มาตรการคุ้มครองความปลอดภัยและความเป็นส่วนตัวของผู้ให้บริการออนไลน์ไทย

ธันวาคม 2557

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

เครือข่ายพลเมืองเน็ต มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง
https://thainetizen.org/
contact@thainetizen.org

สารบัญ

- บทสรุปสำหรับผู้บริหาร 2
- เกณฑ์ที่ใช้ในการประเมิน 5
- ตารางรวมแสดงผลการศึกษามาตรการคุ้มครองความปลอดภัยและความเป็นส่วนตัว 9
- ข้อสังเกต 14
- บทสรุป 17

บทสรุปสำหรับผู้บริหาร

โครงการวิจัยความเป็นส่วนตัวออนไลน์[1] เครือข่ายพลเมืองเน็ต ได้เริ่มต้นสำรวจมาตรการรักษาความปลอดภัยและการคุ้มครองความเป็นส่วนตัวผู้ให้บริการออนไลน์ต่างๆ ของประเทศไทย ในระดับ ‘เบื้องต้น’ เพื่อเป็นข้อมูลแก่ผู้ใช้ทั่วไปในการตัดสินใจใช้บริการต่างๆ และเพื่อกระตุ้นผู้ให้บริการออนไลน์ให้ตระหนักถึงความสำคัญของการปกป้องความปลอดภัยและความเป็นส่วนตัวของผู้ใช้บริการมากขึ้น

ทุกวันนี้อินเทอร์เน็ตมีบทบาทในชีวิตเรามากขึ้น การรักษาความเป็นส่วนตัวและความปลอดภัยจึงเป็นสิ่งที่ผู้ใช้อินเทอร์เน็ตต้องตระหนักมากขึ้น ข้อมูลต่างๆ ของผู้ใช้อินเทอร์เน็ตกระจัดกระจายไปอยู่ในพื้นที่ต่างๆ มากมายจากการใช้บริการออนไลน์ต่างๆ เมื่อเราเชื่อมต่อคอมพิวเตอร์เข้ากับอินเทอร์เน็ต ผู้ให้บริการอินเทอร์เน็ตมักวิเคราะห์การใช้งานของเรา ซึ่งมักมีวัตถุประสงค์เพื่อปรับปรุงคุณภาพการให้บริการ อย่างไรก็ตาม เนื่องจากผู้ให้บริการอินเทอร์เน็ตเป็นผู้ที่สามารถเห็นข้อมูลทุกอย่างที่เรารับส่งระหว่างการเชื่อมต่ออินเทอร์เน็ต หากผู้ให้บริการไม่รักษาความเป็นส่วนตัวของลูกค้าก็เป็นไปได้ที่จะนำข้อมูลบางส่วนไปใช้โดยที่ลูกค้าไม่รู้ตัว ผู้ใช้จำเป็นต้องรู้เท่าทัน และเข้าใจวิธีการคุ้มครองความเป็นส่วนตัวของตนเอง การทำกิจกรรมต่างๆ บนอินเทอร์เน็ต ไม่ว่าจะเป็นการสนทนา การแสดงความคิดเห็น รูปภาพ ประสบการณ์ ตำแหน่งที่อยู่ ข้อมูลส่วนตัว ฯลฯ สัมพันธ์กับความเชื่อใจที่เรามีต่อบริษัทต่างๆ อย่างกูเกิล หรือเฟซบุ๊ก แต่เราจะแน่ใจได้อย่างไรว่าบริษัทเหล่านี้จะคุ้มครองความปลอดภัยให้กับเราได้ ผู้ให้บริการออนไลน์เหล่านี้มีมาตรการปกป้องความปลอดภัยและความเป็นส่วนตัวของเรามากเพียงใด พวกเขามอบข้อมูลส่วนตัวของเราให้ใครอีกหรือไม่ เราควรแลกข้อมูลส่วนตัวของเรา เช่น เลขประจำตัวประชาชน ข้อมูลการเงิน กับระบบการป้องกันที่ไม่ปลอดภัยหรือไม่ ผู้ให้บริการยอมให้เรารู้ว่าพวกเขาทำอะไรกับข้อมูลของเราหรือไม่

ในการพิจารณาว่าเราควรจะใช้บริการออนไลน์ของบริษัทใดจึงจะปลอดภัย ผู้บริโภคควรจะได้รับข้อมูลว่าบริการเหล่านั้นมีระบบดูแลข้อมูลของตนเองอย่างไร ทั้งการคุ้มครองความปลอดภัยในทางเทคนิค และวิธีจัดการข้อมูล ในงานวิจัยนี้จึงพยายามสำรวจเพื่อเป็นข้อมูลให้ผู้บริโภคสามารถตัดสินใจได้ว่าควรจะใช้บริการใด ด้วยการพิจารณาผู้ให้บริการออนไลน์ไทยจำนวน 45 เว็บไซต์ จำแนกออกเป็นหน่วยงานรัฐ ธนาคาร มหาวิทยาลัย ซื้อขายสินค้า บริการขนส่งสาธารณะ และบริการรับสมัครงาน ระหว่างเดือนตุลาคม – พฤศจิกายน 2557

ในรายงานนี้เป็นการรวบรวมข้อมูลและตรวจสอบการเข้ารหัสการเชื่อมต่อ และนโยบายข้อมูลของบริษัทผู้ให้บริการออนไลน์ไทย และพิจารณาว่าผู้ให้บริการออนไลน์เหล่านี้คุ้มครองความปลอดภัยและความเป็นส่วนตัวของผู้ใช้มากเพียงใด ในทางเทคนิค งานวิจัยนี้วิเคราะห์ว่าเข้ารหัสการเชื่อมต่อหน้าเว็บไซต์เพื่อดูว่ามีการป้องกันไม่ให้มีการดักข้อมูลได้ระหว่างการสื่อสารและมีระบบการยืนยันตัวตนที่ปลอดภัยหรือไม่ ด้วยการตรวจสอบว่าเว็บไซต์ใช้ HTTPS (Hypertext Transfer Protocol Secure) หรือไม่ การใช้โปรโตคอลมาตรฐานความปลอดภัย TLS รหัสผ่าน ใบรับรองความปลอดภัยที่ทันสมัย การเก็บข้อมูลคุกกี้ (cookies) โดยเป็นการประเมินระดับความปลอดภัยของเว็บไซต์ขั้นพื้นฐานที่สุด และผู้ใช้อินเทอร์เน็ตทั่วไปสามารถตรวจสอบได้ด้วยตนเอง จากข้อมูลที่ผู้ใช้ทั่วไปเข้าถึงได้ อย่างไรก็ตาม ผลวิจัยที่ได้ไม่สามารถยืนยันได้ว่าเว็บไซต์เหล่านี้ปลอดภัยอย่างสมบูรณ์ เนื่องจากยังมีปัจจัยอื่นๆ ที่เกี่ยวข้อง และการตรวจสอบระบบความปลอดภัยในขั้นสูงไม่สามารถกระทำได้จากบุคคลภายนอกระบบ

---

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

ส่วนนโยบายจัดการข้อมูล งานวิจัยนี้พิจารณาจากนโยบายความเป็นส่วนตัวที่ผู้ให้บริการแสดงหน้าเว็บไซต์ว่าจะดำเนินการกับข้อมูลส่วนตัวของผู้ใช้บริการอย่างไร แนวทางในการพิจารณามาจากกรอบคิดว่าด้วยการคุ้มครองส่วนบุคคลมาจากองค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: OECD) ซึ่งได้ออกแนวปฏิบัติด้านการคุ้มครองความเป็นส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ หลักการคุ้มครองข้อมูลส่วนบุคคลนี้มี 8 ประการ ได้แก่ หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle) ที่ผู้ให้บริการจะรวบรวมข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมายและความยินยอมจากเจ้าของข้อมูลเท่านั้น หลักคุณภาพของข้อมูล (Data Quality Principle) ที่ต้องเป็นข้อมูลที่ถูกต้องและเป็นปัจจุบัน หลักการระบุวัตถุประสงค์(Purpose Specification Principle) ต้องแจ้งให้เจ้าของข้อมูลทราบวัตถุประสงค์ของการเก็บข้อมูล หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle) จะต้องไม่เปิดเผยข้อมูลนอกเหนือไปจากวัตถุประสงค์ที่แจ้งให้เจ้าของข้อมูลทราบ หลักการรักษาความมั่นคงปลอดภัยของข้อมูล (Security Safeguards Principle) ซึ่งผู้ให้บริการควรรักษาความปลอดภัยของข้อมูลเพื่อป้องกันการลักลอบเข้าถึงข้อมูล หลักการเปิดเผย (Openness Principle) ควรประกาศนโยบายเกี่ยวกับการดำเนินการต่อข้อมูลส่วนบุคคลให้ทราบโดยทั่วไป หลักการมีส่วนร่วมของเจ้าของข้อมูล(Individual Participation Principle) และหลักความรับผิดชอบ (Accountability Principle) ที่ผู้ควบคุมข้อมูลต้องมีหน้าที่ปฏิบัติตามหลักการนี้

- ปลอดภัยจากการถูกดักข้อมูลและถูกแก้ไขข้อมูลระหว่างทางหรือไม่

จากการตรวจสอบตัวชี้วัดระบบการเข้ารหัสของเว็บไซต์ในหน้าลงชื่อเข้าใช้งาน ซึ่งได้แก่ เว็บไซต์มีการเชื่อมต่อด้วย HTTPS หรือไม่ ใช้โปรโตคอลมาตรฐานความปลอดภัย TLS รุ่น 1.2 หรือไม่ และกุญแจเข้ารหัสมีความยาว 256 บิตหรือไม่ มาตรฐานเหล่านี้เป็นความปลอดภัยพื้นฐานที่ผู้ให้บริการควรมี

เว็บไซต์สายการบินแอร์เอเชียและการบินไทยได้คะแนนในส่วนของการเข้ารหัสการเชื่อมต่อหน้าเว็บไซต์มากที่สุด โดยมีการเข้ารหัสหน้าเว็บไซต์ HTTPS การใช้มาตรฐานเข้ารหัสความปลอดภัยรุ่นใหม่ล่าสุด และมีความยาวของกุญแจเข้ารหัส 256 บิต กลุ่มที่ได้คะแนนรองลงมา คือ กลุ่มธนาคาร และซื้อขายสินค้าออนไลน์ ที่ใช้การเข้ารหัส TLS 1.2 โดยเห็นได้ว่าผู้ให้บริการค้าปลีกออนไลน์ที่เป็นบริษัทข้ามชาติ ให้ความสำคัญกับการเข้ารหัสที่ปลอดภัยมากกว่าผู้ให้บริการภายในประเทศ

อย่างไรก็ดี ไม่มีเว็บไซต์ใดที่เข้ารหัสในหน้าเนื้อหาทั่วไปที่ไม่ใช่การลงชื่อเข้าใช้งาน ทั้งนี้การเข้ารหัสการใช้งานหน้าเว็บจะยืนยันได้ว่าเป็นเว็บไซต์ปลายทางที่ผู้ใช้บริการต้องการอย่างแท้จริง

โดยส่วนใหญ่ในการติดต่อสื่อสารบนอินเทอร์เน็ตนั้นจะใช้วิธีการส่งข้อมูลที่เรียกว่า http ซึ่งการส่งข้อมูลแบบนี้ข้อมูลจะไม่ถูกเข้ารหัส ซึ่งหมายความว่า ถ้ามีคนมาดักจับข้อมูลของเรา เขาก็สามารถรู้ได้ว่า เราพูดอะไรบ้าง เช่น รู้รหัสผ่านของเรา รู้รหัสบัตรเครดิตของเรา มีวิธีส่งข้อมูลอีกแบบที่ปลอดภัยกว่า คือ https (s มาจากคำว่า secure) ซึ่งจะเข้ารหัสคำพูดของเรา ทำให้แม้ถูกดักฟัง คนอื่นก็ไม่รู้ว่าเราพูดอะไร

เจ้าของเว็บไซต์หรือผู้ดูแลระบบควรพิจารณาติดตั้ง HTTPS และลงทะเบียนรับใบรับรอง SSL เพื่อเพิ่มความมั่นใจให้กับผู้เข้าชมเว็บ การติดตั้งใบรับรองความปลอดภัยที่ออกโดยผู้ได้รับอนุญาตเป็นการยืนยันตัวตนเจ้าของเว็บไซต์ และยืนยันว่าการเข้ารหัสการเชื่อมต่อของเว็บไซต์สมบูรณ์

ส่วนมาตรฐานความปลอดภัย TLS (Transport Layer Security) รุ่น 1.2 เป็นมาตรฐานเข้ารหัสความปลอดภัยรุ่นล่าสุดที่สามารถป้องกันรูรั่วของระบบเมื่อถูกโจมตีได้ระดับหนึ่ง

- รหัสผ่านแข็งแรงแค่ไหน

ธนาคารกำหนดเงื่อนไขรหัสผ่านเข้มงวดที่สุด

การเข้าใช้บริการเว็บไซต์ที่ต้องระบุชื่อผู้ใช้และรหัสผ่านจำเป็นต้องมีระบบการกำหนดรหัสผ่านที่แข็งแรง เนื่องจากเป็นประตูด่านแรกก่อนเข้าสู่ข้อมูลส่วนตัวเพื่อใช้บริการต่างๆ การตั้งรหัสผ่านเป็นการรักษาความปลอดภัยขั้นพื้นฐาน โดยปกติแล้วนักเจาะระบบคอมพิวเตอร์สามารถเดารหัสผ่านจำนวนมากได้ในระยะเวลาอันสั้น การตั้งรหัสผ่านให้มีความทนทานต่อการคาดเดาจึงเป็นเรื่องสำคัญ การกำหนดเงื่อนไขของรหัสผ่านจากผู้ให้บริการมีความสำคัญต่อความทนทานนี้ นอกจากนี้สิ่งที่ควรพิจารณาคือระบบการจัดเก็บรหัสผ่านว่ามีการเข้ารหัสหรือไม่ เพื่อป้องกันกรณีรหัสผ่านรั่วไหลจากเซิร์ฟเวอร์ที่เก็บรหัสผ่าน

ขั้นตอนการตรวจสอบความแข็งแรงของรหัสผ่านวัดจากการกำหนดเงื่อนไขของการรหัสผ่านทั้งความยาวและอักขระและการเก็บรหัสผ่าน จากผลการศึกษาพบว่า เว็บไซต์ที่กำหนดความยาวรหัสผ่านยาวที่สุด คือ กลุ่มธนาคารที่กำหนดความยาวขั้นต่ำ 8 ตัวอักษร ขณะที่เว็บซื้อขายสินค้าออนไลน์ที่เป็นบริษัทข้ามชาติกำหนดรหัสผ่านขั้นต่ำ 6 ตัวอักษร สำหรับหน่วยงานรัฐได้แก่ กรมสรรพากร และกรมขนส่งทางบกได้กำหนดความยาวของรหัสผ่าน 8 และ 6 ตัวอักษรขึ้นไปตามลำดับ อย่างไรก็ตามทั้งสองหน่วยงานใช้เลขประจำตัวประชาชนเป็นชื่อผู้ใช้ และไม่ได้บังคับการใช้อักขระ บางเว็บไซต์กำหนดความยาวรหัสผ่านขั้นต่ำเพียง 4 ตัวอักษรเท่านั้นได้แก่ สำนักงานประกันสังคม เว็บค้าปลีกไทย

เมื่อพิจารณาการเก็บรหัสผ่านจากขั้นตอนการขอรหัสผ่านใหม่ มีทั้งการให้ตอบคำถามที่ผู้ใช้เคยตั้งไว้ หากตอบถูกระบบจะมอบรหัสผ่านให้ทางหน้าเว็บซึ่งผู้ใช้จะเปลี่ยนหรือไม่ก็ได้ เว็บกรมสรรพากรและกรมขนส่งทางบกใช้วิธีนี้ ขณะที่สำนักงานประกันสังคมให้ผู้ใช้กรอกเลขประจำตัวประชาชนและอีเมล จากนั้นส่งรหัสผ่านใหม่ทางอีเมล ส่วนเว็บไซต์ธนาคารมีระบบการรับรหัสผ่านใหม่ด้วยการติดต่อเจ้าหน้าที่ธนาคารซึ่งจะสอบถามข้อมูลส่วนตัวเบื้องต้น เช่น เลขประจำตัวประชาชน วันเกิด เป็นต้น หรือการเปลี่ยนรหัสผ่านจากตู้เอทีเอ็ม และอีกวิธีหนึ่งคือ การส่งลิงก์มาทางอีเมลเพื่อเข้าสู่การตั้งรหัสผ่าน เว็บไซต์ที่ใช้วิธีการนี้คือเว็บซื้อขายสินค้าออนไลน์ นอกจากนี้ยังพบว่ามีเว็บไซต์ที่ส่งรหัสผ่านแบบไม่เข้ารหัสมาทางอีเมล คือ เว็บไซต์ของมหาวิทยาลัยมหิดล

- รับมือกับช่องโหว่ความปลอดภัยใหม่ๆ ได้มากเพียงใด

ใบรับรองความปลอดภัยเว็บไทยส่วนใหญ่ตกรุ่น

เนื่องจากการโจมตีความปลอดภัยบนเครือข่ายอินเทอร์เน็ตมีโอกาสจะเกิดขึ้นได้ตลอดเวลา ผู้ให้บริการจึงต้องเตรียมพร้อมเพื่อรับมือกับการคุกคามที่นับวันจะมีมากขึ้นเรื่อยๆ ได้ ในการพิจารณาว่าการเข้ารหัสของเว็บไซต์สามารถรับมือกับการถูกโจมตีที่เกิดขึ้นล่าสุดได้ทันท่วงทีหรือไม่ การศึกษานี้จะพิจารณาว่าเว็บไซต์สามารถป้องกันการโจมตีซึ่งมาจากช่องโหว่ที่ชื่อว่า POODLE หรือไม่ รวมทั้งตรวจสอบว่าใช้ใบรับรองดิจิทัล SHA-2 ซึ่งใบรับรองที่เว็บไซต์ในปัจจุบันควรจะมีหรือไม่

จากการตรวจสอบด้วยเว็บไซต์ Qualy SSL labs ซึ่งใช้ประเมินความปลอดภัยของการเข้ารหัสของเว็บไซต์ต่างๆ พบว่าเว็บไซต์ธนาคารมีเพียงธนาคารทหารไทยและธนาคารธนชาตเท่านั้นที่สามารถแก้ปัญหาช่องโหว่ POODLE ได้ ขณะที่เว็บไซต์ธนาคารเกือบทั้งหมดยังคงเปิดใช้งาน SSL 3.0 ซึ่งถือเป็นจุดอ่อนของระบบอยู่ ส่วนผู้ให้บริการอื่นๆ มีเพียงเว็บไซต์สายการบินแอร์เอเชีย การบินไทย Lazada และ Jobbkk เท่านั้นที่รับมือกับปัญหานี้ได้

ส่วนใบรับรองดิจิทัล SHA-2 มีเพียงธนาคารกสิกรไทยเท่านั้นจากธนาคารทั้งหมดที่มีใบรับรองนี้ ส่วนเว็บไซต์มหาวิทยาลัยที่มีใบรับรองนี้มี 2 มหาวิทยาลัยซึ่งเป็นมหาวิทยาลัยเพียง 2 แห่งที่มีการเชื่อมต่อแบบเข้ารหัส

- มีกระบวนการเก็บรวบรวม ประมวล แลกเปลี่ยนและเข้าถึงข้อมูลอย่างไร

แอร์เอเชียครองแชมป์นโยบายข้อมูลยอดเยี่ยม

วัตถุประสงค์ของการพิจารณานโยบายด้านข้อมูลของเว็บไซต์ต่างๆ คือ เพื่อประเมินว่าผู้ให้บริการดูแลข้อมูลส่วนตัวของผู้ใช้บริการอย่างไร ในเบื้องต้นพิจารณาว่าผู้ให้บริการแจ้งให้ผู้ใช้ทราบถึงแนวทางการบริหารจัดการข้อมูลที่ได้รับหรือไม่ และ

เว็บไซต์ธนาคารและเว็บซื้อขายสินค้าออนไลน์แสดงนโยบายความเป็นส่วนตัวชัดเจน ขณะที่เว็บไซต์มหาวิทยาลัยทั้งหมดไม่แจ้งข้อกำหนดและเงื่อนไขในการเก็บข้อมูลส่วนตัว ทั้งๆ ที่เป็นพื้นที่ซึ่งเก็บข้อมูลส่วนบุคคลไว้มากที่สุดแห่งหนึ่ง

เว็บไซต์ที่แจ้งวัตถุประสงค์ของการเก็บข้อมูลได้ละเอียดชัดเจน มีเพียง เว็บไซต์สายการบินแอร์เอเชียเพียงเว็บไซต์เดียว โดยมีการระบุว่านำข้อมูลต่างๆ ที่ได้จากลูกค้าไปใช้ด้วยเหตุผลที่มีลักษณะเฉพาะเจาะจง ซึ่งต่างจากหลายเว็บไซต์ที่กล่าวอย่างกว้างๆ เท่านั้นเช่น เว็บไซต์ธนาคารไทยพาณิชย์แจ้งว่า “เก็บข้อมูลเพื่อเหตุผลทางธุรกิจบางประการเท่านั้น”

มี 2 เว็บไซต์จาก 45 เว็บไซต์ที่แจ้งให้ผู้ใช้ทราบอย่างละเอียดว่าเก็บข้อมูลอะไรบ้างอย่างเฉพาะเจาะจง คือ สายการบินแอร์เอเชีย และเว็บไซต์ Lazada

สำหรับการส่งต่อข้อมูลให้กับบุคคลที่สาม มีเพียงสายการบินแอร์เอเชียเท่านั้นที่อธิบายอย่างละเอียดว่า ข้อมูลประเภทใดจะถูกส่งต่อเพื่อวัตถุประสงค์ใด ส่วนใหญ่บริการเกือบทั้งหมดอธิบายกว้างๆ ว่าจะถูกใช้เพื่อประโยชน์หรืออำนวยความสะดวกแก่ลูกค้าให้ได้รับบริการที่ดีขึ้นเท่านั้น

นอกจากนี้เป็นที่น่าสังเกตว่า ผู้ให้บริการหลายรายระบุว่า ข้อมูลที่กรอกไว้ในเว็บไซต์เป็นกรรมสิทธิ์ของบริษัท

เกณฑ์ที่ใช้ในการประเมิน

ในการศึกษาครั้งนี้ได้มีการเพิ่มตัวชี้วัดขึ้นจากรายงานการศึกษาครั้งที่ 1 ที่เผยแพร่เมื่อเดือนสิงหาคม 2557 เพื่อให้ครอบคลุมหลายประเด็นมากขึ้น โดยจำแนกออกเป็น 3 ด้าน ดังนี้

1) การประเมินมาตรการทางเทคนิค

1.1 มีการเข้ารหัสการเชื่อมต่อเว็บไซต์ในขั้นตอนลงชื่อเข้าใช้งานหรือไม่

ในการประเมินนี้จะประเมินการเข้ารหัสการเชื่อมต่อหน้าเว็บไซต์ 3 รูปแบบ ได้แก่ การสื่อสารแบบเข้ารหัสระหว่างผู้ใช้กับเซิร์ฟเวอร์เพื่อไม่ให้ถูกดักข้อมูลได้ด้วย HTTPS (Hypertext Transfer Protocol Secure) การใช้โปรโตคอลความปลอดภัย TLS (Transport Layer Security) ซึ่งเป็นมาตรฐานที่ใช้กันในอุตสาหกรรม ซึ่งพัฒนามาจาก Secure Sockets Layer (SSL) ที่จะเข้ารหัสให้การเชื่อมต่อปลอดภัย และยืนยันตัวตนด้วยการตรวจสอบว่าเซิร์ฟเวอร์ที่เราส่งข้อมูลไปนั้นมีอยู่จริง ในการสำรวจครั้งนี้จะประเมินว่าผู้ให้บริการมีการเข้ารหัส TLS 1.2 หรือไม่ ซึ่งเป็นมาตรฐาน

ความปลอดภัยรุ่นใหม่ล่าสุด และความยาวของกุญแจเข้ารหัส กุญแจการเข้ารหัสแบบ 128 บิต และ 256 บิต แตกต่างกัน ความยาวของกุญแจเข้ารหัสมีหน่วยเป็นบิต ยิ่งกุญแจมีความยาวมาก โอกาสที่ผู้บุกรุกจะคาดเดากุญแจที่ถูกต้องก็ยิ่งยากขึ้นตามไปด้วย ดังนั้นในการสำรวจครั้งนี้จึงถือว่าการเข้ารหัส 256 บิต มีความปลอดภัยมากกว่าการเข้ารหัสแบบ 128 บิต

การตรวจสอบว่าเป็นการเข้ารหัสรุ่นใดทดสอบผ่านเว็บไซต์ SSL Server Test (https://www.ssllabs.com/ssltest) ซึ่งเป็นบริการวิเคราะห์โครงสร้างของเว็บที่เข้ารหัส SSL ทุกประเภทบนอินเทอร์เน็ต และเป็นโครงการวิจัยที่ไม่แสวงหาผลประโยชน์ทางการค้า

1.2 มีการเข้ารหัสการเชื่อมต่อในหน้าเนื้อหาทั่วไปของเว็บไซต์หรือไม่ เพื่อยืนยันว่าเป็นเว็บไซต์ที่ต้องการเข้าชมจริง

1.3 ความแข็งแรงของรหัสผ่านเป็นอย่างไร

ความแข็งแรงของรหัสผ่านมีความสำคัญอย่างยิ่งต่อการปกป้องข้อมูลต่างๆ ของผู้ใช้บริการให้ปลอดภัย การกำหนดเงื่อนไขของรหัสผ่าน ทั้งความยาวและรูปแบบตัวอักษร นอกจากความยาวของรหัสผ่านแล้ว ในงานวิจัยนี้ยังตรวจสอบเงื่อนไขของการตั้งรหัสผ่านว่ามีความสลับซับซ้อนมากเพียงใด ทั้งการบังคับให้ใช้พยัญชนะตัวพิมพ์ใหญ่ ตัวเลข เป็นส่วนประกอบของรหัสผ่านด้วย

1.4 การเก็บรักษารหัสผ่านของเว็บไซต์เป็นอย่างไร

พิจารณาว่าผู้ให้บริการเก็บรหัสผ่านของผู้ใช้ในรูปแบบใด ซึ่งผู้ให้บริการไม่ควรรู้รหัสผ่าน และไม่ควรถูกเก็บอยู่ในตัวอักษรธรรมดาโดยไม่เข้ารหัสข้อความ

1.5 การเก็บข้อมูลคุกกี้

เว็บไซต์โดยทั่วไปมักมีการเก็บข้อมูลคุกกี้ (cookies) ซึ่งเป็นไฟล์ที่เว็บไซต์ต่างๆ ที่คุณเคยเข้าชมสร้างขึ้นเพื่อใช้ในการจัดเก็บข้อมูลการเรียกดู เช่น เก็บข้อมูลว่ามีการใช้งานเว็บไซต์นั้นๆ อย่างไร หน้าใดที่เข้าชมมากที่สุด เข้าชมจากเบราวน์เซอร์ใด เป็นต้น คุกกี้มีสองประเภท ได้แก่ คุกกี้ของบุคคลที่หนึ่ง ซึ่งเป็นคุกกี้ที่กำหนดโดยโดเมนของเว็บไซต์ที่ปรากฏในแถบที่อยู่ คุกกี้ของบุคคลที่สาม มาจากแหล่งโดเมนอื่นๆ ที่มีรายการต่างๆ ฝังอยู่ในหน้าเว็บนั้นๆ เช่น โฆษณา หรือรูปภาพ

ในงานวิจัยนี้สำรวจจากนโยบาย หรือข้อกำหนดและเงื่อนไขที่ผู้ให้บริการแจ้งบนเว็บไซต์ว่ามีวิธีการเก็บอย่างไร โดยพิจารณาว่ามีการอธิบายการเก็บคุกกี้ต่อผู้ใช้บริการหรือไม่ พร้อมกับพิจารณาว่ามีการให้รายละเอียดของการเก็บคุกกี้มากเพียงใด

1.6 ปฏิบัติตามคำขอ “ไม่ติดตาม” ได้หรือไม่

แม้ว่าเว็บไซต์ต่างๆ จะเก็บข้อมูลการเข้าชมเว็บโดยที่ผู้ใช้บริการอาจไม่รู้ตัว แต่ผู้ใช้บริการมีทางเลือกที่จะไม่ให้ข้อมูล และทิ้งร่องรอยการเข้าชมเว็บของตนเองได้ ด้วยวิธีการต่างๆ ที่เรียกว่า “ไม่ติดตาม (Do not track)” เพื่อไม่ให้เว็บไซต์เก็บข้อมูลได้ ในงานวิจัยนี้ได้ใช้ส่วนขยายในเบราวน์เซอร์ที่ชื่อว่า Privacy Badger ที่ออกแบบโดยมูลนิธิพรมแดนอิเล็กทรอนิกส์ (Electronic Frontier Foundation) เพื่อทดสอบว่าเว็บไซต์ใดยอมให้ใช้ฟังก์ชันไม่ติดตาม หรือเก็บข้อมูลคุกกี้แล้วผู้ใช้ยังสามารถใช้บริการเว็บไซต์ได้หรือไม่

1.7 มีระบบป้องกันการคุกคามความปลอดภัยทันสมัยหรือไม่

พิจารณาว่าการเข้ารหัสสามารถรับมือกับการถูกโจมตีที่เกิดขึ้นล่าสุดได้ทันท่วงทีหรือไม่ ในงานวิจัยนี้วิเคราะห์ว่าเว็บไซต์ผู้ให้บริการได้แก้ไขปัญหาช่องโหว่ที่ชื่อว่า POODLE ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถถอดรหัสลับข้อมูลที่รับส่งเพื่ออ่านเนื้อหาของข้อมูลได้ โดยใช้เครื่องมือตรวจสอบของเว็บไซต์ QUALYS SSL LABS

นอกจากนี้จะพิจารณาว่าเว็บไซต์ใช้ใบรับรองดิจิทัลที่ตรวจสอบความถูกต้องด้วย SHA-1 หรือไม่ เนื่องจากเป็นใบรับรอง ซึ่งถูกออกแบบมาตั้งแต่ปี 1995 และพบว่ามีจุดอ่อนหลายอย่างจึงถือว่าเป็นใบรับรองที่ไม่ปลอดภัยอีกต่อไป ใบรับรองที่ปลอดภัยกว่าคือ SHA-2 ปัจจุบันบริษัทใหญ่ด้านไอที เช่น ไมโครซอฟต์และกูเกิลอยู่ในกระบวนการเลิกรับ SHA-1

2) นโยบายข้อมูลและการคุ้มครองทางกฎหมาย

2.1 มีมาตรการบังคับใช้ชื่อจริงหรือไม่

มาตรการบังคับใช้ชื่อจริงสมัครเข้าใช้บริการต่างๆ นั้นเกี่ยวข้องกับการระบุตัวตนที่แท้จริงของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการตรวจสอบได้ว่าผู้ใช้มีตัวตนจริง ในทางเดียวกันก็สามารถติดตามตัวได้หากต้องการ ในงานวิจัยนี้จะสำรวจว่าเว็บไซต์ใดต้องการข้อมูลเพื่อระบุตัวตนของผู้ใช้บริการด้วยเลขประจำตัวประชาชน 13 หลัก และต้องการข้อมูลส่วนตัวที่สามารถระบุตัวตนอื่นๆ หรือไม่ อย่างไร

2.2 มีนโยบายข้อมูลอย่างไร

ผู้ให้บริการควรแจ้งให้ผู้ใช้บริการทราบถึงกระบวนการเก็บรวบรวม ประมวล การเข้าถึง ข้อมูลต่างๆ ขอบเขต และวัตถุประสงค์ของการเก็บข้อมูลให้ชัดเจน ตามหลักเกณฑ์การคุ้มครองความเป็นส่วนตัวและความปลอดภัยสากล

เว็บไซต์ควรแจ้งต่อผู้ใช้บริการว่ามีการเก็บข้อมูลอะไรบ้างเพื่อเข้าใช้บริการ ผ่านทางนโยบายความเป็นส่วนตัว หรือนโยบายความปลอดภัย หรือข้อกำหนดและเงื่อนไขในการใช้บริการเว็บไซต์

เว็บไซต์ควรแจ้งต่อผู้ใช้บริการทราบถึงวัตถุประสงค์ของการเก็บข้อมูลส่วนตัว ผ่านทางนโยบายความเป็นส่วนตัว หรือนโยบายความปลอดภัย หรือข้อกำหนดและเงื่อนไขในการใช้บริการเว็บไซต์

2.3 มีคำอธิบายเกี่ยวกับการส่งต่อข้อมูลให้กับบุคคลที่ 3 หรือไม่

เนื่องจากปัจจุบันผู้ให้บริการออนไลน์มีแนวโน้มที่จะส่งต่อข้อมูลของผู้ใช้บริการเว็บไซต์ให้กับบุคคลที่ 3 โดยมีวัตถุประสงค์ต่างๆ เช่น เพื่อการโฆษณา เพื่อเพิ่มประสิทธิภาพในการให้บริการแก่ลูกค้าให้ดียิ่งขึ้น ผู้ให้บริการจำเป็นต้องแจ้งให้ผู้ใช้บริการทราบว่าข้อมูลของตนเองถูกส่งต่อไปให้กับใคร วัตถุประสงค์อย่างไร ระยะเวลาเท่าใด ในการพิจารณาว่าผู้ให้บริการออนไลน์มีแนวปฏิบัติอย่างไรในการส่งต่อข้อมูลให้กับบุคคลที่ 3 โดยดูจากการให้รายละเอียดต่อผู้ใช้บริการ

2.4 นโยบายการส่งต่อข้อมูลให้กับเจ้าหน้าที่

เนื่องจากข้อมูลส่วนบุคคลในเว็บไซต์สามารถนำไปใช้เพื่อดำเนินการทางกฎหมายได้ โดยเจ้าหน้าที่ต้องได้รับอนุญาตจากศาลก่อน ในประเด็นนี้จึงจะพิจารณาว่าผู้ให้บริการแจ้งต่อผู้ใช้บริการหรือไม่ว่าจะดำเนินการอย่างไร หากได้รับการร้องขอทางกฎหมายจากเจ้าหน้าที่ของรัฐ ให้ส่งต่อข้อมูลของผู้ใช้บริการ

3) บรรทัดฐานทางสังคมในด้านความปลอดภัยและความเป็นส่วนตัวออนไลน์

3.1 มีรายงานความโปร่งใสหรือไม่

รายงานความโปร่งใสเป็นรายงานที่บริษัทเอกชนจะเปิดเผยข้อมูลและสถิติที่มาจากการร้องขอดูข้อมูลส่วนตัว การควบคุมเนื้อหา ส่วนใหญ่แล้วรายงานมักเปิดเผยความถี่ของรัฐบาลแต่ละประเทศที่ร้องขอให้ผู้ให้บริการออนไลน์เปิดเผยข้อมูลในช่วงระยะเวลาหนึ่ง รายงานนี้จะทำให้สาธารณะเห็นว่าข้อมูลส่วนบุคคลลักษณะใดบ้างที่รัฐบาลร้องขอ รวมทั้งเข้าถึงได้เมื่อได้รับใบอนุญาตจากศาล หรือคำสั่งให้เอาเนื้อหาออกจากเว็บ เป็นต้น กูเกิลเปิดเผยรายงานความโปร่งใสครั้งแรกเมื่อพ.ศ. 2553 หลังจากนั้นทวิตเตอร์ก็เผยแพร่รายงานนี้ใน 2 ปีถัดมา ปัจจุบันมีบริษัทด้านเทคโนโลยีและคมนาคมเผยแพร่รายงานความโปร่งใสนี้มากขึ้นเรื่อยๆ ไม่ว่าจะเป็นกูเกิล ไมโครซอฟต์ เอทีแอนด์ที แอปเปิล เป็นต้น

ข้อดีของรายงานความโปร่งใสคือ ผู้ใช้บริการและสาธารณะจะได้รับทราบว่ามีความพยายามเข้าถึงข้อมูลของตนเองจากรัฐบาลหรือไม่ และอย่างไร ปัจจุบันในประเทศไทยยังไม่มีบริษัทใดที่จัดทำรายงานความโปร่งใส

3.2 ผู้ให้บริการแจ้งให้ผู้ใช้บริการทราบถึงนโยบายด้านข้อมูล ในกรณีที่บริษัทหรือบริการถูกซื้อขาย หรือเปลี่ยนเจ้าของหรือไม่

เนื่องจากการที่ผู้ใช้บริการมอบข้อมูลให้เว็บไซต์เป็นการมอบให้กับผู้ให้บริการเหล่านั้นโดยตรง ภายใต้เงื่อนไขและข้อกำหนดของเว็บไซต์ โดยไม่สามารถคาดการณ์ได้ว่าบริษัทจะถูกซื้อขายหรือเปลี่ยนมือหรือไม่ การแจ้งให้ผู้ใช้บริการได้ทราบว่าบริษัทมีนโยบายข้อมูลอย่างไรเป็นแนวทางที่ควรปฏิบัติ

3.4 มีการจัดทำให้นโยบายความเป็นส่วนตัวเข้าใจง่ายหรือไม่ เช่น ภาษา รูปแบบการจัดหน้า

ในส่วนนี้จะพิจารณาว่าผู้ให้บริการได้จัดทำนโยบายความเป็นส่วนตัว ข้อกำหนดและเงื่อนไขในการให้บริการของเว็บไซต์ให้ผู้ใช้โดยทั่วไปเข้าใจได้ง่ายหรือไม่ ซึ่งสะท้อนผ่านการใช้ภาษา การจัดวางเนื้อหา

THAI NETIZEN NETWORK

ตารางรวมแสดงผลการศึกษามาตรการคุ้มครองความปลอดภัยและความเป็นส่วนตัว

ผู้ให้บริการออนไลน์	HTTPS	รุ่น TLS	การรับมือกับ POODLE	ใบรับรอง SHA-2	ความยาวกุญแจ	ความยาวรหัสผ่าน	เงื่อนไขรหัสผ่าน	การเก็บรหัสผ่าน	แจ้งว่าเก็บข้อมูลคุกกี้	ยอมให้ใช้ Do Not Track	บังคับใช้เลขประจำตัวประชาชน	แจ้งว่าเก็บข้อมูลอะไร	แจ้งวัตถุประสงค์การเก็บข้อมูล	แจ้งการส่งต่อข้อมูลให้บุคคลที่สาม	แจ้งการส่งต่อข้อมูลให้เจ้าหน้าที่	นโยบายเมื่อบริษัทเปลี่ยนเจ้าของ	นโยบายเข้าใจง่าย	รวม
กรมสรรพากร	★	½	☆	½	½	★	☆	½	☆	★	ใช้	☆	☆	☆	☆	☆	☆	5
กรมขนส่งทางบก	★	½	½	½	½	★	☆	½	☆	★	ใช้	☆	☆	☆	☆	☆	☆	5.5
สำนักงานประกันสังคม	☆	☆	☆	½	☆	½	½	☆	☆	★	ใช้	☆	☆	☆	☆	☆	★	3.5
กองทุนเงินให้กู้ยืมเพื่อการศึกษา	★	½	½	½	½	☆	☆	½	☆	★	ใช้	☆	☆	☆	☆	☆	½	4.5
ระบบคุ้มครองผู้บริโภคแบบเบ็ดเสร็จ	☆	☆	☆	☆	☆	☆	★	-	☆	★	ไม่	☆	☆	☆	☆	☆	☆	2
ธนาคารกรุงไทย	★	★	½	½	½	★	★	★	½	★	ใช้	½	½	½	½	☆	★	11
ธนาคารกสิกรไทย	★	½	½	★	½	★	½	★	½	★	ใช้	½	½	½	½	☆	★	10.5
ธนาคารไทยพาณิชย์	★	★	½	½	½	★	★	★	½	★	ใช้	½	½	½	½	☆	★	11
ธนาคารกรุงเทพ	★	★	½	½	½	★	★	★	½	★	ใช้	½	½	½	½	☆	½	11.5
ธนาคารทหารไทย	★	★	★	½	½	★	★	★	½	★	ใช้	☆	☆	½	½	☆	½	10
ธนาคารออมสิน	★	½	½	½	★	★	★	★	☆	★	ใช้	☆	☆	½	½	☆	½	9
ธนาคารกรุงศรีอยุธยา	★	½	½	½	½	★	½	★	☆	★	ใช้	☆	½	½	☆	☆	★	8.5
ธนาคารธนชาต	★	½	★	½	½	★	½	★	☆	★	ใช้	½	½	½	☆	☆	★	9.5
การบินไทย	★	★	★	½	★	-	-		½	★	ใช้	½	½	½	½	☆	★	9

ผู้ให้บริการออนไลน์	HTTPS	รุ่น TLS	การรับมือกับ POODLE	ใบรับรอง SHA-2	ความยาวกุญแจ	ความยาวรหัสผ่าน	เงื่อนไขรหัสผ่าน	การเก็บรหัสผ่าน	แจ้งว่าเก็บข้อมูลคุกกี้	ยอมให้ใช้ Do Not Track	บังคับใช้เลขประจำตัวประชาชน	แจ้งว่าเก็บข้อมูลอะไร	แจ้งวัตถุประสงค์การเก็บข้อมูล	แจ้งการส่งต่อข้อมูลให้บุคคลที่สาม	แจ้งการส่งต่อข้อมูลให้เจ้าหน้าที่	นโยบายเมื่อบริษัทเปลี่ยนเจ้าของ	นโยบายเข้าใจง่าย	รวม
บางกอกแอร์เวย์	★	★	⯪	⯪	⯪	-	-		⯪	★	ใช้	⯪	⯪	⯪	⯪	☆	☆ อังกฤษ	7
แอร์เอเชีย	★	★	★	⯪	★	★	★	★	★	★	ใช้	★	★	★	⯪	★	★	15
นกแอร์	★	⯪	⯪	⯪	⯪	-	-	-	⯪	★	ใช้	⯪	⯪	⯪	⯪	☆	☆ อังกฤษ	6.6
Thairoute	☆	☆	☆	☆	☆	☆	☆	★	☆	★	ไม่	☆	☆	☆	☆	☆	☆	2
Bus Ticket	☆	☆	☆	☆	☆	☆	☆	★	☆	★	ไม่	☆	☆	☆	☆	☆	☆	2
จุฬาลงกรณ์	★	⯪	☆	⯪	⯪	☆	☆	⯪	☆	★	ใช้	☆	☆	☆	☆	☆	☆	4
ธรรมศาสตร์	★	⯪	⯪	⯪	⯪	☆	⯪	⯪	☆	★	ใช้	☆	☆	☆	☆	☆	☆	5
มหิดล	☆	☆	☆	☆	☆	⯪	☆	☆	☆	★	ใช้	☆	☆	☆	☆	☆	☆	1.5
อัสสัมชัญ	☆	☆	☆	☆	☆	★	⯪	★	☆	★	ใช้	☆	☆	☆	☆	☆	☆	3.5
หอการค้าไทย	☆	☆	☆	☆	☆	☆	⯪	⯪	☆	★	ใช้	☆	☆	☆	☆	☆	☆	2
เกษตรศาสตร์	★	⯪	⯪	⯪	⯪	☆	☆	★	☆	★	ใช้	☆	☆	☆	☆	☆	☆	5
พระจอมเกล้าธนบุรี	★	★	☆	★	⯪	★	⯪	⯪	☆	★	ใช้	☆	☆	☆	☆	☆	☆	6.5
วลัยลักษณ์	☆	☆	☆	☆	☆	☆	☆	⯪	☆	★	ใช้	☆	☆	☆	☆	☆	☆	1.5
สงขลานครินทร์	★	⯪	⯪	★	⯪	★	★	★	☆	★	ใช้	☆	☆	☆	☆	☆	☆	7.5

ผู้ให้บริการออนไลน์	HTTPS	รุ่น TLS	การรับมือกับ POODLE	ใบรับรอง SHA-2	ความยาวกุญแจ	ความยาวรหัสผ่าน	เงื่อนไขรหัสผ่าน	การเก็บรหัสผ่าน	แจ้งว่าเก็บข้อมูลคุกกี้	ยอมให้ใช้ Do Not Track	บังคับใช้เลขประจำตัวประชาชน	แจ้งว่าเก็บข้อมูลอะไร	แจ้งวัตถุประสงค์การเก็บข้อมูล	แจ้งการส่งต่อข้อมูลให้บุคคลที่สาม	แจ้งการส่งต่อข้อมูลให้เจ้าหน้าที่	นโยบายเมื่อบริษัทเปลี่ยนเจ้าของ	นโยบายเข้าใจง่าย	รวม
Weloveshopping	★	★	☆	◪	◪	★	☆	★	☆	★	ที่อยู่	☆	☆	☆	☆	☆	★	7
Tarad.com	★	◪	☆	◪	◪	★	☆	★	☆	★	ที่อยู่	☆	☆	☆	◪	☆	★	7
Pramool.com	☆	☆	☆	☆	☆	◪	☆	★	☆	★	ที่อยู่	☆	☆	☆	☆	☆	☆	2.5
OLX	☆	☆	☆	★	☆	★	◪	★	☆	★	ที่อยู่	☆	☆	☆	◪	☆	★	6
Lazada	★	★	★	★	◪	★	★	★	★	★	ที่อยู่	★	◪	◪	◪	☆	★	13
Zalora	★	★	◪	◪	◪	◪	☆	★	★	★	ที่อยู่	★	◪	◪	◪	☆	★	10.5
Digital2home	☆	☆	☆	☆	☆	☆	☆	-	☆	★	ไม่	☆	☆	☆	☆	☆	☆	1
Tohome	★	★	☆	★	◪	-	☆	☆	◪	★	ไม่	◪	◪	◪	★	☆	★	8.5
Central	★	★	☆	★	◪	☆	☆	★	☆	★	ที่อยู่	☆	☆	☆	☆	☆	☆	5.5
Officemate	★	◪	◪	◪	◪	☆	☆	★	☆	★	ที่อยู่	☆	◪	◪	☆	☆	★	7
TOPS	☆	☆	☆	☆	☆	◪	◪	☆	☆	★	ที่อยู่	☆	☆	☆	☆	☆	☆	2
Tesco Lotus	★	◪	☆	◪	◪	★	◪	ระบบขัดข้อง	☆	★	ที่อยู่	☆	☆	☆	☆	☆	★	6
Big C	☆	☆	☆	☆	☆	★	◪	★	☆	★	ที่อยู่	☆	☆	☆	☆	☆	☆	3.5
Jobthai	☆	☆	☆	☆	☆	★	◪	☆	☆	★	ที่อยู่	◪	☆	☆	☆	☆	☆	3
Jobtopgun	☆	☆	☆	☆	☆	★	☆	★	★	★	ที่อยู่	◪	◪	☆	★	☆	★	7

ผู้ให้บริการออนไลน์	HTTPS	รุ่น TLS	การรับมือกับ POODLE	ใบรับรอง SHA-2	ความยาวกุญแจ	ความยาวรหัสผ่าน	เงื่อนไขรหัสผ่าน	การเก็บรหัสผ่าน	แจ้งว่าเก็บข้อมูลคุกกี้	ยอมให้ใช้ Do Not Track	บังคับใช้เลขประจำตัวประชาชน	แจ้งว่าเก็บข้อมูลอะไร	แจ้งวัตถุประสงค์การเก็บข้อมูล	แจ้งการส่งต่อข้อมูลให้บุคคลที่สาม	แจ้งการส่งต่อข้อมูลให้เจ้าหน้าที่	นโยบายเมื่อบริษัทเปลี่ยนเจ้าของ	นโยบายเข้าใจง่าย	รวม
Jobbkk	★	★	★	½	½	★	☆	★	☆	★	ที่อยู่	½	½	☆	☆	☆	☆	8
กรมจัดหางาน	☆	☆	☆	☆	☆	☆	☆	-	½	★	ใช้	☆	☆	☆	½	☆	½	2.5

หมายเหตุ

- คำอธิบายสัญลักษณ์

★ หมายถึง 1 คะแนน ½ หมายถึง 0.5 คะแนน ☆ หมายถึง 0 คะแนน

- คำอธิบายตัวชี้วัด

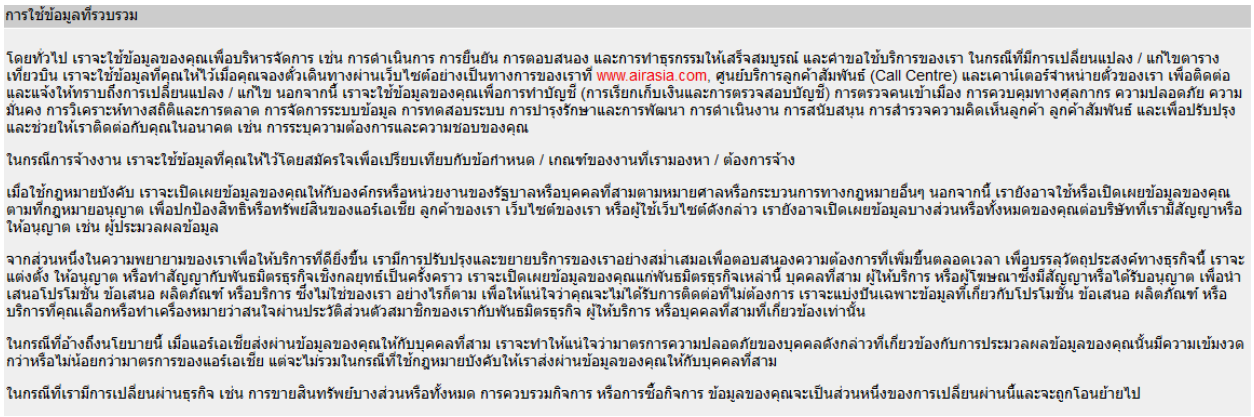
1) การเข้ารหัส HTTPS: เว็บไซต์ที่มีการเข้ารหัส HTTPS ในขั้นตอนลงชื่อเข้าใช้และใส่รหัสผ่านได้ 1 คะแนน เว็บไซต์ที่ไม่เข้ารหัส HTTPS ในขั้นตอนลงชื่อเข้าใช้และใส่รหัสผ่านได้ 0 คะแนน
2) รุ่น TLS: เว็บไซต์ที่ใช้การเข้ารหัส TLS 1.2 ได้ 1 คะแนน เว็บไซต์ที่ใช้การเข้ารหัส TLS 1.0 ได้ 0.5 คะแนน เว็บไซต์ที่ไม่เข้ารหัส TLS ได้ 0 คะแนน
3) ความยาวของกุญแจเข้ารหัส: เว็บไซต์ที่ความยาวของกุญแจเข้ารหัส 256 บิตได้ 1 คะแนน เว็บไซต์ที่ความยาวของกุญแจเข้ารหัส 128 บิต ได้ 0.5 คะแนน เว็บไซต์ที่ไม่เข้ารหัสได้ 0 คะแนน
4) ความยาวรหัสผ่าน: เว็บที่มีการกำหนดความยาวของรหัสผ่านขั้นต่ำ 6 ตัวอักษร ได้ 1 คะแนน เว็บที่มีการกำหนดความยาวของรหัสผ่านขั้นต่ำ 4 ตัวอักษร ได้ 0.5 คะแนน เว็บที่ไม่มีการกำหนดความยาวของรหัสผ่าน ได้ 0 คะแนน
5) ความสลับซับซ้อนของรหัสผ่าน ดูจากการบังคับให้ใช้พยัญชนะตัวพิมพ์ใหญ่ ตัวเลข เป็นส่วนประกอบของรหัสผ่านด้วย เว็บที่กำหนดให้รหัสผ่านประกอบด้วยพยัญชนะภาษาอังกฤษทั้งตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก และตัวเลข ได้ 1 คะแนน เว็บที่กำหนดให้รหัสผ่านประกอบด้วยพยัญชนะภาษาอังกฤษหรือตัวเลขได้ 0.5 คะแนน เว็บที่ไม่กำหนดเงื่อนไขรหัสผ่าน ได้ 0 คะแนน
6) การเก็บรักษารหัสผ่าน: เว็บที่ส่งลิงก์แบบใช้ครั้งเดียวไปทางอีเมลเพื่อเข้าสู่รหัสผ่านใหม่ ได้ 1 คะแนน เว็บที่ให้ผู้ใช้ตอบคำถามเพื่อขอรหัสผ่านใหม่ได้ 0.5 คะแนน เว็บที่ส่งรหัสผ่านทางอีเมลเป็นตัวอักษรแบบไม่เข้ารหัสได้ 0 คะแนน
7) การเก็บข้อมูลด้วยคุกกี้:เว็บไซต์ที่ให้ข้อมูลการเก็บคุกกี้ชัดเจน มีรายละเอียดและเข้าใจง่าย ได้ 1 คะแนน เว็บไซต์ที่ให้ข้อมูลการเก็บคุกกี้ ได้ 0.5 คะแนน เว็บไซต์ที่ไม่ให้ข้อมูลการเก็บคุกกี้ได้ 0 คะแนน
8) ปฏิบัติตามคำขอ "ไม่ติดตาม" หรือไม่: เว็บไซต์ที่สามารถใช้งานได้เมื่อเปิด Privacy Badger เพื่อป้องกันการเก็บข้อมูลคุกกี้ ได้ 1 คะแนน เว็บไซต์ที่ไม่สามารถใช้งานได้เมื่อเปิด Privacy Badger เพื่อป้องกันการเก็บข้อมูลคุกกี้ ได้ 0 คะแนน

9) เว็บไซต์ที่สามารถแก้ปัญหาช่องโหว่ POODLE ได้หรือไม่ ได้ 1 คะแนน เว็บไซต์ที่ลดปัญหา POODLE ได้ แต่ยังเปิดใช้ SSL 3 ได้ 0.5 คะแนน เว็บไซต์ที่เปราะบางต่อช่องโหว่ POODLE ได้ 0 คะแนน
10) เว็บไซต์ที่ใช้ใบรับรอง SHA-2 ได้ 1 คะแนน เว็บไซต์ที่ใช้ใบรับรอง SHA-1 ได้ 0.5 คะแนน
11) การแจ้งว่าเก็บข้อมูลอะไร: ผู้ให้บริการที่แจ้งว่าเก็บข้อมูลอะไรบ้างของผู้ใช้บริการ ละเอียดและชัดเจนได้ 1 คะแนน ผู้ให้บริการที่แจ้งว่าเก็บข้อมูลอะไรบ้างของผู้ใช้บริการ ได้ 0.5 คะแนน ผู้ให้บริการที่ไม่แจ้งว่าเก็บข้อมูลอะไรบ้างของผู้ใช้บริการได้ 0 คะแนน
12) แจ้งวัตถุประสงค์ของการเก็บข้อมูลส่วนตัวของผู้ใช้บริการหรือไม่: ผู้ให้บริการที่แจ้งวัตถุประสงค์ของการเก็บข้อมูลส่วนตัวของผู้ใช้บริการละเอียดและชัดเจนได้ 1 คะแนน ผู้ให้บริการที่แจ้งวัตถุประสงค์ของการเก็บข้อมูลส่วนตัว ได้ 0.5 คะแนน ผู้ให้บริการที่ไม่แจ้งวัตถุประสงค์ของการเก็บข้อมูลส่วนตัว ได้ 0 คะแนน
13) การส่งต่อข้อมูลให้กับบุคคลที่ 3: เว็บที่อธิบายการส่งต่อข้อมูลให้กับบุคคลที่ 3 ละเอียด และชัดเจน ได้ 1 คะแนน เว็บที่แจ้งว่ามีการส่งต่อข้อมูลให้กับบุคคลที่ 3 แต่ไม่ชัดเจน ได้ 0.5 คะแนน เว็บที่ไม่แจ้งรายละเอียดการส่งต่อข้อมูลให้กับบุคคลที่ 3 แก่ผู้ใช้บริการ 0 คะแนน
14) การส่งต่อข้อมูลให้กับเจ้าหน้าที่: ผู้ให้บริการที่แจ้งให้ผู้ใช้บริการรับทราบว่าจะดำเนินการอย่างไร และแจ้งให้ผู้ใช้บริการข้อมูลทราบก่อนส่งต่อข้อมูลให้กับเจ้าหน้าที่ ได้ 1 คะแนน ผู้ให้บริการที่แจ้งให้ผู้ใช้บริการรับทราบว่าจะดำเนินการอย่างไร ได้ 0.5 คะแนน ผู้ให้บริการที่ไม่แจ้งว่าจะดำเนินการอย่างไรเมื่อมีเจ้าหน้าที่รัฐร้องขอข้อมูลส่วนบุคคลของผู้ใช้บริการ ได้ 0 คะแนน
15) ช่องทางการติดต่อกับผู้ให้บริการด้านความปลอดภัยและความเป็นส่วนตัวโดยตรง: ผู้ให้บริการที่แจ้งช่องทางการติดต่อกับเจ้าหน้าที่โดยตรง ได้ 1 คะแนน ผู้ให้บริการที่มีช่องทางการติดต่อ ได้ 0.5 คะแนน ผู้ให้บริการที่ไม่แจ้งช่องทางการติดต่อได้ 0 คะแนน
16) นโยบายเกี่ยวกับความเป็นเจ้าของข้อมูล ในกรณีที่บริษัทหรือบริการถูกซื้อขาย: ผู้ให้บริการที่แจ้งว่าจะดำเนินการกับข้อมูลอย่างไรเมื่อบริษัทเปลี่ยนมือเจ้าของเก็บข้อมูลได้ 1 คะแนน ผู้ให้บริการที่ไม่แจ้งว่าจะดำเนินการกับข้อมูลอย่างไรเมื่อบริษัทเปลี่ยนมือเจ้าของเก็บข้อมูลได้ 0 คะแนน
17) การจัดทำนโยบายความเป็นส่วนตัวที่เข้าใจง่าย: ผู้ให้บริการที่มีภาษาที่ใช้ในข้อตกลงการใช้และบริการเข้าใจง่าย ละเอียด และชัดเจน ได้ 1 คะแนน ผู้ให้บริการที่มีภาษาที่ใช้ในข้อตกลงการใช้และบริการไม่ละเอียด และชัดเจน ได้ 0 คะแนน

ข้อสังเกต

จากการประเมินมาตรการคุ้มครองความปลอดภัยและความเป็นส่วนตัวของผู้ให้บริการออนไลน์ไทย พบข้อสังเกตที่น่าสนใจหลายประการ ดังนี้

1. มีเพียงร้อยละ 31 ของเว็บไซต์กลุ่มตัวอย่างที่ได้คะแนนเกินครึ่ง (13 เว็บไซต์จากทั้งหมด 45 เว็บไซต์) เว็บไซต์ที่ได้คะแนนมากที่สุดคือ เว็บไซต์แอร์เอเชีย ส่วนเว็บไซต์ธนาคารจัดอยู่ในกลุ่มเว็บไซต์ที่ได้คะแนนสูง เมื่อเทียบกับบริการออนไลน์ประเภทอื่นๆ ส่วนหน่วยงานรัฐและมหาวิทยาลัยอยู่ในกลุ่มคะแนนต่ำที่สุด
2. เมื่อเปรียบเทียบกับบริการประเภทอื่นๆ เว็บไซต์สายการบินให้ความสำคัญกับนโยบายด้านข้อมูลมากที่สุด เหตุผลที่ทำให้เป็นเช่นนี้เนื่องจากเป็นธุรกิจที่ดำเนินการระหว่างประเทศ ซึ่งแม้ในประเทศไทยจะยังไม่มีกฎหมายกลางด้านการคุ้มครองข้อมูลส่วนบุคคล แต่ธุรกิจสายการบินจำเป็นต้องปฏิบัติตามกฎหมายด้านการคุ้มครองส่วนบุคคลของประเทศอื่นๆ จึงทำให้ต้องมีมาตรการที่ครอบคลุมความปลอดภัยและความเป็นส่วนตัวของข้อมูลไปด้วย ตัวอย่างที่เห็นได้ชัดเจนคือ สายการบินแอร์เอเชียที่บริษัทแม่อยู่ที่ประเทศมาเลเซีย ซึ่งมีคะแนนด้านการคุ้มครองทางเทคนิคสูงที่สุด และเป็นบริการเดียวที่แจ้งว่าจะปฏิบัติต่อข้อมูลส่วนตัวอย่างไร หากมีการซื้อขายกิจการ



การใช้ข้อมูลที่รวบรวม

โดยทั่วไป เราจะใช้ข้อมูลของคุณเพื่อบริหารจัดการ เช่น การดำเนินการ การยืนยัน การตอบสนอง และการทำธุรกรรมให้เสร็จสมบูรณ์ และคำขอใช้บริการของเรา ในกรณีที่มีการเปลี่ยนแปลง / แก้ไขตารางเที่ยวบิน เราจะใช้ข้อมูลที่คุณให้ไว้เมื่อคุณจองตั๋วเดินทางผ่านเว็บไซต์อย่างเป็นทางการของเราที่ www.airasia.com, ศูนย์บริการลูกค้าสัมพันธ์ (Call Centre) และเคาน์เตอร์จำหน่ายตั๋วของเรา เพื่อติดต่อและแจ้งให้ทราบถึงการเปลี่ยนแปลง / แก้ไข นอกจากนี้ เราจะใช้ข้อมูลของคุณเพื่อการทำบัญชี (การเรียกเก็บเงินและการตรวจสอบบัญชี) การตรวจคนเข้าเมือง การควบคุมทางศุลกากร ความปลอดภัย ความมั่นคง การวิเคราะห์ทางสถิติและการตลาด การจัดการระบบข้อมูล การทดสอบระบบ การปรับรุงรักษาและการพัฒนา การดำเนินงาน การสนับสนุน การสำรวจความคิดเห็นลูกค้า ลูกค้าสัมพันธ์ และเพื่อปรับปรุงและช่วยให้เราติดต่อกับคุณในอนาคต เช่น การระบุความต้องการและความชอบของคุณ

ในกรณีการจ้างงาน เราจะใช้ข้อมูลที่คุณให้ไว้โดยสมัครใจเพื่อเปรียบเทียบกับข้อกำหนด / เกณฑ์ของงานที่เรามองหา / ต้องการจ้าง

เมื่อใช้กฎหมายบังคับ เราจะเปิดเผยข้อมูลของคุณให้กับองค์กรหรือหน่วยงานของรัฐบาลหรือบุคคลที่สามตามหมายศาลหรือกระบวนการทางกฎหมายอื่นๆ นอกจากนี้ เรายังอาจใช้หรือเปิดเผยข้อมูลของคุณตามที่กฎหมายอนุญาต เพื่อปกป้องสิทธิหรือทรัพย์สินของแอร์เอเชีย ลูกค้าของเรา เว็บไซต์ของเรา หรือผู้ใช้เว็บไซต์ดังกล่าว เรายังอาจเปิดเผยข้อมูลบางส่วนหรือทั้งหมดของคุณต่อบริษัทที่เรามีสัญญาหรือให้อนุญาต เช่น ผู้ประมวลผลข้อมูล

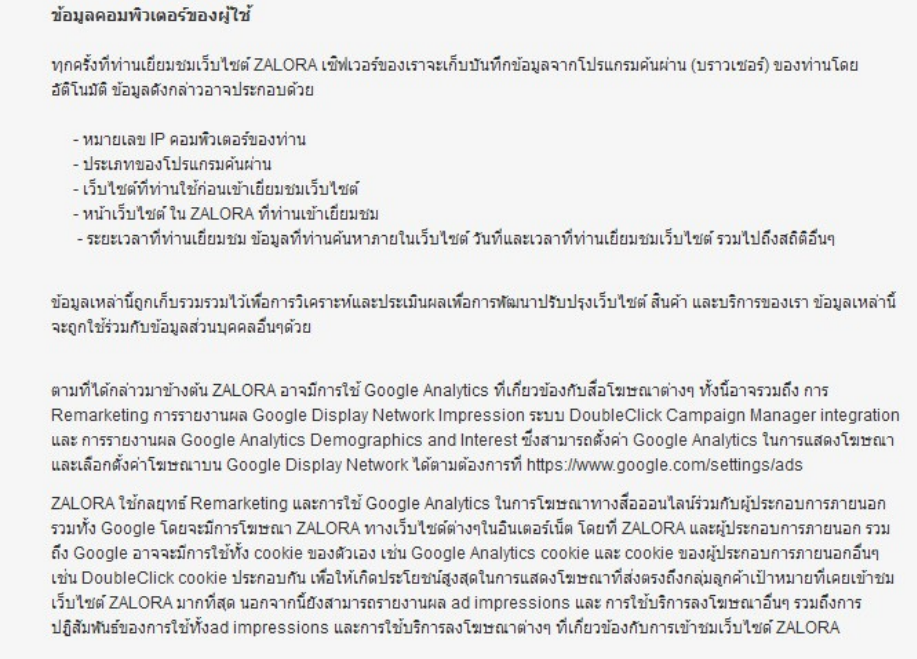
จากส่วนหนึ่งในความพยายามของเราเพื่อให้บริการที่ดียิ่งขึ้น เรามีการปรับปรุงและขยายบริการของเราอย่างสม่ำเสมอเพื่อตอบสนองความต้องการที่เพิ่มขึ้นตลอดเวลา เพื่อบรรลุวัตถุประสงค์ทางธุรกิจนี้ เราจะแต่งตั้ง ให้อนุญาต หรือทำสัญญากับพันธมิตรธุรกิจเชิงกลยุทธ์เป็นครั้งคราว เราจะเปิดเผยข้อมูลของคุณแก่พันธมิตรธุรกิจเหล่านี้ บุคคลที่สาม ผู้ให้บริการ หรือผู้โฆษณาซึ่งมีสัญญาหรือได้รับอนุญาต เพื่อนำเสนอโปรโมชั่น ข้อเสนอ ผลิตภัณฑ์ หรือบริการ ซึ่งไม่ใช่ของเรา อย่างไรก็ตาม เพื่อให้แน่ใจว่าคุณจะไม่ได้รับการติดต่อที่ไม่ต้องการ เราจะแบ่งปันเฉพาะข้อมูลที่เกี่ยวกับโปรโมชั่น ข้อเสนอ ผลิตภัณฑ์ หรือบริการที่คุณเลือกหรือทำเครื่องหมายว่าสนใจผ่านประวัติส่วนตัวสมาชิกของเรากับพันธมิตรธุรกิจ ผู้ให้บริการ หรือบุคคลที่สามที่เกี่ยวข้องเท่านั้น

ในกรณีที่อ้างถึงนโยบายนี้ เมื่อแอร์เอเชียส่งผ่านข้อมูลของคุณให้กับบุคคลที่สาม เราจะทำให้แน่ใจว่ามาตรการความปลอดภัยของบุคคลดังกล่าวที่เกี่ยวข้องกับการประมวลผลข้อมูลของคุณนั้นมีความเข้มงวดกว่าหรือไม่น้อยกว่ามาตรการของแอร์เอเชีย แต่จะไม่รวมในกรณีที่ใช้กฎหมายบังคับให้เราส่งผ่านข้อมูลของคุณให้กับบุคคลที่สาม

ในกรณีที่เรามีการเปลี่ยนผ่านธุรกิจ เช่น การขายสินทรัพย์บางส่วนหรือทั้งหมด การควบรวมกิจการ หรือการซื้อกิจการ ข้อมูลของคุณจะเป็นส่วนหนึ่งของการเปลี่ยนผ่านนี้และจะถูกโอนย้ายไป

ตัวอย่างการแจ้งให้ผู้ใช้บริการทราบถึงการเก็บรวบรวมข้อมูลของแอร์เอเชีย

3. หน่วยงานรัฐและมหาวิทยาลัยให้ความสำคัญกับการปกป้องความปลอดภัยด้านเทคนิคมากกว่าการคุ้มครองข้อมูลส่วนตัวของผู้ใช้บริการ ดังเห็นได้จากระดับคะแนนด้านนโยบายข้อมูลซึ่งเกือบทั้งหมดได้ 0 คะแนน ซึ่งมาจากการที่ไม่มีนโยบายความเป็นส่วนตัวเลย
4. เว็บไซต์จำนวนหนึ่งแม้จะมีลิงก์แสดงนโยบายข้อมูลส่วนบุคคลก็ตาม แต่เมื่อคลิกเข้าไปแล้วปรากฏว่าไม่มีหน้านโยบายความเป็นส่วนตัว ขณะที่บางเว็บไซต์เป็นภาษาอังกฤษ
5. ขณะที่ทุกเว็บไซต์มีการเก็บข้อมูลคุกกี้ ซึ่งเป็นการเก็บข้อมูลการเข้าชมเว็บไซต์ มีบางเว็บไซต์เท่านั้นที่แจ้งให้ทราบอย่างละเอียดว่าเก็บข้อมูลอะไรบ้าง ตัวอย่างคือ เว็บไซต์ Zalora



ข้อมูลคอมพิวเตอร์ของผู้ใช้

ทุกครั้งที่ท่านเยี่ยมชมเว็บไซต์ ZALORA เซิฟเวอร์ของเราจะเก็บบันทึกข้อมูลจากโปรแกรมค้นผ่าน (บราวเซอร์) ของท่านโดยอัตโนมัติ ข้อมูลดังกล่าวอาจประกอบด้วย

- หมายเลข IP คอมพิวเตอร์ของท่าน
- ประเภทของโปรแกรมค้นผ่าน
- เว็บไซต์ที่ท่านใช้ก่อนเข้าเยี่ยมชมเว็บไซต์
- หน้าเว็บไซต์ ใน ZALORA ที่ท่านเข้าเยี่ยมชม
- ระยะเวลาที่ท่านเยี่ยมชม ข้อมูลที่ท่านค้นหาภายในเว็บไซต์ วันที่และเวลาที่ท่านเยี่ยมชมเว็บไซต์ รวมไปถึงสถิติอื่นๆ

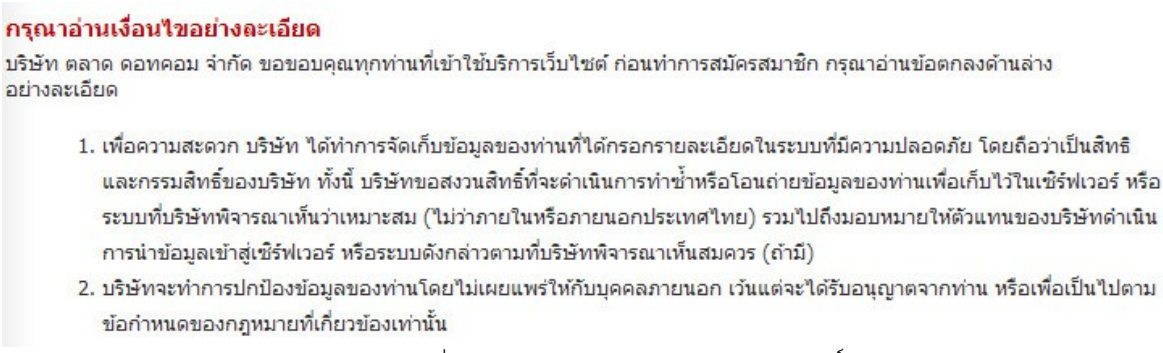
ข้อมูลเหล่านี้ถูกเก็บรวมรวมไว้เพื่อการวิเคราะห์และประเมินผลเพื่อการพัฒนาปรับปรุงเว็บไซต์ สินค้า และบริการของเรา ข้อมูลเหล่านี้จะถูกใช้ร่วมกับข้อมูลส่วนบุคคลอื่นๆด้วย

ตามที่ได้กล่าวมาข้างต้น ZALORA อาจมีการใช้ Google Analytics ที่เกี่ยวข้องกับสื่อโฆษณาต่างๆ ทั้งนี้อาจรวมถึง การ Remarketing การรายงานผล Google Display Network Impression ระบบ DoubleClick Campaign Manager integration และ การรายงานผล Google Analytics Demographics and Interest ซึ่งสามารถตั้งค่า Google Analytics ในการแสดงโฆษณาและเลือกตั้งค่าโฆษณาบน Google Display Network ได้ตามต้องการที่ https://www.google.com/settings/ads

ZALORA ใช้กลยุทธ์ Remarketing และการใช้ Google Analytics ในการโฆษณาทางสื่อออนไลน์ร่วมกับผู้ประกอบการภายนอก รวมทั้ง Google โดยจะมีการโฆษณา ZALORA ทางเว็บไซต์ต่างๆในอินเตอร์เน็ต โดยที่ ZALORA และผู้ประกอบการภายนอก รวมถึง Google อาจจะมีการใช้ทั้ง cookie ของตัวเอง เช่น Google Analytics cookie และ cookie ของผู้ประกอบการภายนอกอื่นๆ เช่น DoubleClick cookie ประกอบกัน เพื่อให้เกิดประโยชน์สูงสุดในการแสดงโฆษณาที่ส่งตรงถึงกลุ่มลูกค้าเป้าหมายที่เคยเข้าชมเว็บไซต์ ZALORA มากที่สุด นอกจากนี้ยังสามารถรายงานผล ad impressions และ การใช้บริการลงโฆษณาอื่นๆ รวมถึงการปฏิสัมพันธ์ของการใช้ทั้งad impressions และการใช้บริการลงโฆษณาต่างๆ ที่เกี่ยวข้องกับการเข้าชมเว็บไซต์ ZALORA

ตัวอย่างการแจ้งรายละเอียดข้อมูลคอมพิวเตอร์ที่เว็บไซต์ Zalora จัดเก็บ
(http://www.zalora.co.th/privacy-policy)

6. บางเว็บไซต์ได้ระบุอย่างกว้างว่าจะจัดเก็บข้อมูลส่วนบุคคลที่ผู้ใช้บริการมอบให้อย่างปลอดภัย โดยไม่ชี้แจงรายละเอียดว่ามีวิธีจัดเก็บอย่างไร อีกทั้งยังอ้างความเป็นเจ้าของข้อมูลด้วย ตัวอย่างเช่น เว็บไซต์ตลาดดอทคอม



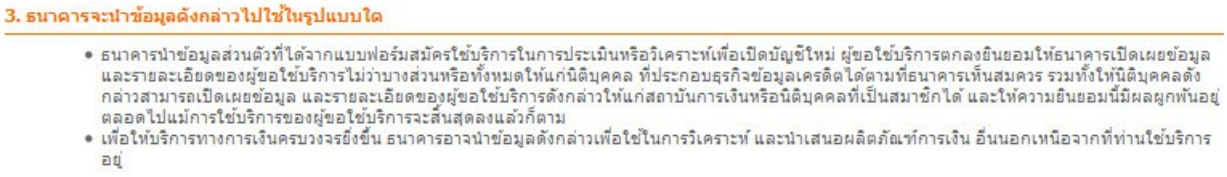
กรุณาอ่านเงื่อนไขอย่างละเอียด

บริษัท ตลาด ดอทคอม จำกัด ขอขอบคุณทุกท่านที่เข้าใช้บริการเว็บไซต์ ก่อนทำการสมัครสมาชิก กรุณาอ่านข้อตกลงด้านล่างอย่างละเอียด

1. เพื่อความสะดวก บริษัท ได้ทำการจัดเก็บข้อมูลของท่านที่ได้กรอกรายละเอียดในระบบที่มีความปลอดภัย โดยถือว่าเป็นสิทธิและกรรมสิทธิ์ของบริษัท ทั้งนี้ บริษัทขอสงวนสิทธิ์ที่จะดำเนินการทำซ้ำหรือโอนถ่ายข้อมูลของท่านเพื่อเก็บไว้ในเซิร์ฟเวอร์ หรือระบบที่บริษัทพิจารณาเห็นว่าเหมาะสม (ไม่ว่าภายในหรือภายนอกประเทศไทย) รวมไปถึงมอบหมายให้ตัวแทนของบริษัทดำเนินการนำข้อมูลเข้าสู่เซิร์ฟเวอร์ หรือระบบดังกล่าวตามที่บริษัทพิจารณาเห็นสมควร (ถ้ามี)
2. บริษัทจะทำการปกป้องข้อมูลของท่านโดยไม่เผยแพร่ให้กับบุคคลภายนอก เว้นแต่จะได้รับอนุญาตจากท่าน หรือเพื่อเป็นไปตามข้อกำหนดของกฎหมายที่เกี่ยวข้องเท่านั้น

ตัวอย่างผู้ให้บริการที่อ้างว่าข้อมูลของผู้ใช้บริการเป็นกรรมสิทธิ์ของบริษัท
(http://www.tarad.com/faq/term_condition)

7. การนำข้อมูลไปใช้ของผู้ให้บริการบางรายไม่มีระยะเวลาสิ้นสุด แม้การใช้บริการจะสิ้นสุดแล้วก็ตาม เมื่อยอมรับข้อตกลงแล้วผู้ให้บริการถือว่าความยินยอมนี้มีผลผูกพันอยู่ตลอดไป ตัวอย่างเช่น ธนาคารธนชาต



3. ธนาคารจะนำข้อมูลดังกล่าวไปใช้ในรูปแบบใด

- ธนาคารนำข้อมูลส่วนตัวที่ได้จากแบบฟอร์มสมัครใช้บริการในการประเมินหรือวิเคราะห์เพื่อเปิดบัญชีใหม่ ผู้ขอใช้บริการตกลงยินยอมให้ธนาคารเปิดเผยข้อมูลและรายละเอียดของผู้ขอใช้บริการไม่ว่าบางส่วนหรือทั้งหมดให้แก่นิติบุคคล ที่ประกอบธุรกิจข้อมูลเครดิตได้ตามที่ธนาคารเห็นสมควร รวมทั้งให้นิติบุคคลดังกล่าวสามารถเปิดเผยข้อมูล และรายละเอียดของผู้ขอใช้บริการดังกล่าวให้แก่สถาบันการเงินหรือนิติบุคคลที่เป็นสมาชิกได้ และให้ความยินยอมนี้มีผลผูกพันอยู่ตลอดไปแม้การใช้บริการของผู้ขอใช้บริการจะสิ้นสุดลงแล้วก็ตาม
- เพื่อให้บริการทางการเงินครบวงจรยิ่งขึ้น ธนาคารอาจนำข้อมูลดังกล่าวเพื่อใช้ในการวิเคราะห์ และนำเสนอผลิตภัณฑ์การเงิน อื่นนอกเหนือจากที่ท่านใช้บริการอยู่

ตัวอย่างการระบุไว้ในนโยบายข้อมูลส่วนบุคคลเกี่ยวกับการเปิดเผยข้อมูลแม้จะผู้ใช้จะเลิกใช้บริการแล้วก็ตาม

(http://www.thanachartbank.co.th/TbankCMSFrontend/SecurityTH.aspx)

8. ในข้อตกลงการให้บริการ หรือนโยบายความเป็นส่วนตัวของบางเว็บไซต์ได้ระบุว่า ไม่รับรองความปลอดภัยของข้อมูลส่วนบุคคล เมื่อเกิดความบกพร่องทางเทคนิค เว็บไซต์จะปฏิเสธความรับผิดทั้งหมด ตัวอย่างเช่น เว็บไซต์ตลาดงาน ของกรมจัดหางาน

2.4 สำหรับบริการที่ต้องสมัครสมาชิก ท่านต้องรับผิดชอบในการรักษาความลับของรหัสผ่านและบัญชีของท่าน และรับผิดชอบในกิจกรรมทั้งหมดที่เกิดขึ้นภายใต้รหัสผ่านหรือบัญชีของท่าน แม้กิจกรรมนั้นจะทำขึ้นโดยบุคคลอื่นซึ่งเข้าสู่บัญชีของท่านผ่านรหัสผ่านของท่านก็ตาม

2.5 กรมการจัดหางานถือว่าข้อมูลส่วนบุคคลของท่านในบริการของกรมการจัดหางานเป็นสิ่งที่สำคัญที่จะต้องปกป้องดูแล กรมการจัดหางานได้ใช้วิธีการมาตรฐานในการเก็บรักษาความปลอดภัยของข้อมูลส่วนบุคคลของท่าน แต่ไม่มีเนื้อหาใดในบริการที่จะได้รับการรับรองว่าจะปลอดภัยอย่างสมบูรณ์ ดังนั้น กรมการจัดหางานจึงไม่รับรองและรับประกันใดๆ ทั้งสิ้นว่ากรมการจัดหางานมีมาตรการความปลอดภัยที่เพียงพอแล้ว และข้อมูลส่วนบุคคลและเนื้อหาที่ปรากฏในบริการจะปลอดภัย ในกรณีที่ข้อมูลส่วนบุคคลของท่านถูกจารกรรมโดยวิธีการทางอิเล็กทรอนิกส์ (hack) สูญหาย หรือเสียหายอันเนื่องจากเหตุสุดวิสัย จากการละเมิดมาตรการความปลอดภัยโดยบุคคลใดๆ จากความบกพร่องด้านเทคนิคของกรมการจัดหางาน หรือไม่ว่าเหตุใดๆ กรมการจัดหางานขอสงวนสิทธิในการปฏิเสธความรับผิดจากเหตุดังกล่าวทั้งหมด

ตัวอย่างการระบุเงื่อนไขการรับผิดไว้ล่วงหน้าของผู้ให้บริการ

(http://job.doe.go.th/screen/register_rule.php)

บทสรุป

การปกป้องความปลอดภัยและความเป็นส่วนตัวของผู้ใช้อินเทอร์เน็ตสามารถทำได้หลายวิธี ตั้งแต่ระดับปัจเจกบุคคล ไปจนถึงระดับรัฐ ในโลกยุคดิจิทัลนี้ ผู้ให้บริการออนไลน์เป็นผู้พิทักษ์ และผู้สัมผัสข้อมูลส่วนตัวของเราอย่างใกล้ชิดมากที่สุด ตั้งแต่เนื้อหาในอีเมล ข้อมูลตำแหน่งที่อยู่ ไปจนถึงความสัมพันธ์ทางสังคมของเรา และครอบครัวของเรา วิธีที่ผู้ให้บริการเหล่านี้ปฏิบัติและนโยบายข้อมูลส่วนบุคคลที่มีนั้นสามารถกำหนดได้ว่าผู้ใช้อินเทอร์เน็ตแต่ละคนจะสื่อสารอย่างปลอดภัยหรือไม่ รวมถึงมีสิทธิเสรีภาพในการสื่อสารโดยปราศจากการสอดแนมจากรัฐได้อีกด้วย ผู้ให้บริการออนไลน์จึงควรตระหนักถึงความสำคัญของตนเองในฐานะผู้ปกป้องข้อมูลส่วนตัวของผู้ใช้อินเทอร์เน็ต

ในภาพรวมผู้ให้บริการออนไลน์ให้ความสำคัญกับความปลอดภัยทางเทคนิคค่อนข้างมาก มีความพยายามใช้การเข้ารหัสการเชื่อมต่อ อย่างไรก็ตามเนื่องจากความน่าเชื่อถือและความปลอดภัยยังขึ้นอยู่กับรายละเอียดของใบรับรองความปลอดภัย และระดับความยากง่ายของการเข้ารหัสอีกด้วย ผู้ให้บริการจึงควรปรับปรุงระบบความปลอดภัยและการเข้ารหัสการเชื่อมต่อให้ใหม่ล่าสุดอยู่เสมอ เพื่อให้สามารถรับมือกับการคุกคามทางอินเทอร์เน็ตได้

ขณะที่การแจ้งให้ผู้ใช้บริการทราบว่า ข้อมูลของตนเองจะถูกดำเนินการอย่างไรจากผู้ให้บริการได้รับความสนใจน้อยกว่าผู้ให้บริการโดยส่วนใหญ่มักไม่ระบุรายละเอียดให้ชัดเจนเกี่ยวกับการจัดเก็บข้อมูล ตั้งแต่วัตถุประสงค์ ข้อมูลที่จัดเก็บ การส่งต่อให้กับบุคคลที่ 3 ระยะเวลา การจัดการกับข้อมูลเมื่อมีการโอนย้ายกิจการ แต่ใช้คำพูดแบบกว้างๆ โดยให้ผู้ใช้บริการเชื่อมั่นว่าบริษัทมีความพยายามคุ้มครองข้อมูลของลูกค้า นอกจากนี้ผู้ให้บริการจำนวนหนึ่งยังใช้วิธีแจ้งให้ทราบในขั้นตอนยินยอมเงื่อนไขการให้บริการว่า ผู้ให้บริการจะไม่รับผิดชอบในกรณีที่เกิดการรั่วไหลของข้อมูลขึ้น