารหัส ข้อมูลทั้งหมดที่ส่งไปจากเครื่องต้นทางไปยังเครื่องปลายทางนั้น แม้อาจจะถูกดักฟังได้ระหว่างทาง แต่ผู้ที่ดักฟังก็จะได้ข้อมูลที่อ่านแล้วไม่เข้าใจ การเข้ารหัสมีหลายรูปแบบและแต่ละแบบมีข้อจำกัดแตกต่างกัน การดักฟังไม่ได้มีเป้าหมายเพื่อจารกรรมข้อมูลสำคัญเท่านั้น แต่ยังมีจุดประสงค์เพื่อตรวจสอบพฤติกรรมทั่วไป เช่น การใช้เว็บค้นหา (search engine) ที่ผู้ให้บริการอินเทอร์เน็ตบางราย (Internet Service Provider: ISP) อาจดักฟังข้อมูลลูกค้า เมื่อลูกค้าใช้งานเว็บค้นหาเพื่อดูว่าลูกค้าค้นหาอะไรบ้างในอินเทอร์เน็ต และนำข้อมูลเหล่านี้ไปวิเคราะห์เพื่อประโยชน์ทางการตลาด

การสำรวจนี้เป็นการประเมินระดับความปลอดภัยของเว็บไซต์ขั้นพื้นฐานที่สุด และผู้ใช้อินเทอร์เน็ตทั่วไปสามารถตรวจสอบได้ด้วยตนเอง จากข้อมูลที่ผู้ใช้ทั่วไปเข้าถึงได้ อย่างไรก็ตาม ผลวิจัยที่ได้ไม่สามารถยืนยันได้ว่าเว็บไซต์เหล่านี้ปลอดภัยอย่างสมบูรณ์ เนื่องจากยังมีปัจจัยอื่นๆ ที่เกี่ยวข้อง และการตรวจสอบระบบความปลอดภัยในขั้นสูงไม่สามารถกระทำได้จากบุคคลภายนอก

ผลสำรวจครั้งต่อไปซึ่งจะมีการเพิ่มตัวชี้วัดที่ในการประเมินเพิ่มมากขึ้น เช่น นโยบายการตั้งรหัสผ่าน นโยบายกักเก็บบัญชีผู้ใช้ การผูกกับเว็บภายนอก เป็นต้น

ในเบื้องต้นโครงการวิจัยความเป็นส่วนตัวฯ สำรวจด้วยการพิจารณาว่า

1. เว็บไซต์มีการเชื่อมต่อแบบ HTTPS:// หรือไม่ ซึ่งจะแสดงให้เห็นว่าผู้ให้บริการออนไลน์ใช้การเข้ารหัสข้อมูลที่ส่งระหว่างเว็บเบราว์เซอร์และเว็บเซิร์ฟเวอร์ (เข้ารหัสจากต้นทางถึงปลายทาง) เพื่อคุ้มครองข้อมูลของผู้ใช้บริการหรือไม่ และพิจารณา

¹ สนับสนุนโดย ไพรเวซี อินเตอร์เนชันแนล (Privacy International) ภายใต้ชุดโครงการ Surveillance and Freedom: Global Understandings and Rights Development (SAFEGUARD)

² ผลสำรวจครั้งต่อไปซึ่งจะมีการเพิ่มตัวชี้วัดที่ในการประเมินเพิ่มมากขึ้น เช่น นโยบายการตั้งรหัสผ่าน นโยบายกักเก็บบัญชีผู้ใช้ การผูกกับเว็บภายนอก เป็นต้น

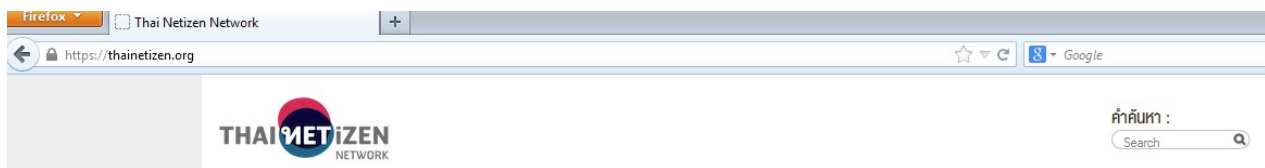
ว่าการเข้ารหัสนี้มีความปลอดภัยอยู่ในระดับใดจากเทคโนโลยีที่เรียกว่า SSL (Secure Sockets Layer) หรือ Transport Layer Security (TLS) ว่าเป็นรุ่น SSL 3.0 หรือ TLS 1.0 ขึ้นไปหรือไม่

2. **กุญแจการเข้ารหัสมีความยาว 256 บิตหรือไม่** ความยาวของกุญแจเข้ารหัสมีหน่วยเป็นบิต ยิ่งกุญแจมีความยาวมาก โอกาสที่ผู้บุกรุกจะคาดเดากุญแจที่ถูกต้องก็ยิ่งยากขึ้นตามไปด้วย ดังนั้นในการสำรวจครั้งนี้จึงถือว่าการเข้ารหัส 256 บิต มีความปลอดภัยมากกว่าการเข้ารหัสแบบ 128 บิต

3. **แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจนหรือไม่** พิจารณาว่าเว็บไซค์มีนโยบายความเป็นส่วนตัวหรือไม่ และชัดเจนหรือไม่ โดยดูจากการใช้คำและตำแหน่งที่ถูกจัดวางในเว็บไซค์ว่าสามารถเข้าถึงได้อย่างไร

วิธีตรวจสอบการเข้ารหัสของเว็บไซต์

1. ตรวจสอบว่าการเชื่อมต่อกับเว็บไซต์นั้นมีการเข้ารหัส HTTPS หรือไม่ ผ่านข้อมูลที่ระบุในเบราว์เซอร์ และตรวจสอบว่าการเข้ารหัสเป็น SSL/TLS รุ่นใด ด้วยการทดสอบผ่านเว็บไซต์ SSL Server Test (<https://www.ssllabs.com/ssltest>) ซึ่งเป็นบริการวิเคราะห์โครงสร้างของเว็บที่เข้ารหัส SSL/TLS ทุกประเภทบนอินเทอร์เน็ต และเป็นโครงการวิจัยที่ไม่แสวงหาผลประโยชน์ทางการค้า
2. ตรวจสอบความยาวของกุญแจเข้ารหัสว่าเป็น 256 บิต หรือไม่ ผ่านข้อมูลที่ระบุในเบราว์เซอร์



ตัวอย่างเว็บไซต์ที่มีการเข้ารหัส HTTPS ซึ่งมีเครื่องหมายรูปแม่กุญแจอยู่หน้า url

ตารางเปรียบเทียบ สรุปผลการประเมินความปลอดภัยพื้นฐานของเว็บไซต์

- เว็บไซต์ที่มีการเข้ารหัสด้วย HTTPS และ SSL รุ่น 3.0 หรือ TLS 1.0 หรือสูงกว่า ได้ 1 คะแนน; เว็บไซต์ที่มีการเข้ารหัสด้วย HTTPS และ SSL ต่ำกว่า 3.0 ได้ 0.5 คะแนน
- เว็บไซต์ที่มีความยาวกุญแจเข้ารหัส 256 บิต ได้ 1 คะแนน; 128 บิต ได้ 0.5 คะแนน
- เว็บไซต์ที่แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน ได้ 1 คะแนน; มีแต่ไม่ชัดเจน ได้ 0.5 คะแนน

1. หน่วยงานรัฐ

เว็บไซต์	เข้ารหัสด้วย HTTPS	กุญแจยาว 256 บิต	แสดงนโยบาย ความเป็นส่วนตัว ชัดเจน
 สำนักงานคณะกรรมการอาหารและยา	★	★	★
 กรมสุขภาพจิต สำนักงานบริหารสุขภาพเฉพาะกิจ	★	★	☆
 กรมการขนส่งทางบก	★	★	☆
 การไฟฟ้านครหลวง Metropolitan Electricity Authority	★	★	☆
 สำนักงานประกันสังคม Social Security Office	☆	☆	★
 ศูนย์ กกม.1556 กกต. 1556	☆	☆	☆
 สำนักงานกฤษฎีกา www.1111.go.th	☆	☆	☆
 สำนักงานคณะกรรมการคุ้มครองผู้บริโภค Office of the Consumer Protection Board	☆	☆	☆

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ

2. ธนาคาร

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฎหมาย 256 บิต	แสดงนโยบายความเป็นส่วนตัวชัดเจน
	★	★	★
	★	☆	★
	★	☆	★
	★	☆	★
	★	☆	★
	★	☆	★
	★	☆	★
	★	☆	★
	★	☆	★

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ









































3. คมนาคมขนส่ง

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฎหมาย 256 บิต	แสดงนโยบาย ความเป็นส่วนตัว ชัดเจน
	★	★	★
	★	★	★
	★	★	★
	★	★	★

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฎหมาย 256 บิต	แสดงนโยบาย ความเป็นส่วนตัว ชัดเจน
	☆	☆	☆
	☆	☆	☆
	☆	☆	☆

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ

4. สถาบันการศึกษา: การรับสมัครสอบเข้ามหาวิทยาลัย

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฎหมาย 256 บิต	แสดงนโยบายความเป็นส่วนตัวชัดเจน
			
			
			
			
			
			
			
			
			
			

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ

5. เว็บไซต์ขายสินค้าออนไลน์

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฏหมาย 256 บิด	แสดงนโยบาย ความเป็นส่วนตัว ชัดเจน
			
			
			
			
			
			
			
			
			
			
			
			

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ

6. บริการจัดหางาน

เว็บไซต์	เข้ารหัสด้วย HTTPS	กฎหมาย 256 บิต	แสดงนโยบาย ความเป็นส่วนตัว ชัดเจน
			
			
			
			

หมายเหตุ: ตรวจสอบการเข้ารหัสจากหน้าลงทะเบียนของเว็บ

ผลการสำรวจความปลอดภัยเบื้องต้น

1.หน่วยงานรัฐ

บริการออนไลน์ที่เป็นหน่วยงานของรัฐส่วนใหญ่ เป็นการชำระภาษีและค่าธรรมเนียมต่างๆ รวมทั้งการรับเรื่องร้องเรียนจากประชาชน ได้แก่ กรมสรรพากรซึ่งรับยื่นภาษี กรมขนส่งทางบกซึ่งรับชำระภาษีรถยนต์ การไฟฟ้านครหลวงซึ่งรับจ่ายค่าบริการสำนักงานประกันสังคมและกองทุนให้กู้ยืมเงินเพื่อการศึกษาใช้ตรวจสอบข้อมูลส่วนตัวของสมาชิก ส่วนศูนย์รับเรื่องราวร้องทุกข์สำนักงานนายกรัฐมนตรี และระบบคุ้มครองผู้บริโภคฯ เป็นเว็บไซต์รับเรื่องร้องเรียน

ครึ่งหนึ่งของเว็บไซต์ภาครัฐที่สำรวจมีการเชื่อมต่อแบบ HTTPS ยกเว้นเว็บที่อยู่ในกลุ่มรับเรื่องเรียนทั้งหมดที่ไม่ได้เข้ารหัสข้อมูลที่ส่งระหว่างเว็บเบราว์เซอร์และเว็บเซิร์ฟเวอร์ ทั้งที่ผู้ร้องเรียนต้องกรอกข้อมูลส่วนตัวที่สามารถระบุตัวตนของตนเองลงไป

เว็บไซต์กรมสรรพากรที่รับยื่นภาษี ยังมีการเข้ารหัส SSL รุ่น 2.0 ซึ่งมีความปลอดภัยต่ำ ที่ไม่สามารถป้องกันการดักข้อมูลระหว่างทางได้

5 เว็บไซต์จาก 8 เว็บไซต์ที่ไม่มีนโยบายความเป็นส่วนตัว หรือคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ

การกำกับดูแลเว็บไซต์ของหน่วยงานรัฐเกี่ยวข้องกับพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 มาตรา 23 ที่กำหนดให้ หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล รวมทั้งจัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูลด้วย นอกจากนี้ยังมีพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 5 ที่กำหนดว่า หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ตารางที่ 1 ผลการประเมินเว็บไซต์หน่วยงานรัฐ และรัฐวิสาหกิจ

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
1.กองทุนเงินให้กู้ยืมเพื่อการศึกษา	https://www2.studentloan.or.th/SLFSTUDENT/jsp/reg/REGBE0001.jsp	/	128	มี หน้าแรก ด้านบน
2.กรมสรรพากร	https://epit.rd.go.th (หน้าลงทะเบียน)	/ แต่ยังใช้ SSL 2.0 ด้วย ซึ่งไม่ปลอดภัย	256	ไม่มี
3.กรมขนส่งทางบก	https://www.dlte-serv.in.th/dltWeb/dlt/tax/PrepareRegisterAction.do	/	128	ไม่มี
4.การไฟฟ้านครหลวง	https://eservice.mea.or.th/eservice/register/regis_form.php การลงทะเบียน	/ แต่ยังใช้ SSL 2.0 ด้วย ซึ่งไม่ปลอดภัย	256	ไม่มี
5.สำนักงานประกันสังคม	http://www.sso.go.th/wpr/memberAction.do?method=register&webId=0 การลงทะเบียน	X	X	มี อยู่ในหน้าลงทะเบียนหัวข้อ นโยบายการคุ้มครองสิทธิข้อมูลส่วนบุคคล
6.ศูนย์รับเรื่องราวร้องทุกข์ กทม.	http://203.155.220.105/rongtook/html/rongtook2.html หน้าส่งเรื่องร้องทุกข์	X	X	ไม่มี
7.สำนักงานรัฐมนตรี	http://www.1111.go.th/form.aspx หน้าส่งเรื่องร้องทุกข์	X	X	ไม่มี
8.ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	http://complain.ocpb.go.th/	X	X	มี นโยบายการคุ้มครองข้อมูลส่วนบุคคล ใน

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
สำนักงานคณะกรรมการคุ้มครองผู้บริโภค				หน้าแรกแต่กดแล้วไม่เชื่อมต่อกับหน้าใดๆ

2. ธนาคาร

บริการออนไลน์ของธนาคารเป็นการทำธุรกรรมทางการเงินด้วยระบบออนไลน์ทั้งหมด ได้แก่ การฝาก-ถอน การชำระค่าบริการต่างๆ เพื่อให้ลูกค้าได้ทำธุรกรรมด้วยตนเองได้สะดวกสบาย โดยไม่จำเป็นต้องเดินทางไปที่ธนาคาร จากข้อมูลของธนาคารแห่งประเทศไทยในปี พ.ศ. 2556 มีจำนวนบัญชีที่ทำธุรกรรมทางอินเทอร์เน็ตราว 7 ล้านบัญชี ซึ่งเพิ่มขึ้นจากปี 2556 1 ล้านบัญชี (ธนาคารแห่งประเทศไทย 2556)

ทุกธนาคารมีการเข้ารหัสด้วย HTTPS ใช้ SSL รุ่น 3.0 ทั้งหมด มีความยาวกุญแจเข้ารหัส 128 บิต ยกเว้นเว็บไซต์ธนาคารกรุงเทพ ใช้การเข้ารหัสแบบ 256 บิต

ในส่วนโยบายความเป็นส่วนตัว แม้ทุกธนาคารจะมีนโยบายความเป็นส่วนตัว แต่มีการใช้คำและจัดวางในตำแหน่งที่แตกต่างกัน โดยอาจแบ่งได้เป็น 2 รูปแบบ คือ เว็บไซต์ธนาคารที่ใช้คำว่าความเป็นส่วนตัว หรือ privacy วางอยู่ในแถบด้านล่างหน้าแรกของเว็บไซต์ และเว็บไซต์ธนาคารที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอยู่ในหัวข้อนโยบายความปลอดภัย ที่วางอยู่ในแถบด้านล่าง หน้าแรกของเว็บไซต์

ธนาคารออนไลน์ที่เป็นบริการทางการเงิน เกี่ยวข้องกับพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551 ในพระราชกฤษฎีกานี้กำหนดให้ผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ต้องปฏิบัติตามประกาศธนาคารแห่งประเทศไทยที่ สรข. 3/2552 เรื่องนโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ ซึ่งกำหนดให้ผู้ให้บริการต้องมีมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับการให้บริการชำระเงินทางอิเล็กทรอนิกส์ให้สอดคล้องกับนโยบายที่กำหนดขึ้น และมาตรการดังกล่าวจะต้องเหมาะสมกับลักษณะของธุรกิจ โดยครอบคลุมถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนของผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้องเชื่อถือได้ของระบบสารสนเทศ ดังนั้นเว็บไซต์ธนาคารจึงต้องมีระบบเข้ารหัสเพื่อรักษาความปลอดภัยในการให้บริการให้ได้มากที่สุด

ตารางที่ 2 ผลการประเมินเว็บไซต์ธนาคาร

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
9. ธนาคารกรุงเทพ	https://ibanking.bangkokbank.com/Register/SignUp.aspx		256	มี ในนโยบายการรักษาความปลอดภัย ด้านล่างของหน้าแรก
10. ธนาคารกรุงไทย	https://www.ktbnetbank.com/th/		128	มี ใน <i>privacy</i> ด้านล่างของหน้าแรก
11. ธนาคารกสิกรไทย	https://online.kasikornbankgroup.com/K-Online/onlineRegistration.do		128	มี ใน นโยบายความเป็นส่วนตัว ด้านล่างของหน้าแรก
12. ธนาคารไทยพาณิชย์	https://www.scbeasy.com/online/easynet/page/rgt/rgstatn_v2_01.aspx?LANG=th		128	มี ใน <i>privacy policy</i> ด้านล่างของหน้าแรก
13. ธนาคารออมสิน	https://ib.gsb.or.th/retail/FirstTimeLogin.do?event=ftl_login&action=ftl_login		128	มี ความเป็นส่วนตัวของลูกค้าด้านล่างของหน้าแรก
14. ธนาคารทหารไทย	https://www.tmbdirect.com/		128	มี หัวข้อ นโยบายด้านการรักษาความลับ ในนโยบายรักษาความปลอดภัย แบนเนอร์หน้าแรก
15. ธนาคารกรุงศรีอยุธยา	https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp		128	มี หัวข้อ การเฝ้าตรวจสอบควบคุม ใน ระบบรักษาความปลอดภัย ด้านล่างของหน้าแรก>>มาตรการรักษาความปลอดภัยที่

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
				ธนาคารเลือกใช้
16. ธนาคารธนชาติ	https://retailib.thanachartbank.co.th/retail/Login.do?action=form&lang=th_TH	/	128	มี การรักษาข้อมูลส่วนบุคคล ด้านล่างของหน้าแรก
17.ธนาคาร LH	https://www.lhbankspeedy.com/lh-rib/ib101/ibRegister.do?lang=th&method=executeTerms	/	128	มี ใน นโยบายความปลอดภัย ด้านล่างของหน้าแรก

3. การคมนาคมขนส่ง

ปัจจุบัน ผู้ให้บริการคมนาคมขนส่งมีระบบการสำรองที่นั่งและจำหน่ายบัตรโดยสารผ่านอินเทอร์เน็ตเป็นจำนวนมาก โดยเฉพาะสายการบิน การประเมินความปลอดภัยและความเป็นส่วนตัวของบริการคมนาคมขนส่งแบ่งออกเป็น 2 ประเภท คือบัตรโดยสารเครื่องบิน และบัตรโดยสารรถประจำทาง ซึ่งมีลักษณะเฉพาะที่แตกต่างกัน

3.1 บัตรโดยสารเครื่องบิน

การซื้อบัตรโดยสารเครื่องบินผ่านอินเทอร์เน็ต ขยายตัวอย่างรวดเร็วพร้อมกับการเติบโตของสายการบินต้นทุนต่ำในประเทศไทย ซึ่งส่งเสริมให้ซื้อบัตรโดยสารออนไลน์เพื่อประหยัดค่าใช้จ่ายมากกว่า

เว็บไซต์สายการบินทั้งหมดมีการเข้ารหัส HTTPS และเข้ารหัส SSL รุ่น 3.0 ทั้งหมด

แอร์เอเชีย เป็นเว็บเดียวที่ระบุชัดเจนว่า นโยบายความเป็นส่วนตัวส่วนตัว ในหน้าแรกของเว็บไซต์ ส่วนเว็บไซต์อื่นๆ แทรกอยู่ในนโยบายรักษาความปลอดภัย ที่แถบด้านล่าง หน้าแรกของเว็บไซต์ มีเพียงเว็บนกแอร์เท่านั้น ที่นโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแทรกอยู่ใน เงื่อนไขและข้อกำหนด ที่จะปรากฏให้เห็นเฉพาะขั้นตอนเลือกเที่ยวบิน

เนื่องจากเว็บไซต์สายการบินมีการทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ จึงต้องปฏิบัติตามประกาศธนาคารแห่งประเทศไทยที่ สรช. 3/2552 เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ตารางที่ 3 ผลการประเมินเว็บไซต์สายการบิน

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
18.แอร์เอเชีย	https://booking.airasia.com/Tra/veler.aspx	/	256	มี ใน นโยบายความเป็นส่วนตัว ส่วนตัว ด้านล่างของหน้าแรก
19. การบินไทย	https://wftc3.e-travel.com/plnext/tgpnnext/Override.action	/	256	มี ใน นโยบายการรักษาความปลอดภัย ด้านล่างของหน้าแรก
20. บางกอกแอร์เวย์	https://pg-prod.sabresonicweb.com	/	128	มี (ภาษาอังกฤษ) ใน ข้อมูลส่วนบุคคลและ ความปลอดภัย ด้านล่างของหน้าแรก
21. นกแอร์	https://www.nokair.com/nokco/nnext/asp/payment.aspx	/	256	มี ข้อมูลส่วนตัว อยู่ใน หน้า เลือกเที่ยวบิน>>เงื่อนไขและข้อกำหนด

3.2 บัตรโดยสารรถประจำทาง

บริการจองบัตรโดยสารด้วยรถประจำทาง แตกต่างจากบริการจำหน่ายบัตรโดยสารเครื่องบินตรงที่ผู้ซื้อไม่จำเป็นต้องใส่ข้อมูลส่วนตัวของตนเองอย่างละเอียด และส่วนใหญ่ไม่รับชำระเงินผ่านเว็บไซต์ ดังนั้นจึงไม่ให้ความสำคัญกับการเข้ารหัสข้อมูล และนโยบายความเป็นส่วนตัวส่วนตัวมากเท่าที่ควร

ตารางที่ 4 ผลการประเมินเว็บไซต์รับจองตั๋วรถโดยสารประจำทาง

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวชัดเจน
22. Thairoute	http://agent.thairoute.com/www.thairoute/modules/sales/customerinfo.php	X	X	X
23. บขส.	http://booking.busticket.in.th/availabletrip.php	X	X	X
24. Thaiticketmajor	http://www.thaiticketmajor.com/tickets/register.php?lang=th (หน้าสมัครสมาชิกเว็บไซต์ ที่มีการใส่ข้อมูลส่วนตัว)	X	X	X

4. สถาบันการศึกษา: เว็บไซต์รับสมัครเข้าศึกษาของมหาวิทยาลัย

ในการสำรวจครั้งนี้ใช้การสุ่มตัวอย่างเว็บไซต์รับสมัครเข้าศึกษาต่อระดับปริญญาตรี แบบรับตรงของมหาวิทยาลัยต่างๆ ทั้งในส่วนกลาง และภูมิภาค จำนวน 10 แห่ง และประเมินจากหน้าเว็บไซต์รับสมัครเป็นหน้าที่ผู้สมัครต้องกรอกข้อมูลส่วนตัวของตนเองลงไปทั้งหมด

มีเพียงมหาวิทยาลัยพระจอมเกล้า ธนบุรี และมหาวิทยาลัยสงขลานครินทร์เท่านั้น ที่มีการเข้ารหัสข้อมูลแบบ HTTPS ไม่มีมหาวิทยาลัยใดที่มีนโยบายความเป็นส่วนตัวชัดเจนเลย

ตารางที่ 5 ผลการประเมินเว็บไซต์มหาวิทยาลัย

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวชัดเจน
25. ศูนย์ทดสอบทางวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย	http://register.atc.chula.ac.th/ChulaATC/index.php?mod=applicant&op=register	X	X	X

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวตัวชัดเจน
26.สำนักทะเบียนและประมวลผล มหาวิทยาลัยธรรมศาสตร์	http://web.reg.tu.ac.th/registrar/appbioentryconfigregis.asp?f_cmd=88	X	X	X
27.มหาวิทยาลัยมหิดล	http://www.student.mahidol.ac.th/directadmission/ApplicationInput.asp?page=2&PID=1959800003355&AUser=&QuotaGroup=Q	X	X	X
28. มหาวิทยาลัยอัสสัมชัญ	http://its-1.au.edu/admission/index.php?item=thai&action=1	X	X	X
29. มหาวิทยาลัยหอการค้าไทย	http://202.28.9.143/registrar/appbioentryconfigregis.asp?f_cmd=88	X	X	X
30.คณะสถาปัตยกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์	http://www.direct.arch.ku.ac.th/rssystem/index.php	X	X	X
31.มหาวิทยาลัยพระจอมเกล้าธนบุรี	https://sinfo.kmutt.ac.th/New/Acis/public/admission/student/bachelorAppForm/appForm.jsf		256	X
32.มหาวิทยาลัยวลัยลักษณ์	http://quota.wu.ac.th/apply.asp?step=3	X	X	X
33. สงขลานครินทร์	https://admission.psu.ac.th/Members/	/ แต่ใช้ ssl 2 ตัว	X	X

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
34.ขอนแก่น	http://reg2.kku.ac.th/eregistration/centralsearch2557_new.asp	X	X	X

5. เว็บไซต์ซื้อขายสินค้าออนไลน์

5.1 เว็บไซต์ซื้อขายสินค้า

เว็บไซต์ที่เป็นศูนย์กลางในการติดต่อระหว่างผู้ซื้อและผู้ขาย ส่วนใหญ่แล้วไม่มีการทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ กระบวนการซื้อสินค้าใช้การโอนเงินนอกพื้นที่เว็บไซต์

ในกลุ่มนี้มีเพียงเว็บตลาดดอทคอม เพียงเว็บเดียวที่มีการเข้ารหัสแบบ HTTPS ซึ่งอาจจะเกี่ยวข้องกับการที่เป็นบริษัท ร่วมทุนกับบริษัท Rakuten จากประเทศญี่ปุ่น

นโยบายความเป็นส่วนตัวส่วนใหญ่จะไปปรากฏอยู่ในหน้าลงทะเบียนซึ่งต้องมีการกรอกข้อมูลส่วนตัวอย่างละเอียดของผู้ใช้บริการ ที่น่าสังเกตคือ เว็บไซต์ Weloveshopping แม้จะมีนโยบายคุ้มครองข้อมูลบุคคลที่แถบด้านล่างของหน้าแรก แต่เมื่อคลิกเข้าไปแล้ว กลับเชื่อมโยงไปที่เว็บอื่น

ตารางที่ 6 ผลการประเมินเว็บไซต์ซื้อขายสินค้าออนไลน์

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
35. Weloveshopping	http://www.weloveshopping.com/portal/sso/registerform.php?read&status=memonly	X	X	X ใน นโยบายคุ้มครองข้อมูลบุคคล ด้านล่างหน้าแรก แต่กดเข้าไปแล้วไม่พบรายละเอียด
36. Tarad.com	https://member.tarad.com/register	/	256	มี อยู่ใน เงื่อนไขและข้อตกลง หน้าลงทะเบียน
37. Pramool.com	http://www.pramool.com	X	X	ไม่มี หน้าลงทะเบียน

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวชัดเจน
	/cgi-bin/user.cgi?1&1&u			เขียนว่า 'ข้อมูลที่ถูกรวบรวมจะถูกรักษาไว้เป็นความลับ'
38. Dealfish (เปลี่ยนชื่อเป็น OLX)	http://www.olx.co.th/member/register	X	X	ใน หัวข้อ <i>ข้อมูลส่วนบุคคล (Privacy notes)</i> หน้าสมัครสมาชิกด้วยอีเมล >> เงื่อนไขการใช้บริการของเว็บไซต์

5.2 เว็บค้าปลีกออนไลน์

ก่อนที่จะซื้อสินค้าในเว็บค้าปลีกออนไลน์ ผู้ใช้บริการต้องสมัครสมาชิกก่อน ซึ่งในขั้นตอนนี้จำเป็นต้องกรอกข้อมูลส่วนตัวอย่างละเอียดก่อนที่จะซื้อสินค้าได้ การสำรวจนี้ประเมินความปลอดภัยในขั้นตอนการสมัครสมาชิกเท่านั้น

ร้อยละ 80 ของเว็บค้าปลีกออนไลน์มีการเข้ารหัส HTTPS ในหน้าลงทะเบียนสมัครสมาชิกเพื่อใช้บริการ ยกเว้นเว็บ TOPS และ Big C ที่ไม่มีการเข้ารหัส ระหว่างที่ลูกค้ากรอกข้อมูลส่วนตัวเพื่อสมัครสมาชิก

นโยบายความเป็นส่วนตัวส่วนตัวยูอยู่ในหน้าแรกของเว็บไซต์ Lazada และ Zalora ซึ่งอาจจะเกี่ยวข้องกับการที่ทั้งสองเว็บนี้เป็นบริษัทข้ามชาติ มีสาขาหลายประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ส่วนเว็บอื่นๆ ไม่ได้ใช้คำว่านโยบายข้อมูลความเป็นส่วนตัวโดยตรง แต่เป็นหัวข้อย่อยที่แทรกอยู่ในข้อตกลงการใช้บริการในหน้าลงทะเบียน

ตารางที่ 7 ผลการประเมินเว็บค้าปลีกออนไลน์

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวชัดเจน
39. Lazada	https://www.lazada.co.th/customer/account/create/	/	128	มี ใน <i>นโยบายความเป็นส่วนตัว</i> ด้านล่างของหน้าแรก
40. Zalora	https://www.zalora.co.th/customer/account/create/	/	128	มี ใน <i>ความเป็นส่วนตัว</i> ด้านล่างของหน้าแรก

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
41. Tohome	https://www.tohome.com/register.aspx	/	128	มี ใน นโยบายบริษัท ด้านล่างของหน้าแรก
42. Central	https://www.central.co.th/account/signup.aspx	/	256	มี ใน หน้าสมัครสมาชิก >>ข้อตกลงการใช้บริการ
43. Officemate	https://www.officemate.co.th/Account/GeneralInformation	/ แต่ใช้ ssl 2 ซึ่งไม่ปลอดภัย	X	มี อยู่ในหน้าสมัครสมาชิก >>ข้อตกลงการใช้บริการ
44. TOPS	http://www.tops.co.th/topsshonline/Member/Register.aspx	X	X	X
45. Tesco Lotus	https://r.tescolotus.com	/	256	มี การป้องกันข้อมูลส่วนบุคคลและความยินยอมในการดำเนินการกับข้อมูล ใน ข้อตกลงและเงื่อนไขการใช้บริการ ด้านล่างของหน้าแรก
46. Big C	http://shoppingonline.bigc.co.th/bigcjumbo/customer/account/create?type=personal	X	X	X มีหัวข้อ นโยบายความเป็นส่วนตัวเป็นส่วนตัว ในหน้าสมัครสมาชิกแต่เปิดไม่ได้

6. บริการจัดหางาน

เว็บไซต์ที่ให้บริการรับสมัครงานเป็นอีกพื้นที่หนึ่งที่ต้องกรอกข้อมูลส่วนตัวของตนเองลงไปเป็นจำนวนมากเพื่อต้องการให้ทำงาน ในส่วนนี้จะเป็นการสำรวจหน้ากรอกข้อมูลสมัครสมาชิกเว็บไซต์ ผลปรากฏว่าไม่มีเว็บใดเลยที่เข้ารหัสในหน้าที่ผู้ใช้ต้องกรอกข้อมูลส่วนตัว แต่น่าสนใจว่าทุกเว็บมีรายละเอียดของนโยบายความเป็นส่วนตัว

ตารางที่ 8 ผลการประเมินเว็บไซต์บริการจัดหางาน

หน่วยงาน	URL	เข้ารหัสด้วย HTTPS	ความยาวกุญแจเข้ารหัส (บิต)	แสดงนโยบายความเป็นส่วนตัวส่วนตัวชัดเจน
47. Jobthai	http://www.jobthai.com/storeresume/resume_register.php	X	X	มี ใน ข้อตกลงและเงื่อนไขการใช้บริการหน้าแรกก่อนเข้าสู่หน้าสมัครสมาชิก
48. Jobtopgun	http://register.superresume.com/SRIX?view=register	X	X	มี นโยบายการเก็บรักษาข้อมูลส่วนบุคคล ในหน้าลงทะเบียน
49. Jobbkk	http://www.jobbkk.com/th/member/member01_resume_step_a.php	X	X	มี ใน นโยบายบริษัท ด้านล่างของหน้าแรก
50. กรมจัดหางาน	http://lmi.doe.go.th/jobs-doe/screen/register/register_employee.php	X	X	มี นโยบายข้อมูลส่วนบุคคล ใน ข้อกำหนดและเงื่อนไขการใช้บริการหน้าลงทะเบียน

สรุป

จากการสำรวจมาตรการรักษาความปลอดภัยและการคุ้มครองความเป็นส่วนตัวส่วนตัวให้บริการออนไลน์ต่างๆ ของประเทศไทยเบื้องต้นเพื่อเป็นข้อมูลแก่ผู้ใช้ทั่วไปในการตัดสินใจใช้บริการสามารถสรุปได้ดังนี้

1. จากเว็บไซต์ทั้งหมด 50 เว็บไซต์ที่มีเว็บไซต์ที่เข้ารหัส HTTPS จำนวน 24 เว็บไซต์
2. เมื่อเปรียบเทียบกับบริการประเภทอื่นๆ แล้ว ธนาคารและสายการบินมีระดับการปกป้องความปลอดภัยและความเป็นส่วนตัวมากที่สุด เห็นได้จากการที่ทุกเว็บมีการเชื่อมต่อแบบ HTTPS มีการเข้ารหัส SSL 3.0 และมีนโยบายความเป็นส่วนตัว ทั้งนี้บริการทางการเงินออนไลน์อยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย ที่อยู่ภายใต้

พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551 ต่างจากบริการที่ไม่มีการทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ซึ่งมีคะแนนต่ำกว่า

อย่างไรก็ตาม มีข้อสังเกตว่า แม้ผลสำรวจเบื้องต้นจะชี้ว่าธนาคารจะมีระบบปกป้องความปลอดภัยดีกว่าบริการออนไลน์ประเภทอื่นๆ แต่ธนาคารบนอินเทอร์เน็ตเป็นหนึ่งในบริการออนไลน์ที่มีผู้ร้องเรียนด้านความปลอดภัยมากที่สุดด้วยเช่นกัน

3. มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีเท่านั้นที่มีระดับการคุ้มครองความปลอดภัยสูงสุด เมื่อเทียบกับมหาวิทยาลัยอื่นๆ เนื่องจากมีการเชื่อมต่อเว็บไซต์แบบ HTTPS มีการเข้ารหัส SSL 3.0 เพียงเว็บเดียวเท่านั้น กระนั้นก็ตามไม่มีนโยบายความเป็นส่วนตัว
4. เว็บซื้อขายสินค้ามีความแตกต่างระหว่างเว็บทำขายสินค้าที่ทำหน้าที่เป็นตัวกลางระหว่างผู้ซื้อกับผู้ขาย กับเว็บค้าปลีกออนไลน์โดยตรงกับผู้บริโภค เว็บทำมีการเข้ารหัสข้อมูลน้อยกว่าเว็บขายปลีก อาจจะมีเหตุผลที่ว่าร้านค้าย่อยส่วนใหญ่เป็นการชำระเงินโดยโอนเงินผ่านธนาคาร ขณะที่ร้านค้าปลีกมีการชำระเงินผ่านบัตรเครดิตโดยตรงซึ่งต้องการความปลอดภัยและความน่าเชื่อถือมากกว่า ในทำนองเดียวกันกับการคมนาคมขนส่ง เว็บจองบัตรโดยสารรถประจำทางมีระดับการปกป้องความปลอดภัยต่ำ เมื่อเทียบกับบริการจำหน่ายบัตรโดยสารเครื่องบิน เหตุผลหลักเป็นเพราะวิธีการชำระเงินแตกต่างกัน เนื่องจากเป็นการรับจองแล้วลูกค้าต้องไปชำระเงินด้วยตนเองช่องทางอื่น มีเพียงเว็บไซต์ไทยทิคเก็ตเมเจอร์เท่านั้นที่รับชำระผ่านบัตรเครดิตด้วย ซึ่งเว็บจะเข้ารหัสเมื่อเชื่อมต่อเข้าสู่หน้ากรอกรายละเอียดบัตรเครดิตเป็นต้นไป
5. เว็บบริการรับสมัครงาน ซึ่งเป็นบริการออนไลน์ที่ผู้ใช้บริการมอบข้อมูลส่วนตัวของตนเองด้วยความสมัครใจ และให้รายละเอียดมากเพื่อทำให้ตนเองได้งาน ไม่มีการเข้ารหัสเว็บไซต์แต่อย่างใด กระนั้นก็ตามสิ่งที่น่าสนใจคือ เว็บไซต์บริการรับสมัครงานทั้งหมด มีนโยบายความเป็นส่วนตัว
6. ด้านความเป็นส่วนตัว จะเห็นได้ว่ามีการให้ความสำคัญต่อเรื่องนี้แตกต่างกัน ทั้งการใช้คำเพื่อสื่อความหมายถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีทั้งคำว่า นโยบายความเป็นส่วนตัว นโยบายการคุ้มครองสิทธิ์ข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคล ฯลฯ รวมถึงตำแหน่งที่อยู่ซึ่งมีทั้งการจัดวางไว้ชัดเจนที่หน้าแรก อยู่ภายใต้หัวข้ออื่นๆ แทรกอยู่ในข้อกำหนดและเงื่อนไขที่มักต้องคลิกเข้าไปอีกครั้ง ในหน้าสมัครสมาชิก