

เว็บไซต์ของคุณต้องการ การรักษาความปลอดภัย หรือไม่?

INTERRISK ASIA (THAILAND) CO., LTD.



40,000

มากกว่า 40,000
เว็บไซต์โดนแฮกต่อวัน



86%

ของเว็บไซต์มีข้อมูลสำคัญ
สามารถรั่วไหลได้



1 ล้าน

ภัยคุกคาม หรือ มัลแวร์
ถูกสร้างเพิ่มขึ้นทุกวัน



\$6 ล้านล้าน

คิดเป็นความเสียหายที่อาจ
เกิดขึ้นในปี 2021

ความปลอดภัยเว็บไซต์ จำเป็นหรือไม่?

เว็บไซต์ของคุณมีความปลอดภัยแค่ไหน?
ผู้ใช้งานทั่วไปอาจไม่คำนึงถึงเรื่องความเสี่ยงของ
เว็บไซต์ที่ไม่ปลอดภัยและความเสียหายที่อาจจะเกิดขึ้น
เราจึงขอแนะนำวิธีการรักษาความปลอดภัยสำหรับเว็บไซต์ของคุณ
ซึ่งสามารถช่วยให้ธุรกิจของคุณปลอดภัยจากผู้ไม่หวังดี
ขั้นแรกเราต้องรู้จักคำว่า "SSL certificate" คืออะไร
ควรใช้ประเภทใด และทำไมเราจำเป็นต้องใช้

SSL certificate คืออะไร?

SSL certificate หรือ Secure Sockets Layer
certificate คือ การตรวจสอบโดยบุคคลที่สาม
ซึ่งใช้เทคโนโลยีเพื่อป้องกันข้อมูลรั่วไหลโดยการเข้ารหัส
(encryption)

โดยทั่วไปข้อมูลสามารถแลกเปลี่ยนได้หลายแบบ
อย่างเช่น การเขียนข้อความในบล็อก การพิมพ์ข้อมูล
login หรือหน้าต่างอื่นๆในเว็บไซต์ อย่างไรก็ตาม
ทุกเว็บไซต์ต้องมี SSL certificate อย่างน้อยหนึ่งใบ

เว็บไซต์ มีหลายประเภท:

บล็อก หรือ เว็บไซต์ที่ให้ข้อมูลทั่วไป:

เว็บไซต์ประเภทนี้เก็บข้อมูลของคุณโดยใช้ Google Analytics และ Cookies ดังนั้นการรักษาความปลอดภัยจึงไม่ซับซ้อนมาก เนื่องจากไม่มีการเก็บข้อมูลส่วนตัว

เว็บไซต์บริษัท:

ข้อมูลได้มาจากการค้นหาของผู้ใช้งานเว็บไซต์ซึ่งจะถูกนำมาใช้ในการกำหนดเป้าหมายทางการตลาด อย่างไรก็ตามข้อมูลต้องได้รับการยินยอมจากผู้ใช้งาน ยิ่งข้อมูลมีจำนวนมากเท่าใด ความเสี่ยงในการถูกขโมยก็ยิ่งสูงขึ้นมากเท่านั้น ดังนั้นความปลอดภัยสำหรับเว็บไซต์ประเภทนี้จึงเป็นสิ่งสำคัญ

เว็บไซต์ที่มีการสนับสนุนจากโฆษณา:

ข้อมูลของผู้ใช้งานเว็บไซต์จะถูกนำไปใช้ในเครือข่ายของบริษัทโฆษณา ซึ่งข้อมูลดังกล่าวจะถูกจัดเก็บหรือใช้งานโดยวิธีใดขึ้นอยู่กับองค์กรนั้นๆ รวมถึงเว็บไซต์ประเภทนี้จะมีการแชร์ข้อมูลบน social network อย่างเช่น Facebook เป็นต้น

เว็บไซต์ขายของ (E-commerce) :

การซื้อขายบนเว็บไซต์จำเป็นต้องใช้ข้อมูลพื้นฐาน อย่างเช่น ที่อยู่ เบอร์โทรศัพท์ หมายเลขบัตรเครดิต และอื่นๆ ซึ่งการใช้ username และ password ทำให้เว็บมีความเสี่ยงมากขึ้นจากเหล่าแฮกเกอร์ จึงจำเป็นต้องมีมาตรการรักษาความปลอดภัยที่สูงขึ้น เช่น ข้อมูลต้องได้รับการเข้ารหัส และควรมีใบรับรอง SSL

เว็บไซต์ที่มีการแสดงความคิดเห็นและข้อมูลส่วนบุคคล:

เว็บไซต์ที่มีการบันทึกหัวข้อทางด้านศาสนา การแพทย์ หรือ อาชญากรรม ซึ่งเป็นข้อมูลที่อาจส่งผลกระทบต่อผู้ใช้งาน ดังนั้นถือว่าเป็นกรณีที่ต้องมีการป้องกันเป็นพิเศษ

ประเภท SSL Certificate:

ต้องมี SSL certificate กี่ใบ?

จำนวน SSL certificate ขึ้นอยู่กับจำนวน 'common name' ของเว็บไซต์ ถ้าหากเว็บไซต์สามารถเข้าได้สองแบบ ตัวอย่างเช่น ไม่ว่าผู้ใช้งานจะพิมพ์ "www.example.com" หรือ "example.com" ก็สามารถเข้าถึงเว็บไซต์ดังกล่าวได้เช่นเดียวกัน ดังนั้นเว็บไซต์นี้จำเป็นต้องมี SSL certificate อย่างน้อยสองใบ และถ้ามีเซิร์ฟเวอร์หลายตัว ควรใช้ SSL certificate หลายใบเช่นเดียวกัน

ประเภทของ SSL certificate มี 3 ประเภทได้แก่

1. Domain Validated (DV) ซึ่งเป็น certificate พื้นฐาน โดยหน่วยงาน "Certificate Authorities" จะต้องส่ง email ถึง domain admin ของเว็บไซต์นั้นๆ ถ้าหากต้องการให้เว็บไซต์ปลอดภัยยิ่งขึ้น ต้องมี SSL ประเภทอื่นร่วมด้วย

2. Organizational Validated (OV) จะมีการตรวจสอบที่เข้มงวดมากขึ้น มีรายละเอียดของบริษัทเช่น ชื่อบริษัท ชื่อเจ้าของบริษัท และ ที่อยู่ ซึ่งข้อมูลเหล่านี้จะต้องปรากฏบนเว็บไซต์

3. Extended Validation (EV) จะแสดงเครื่องหมายอย่างชัดเจนว่าเว็บไซต์มีความปลอดภัย ตัวอย่างเช่น address bar สีเขียวบน browser เป็นการแสดงว่า บริษัทได้ให้ข้อมูลโดยละเอียดซึ่งได้รับการตรวจสอบโดยผู้ออกใบรับรอง (Certificate Authority)

ทำไมต้องระวังเรื่องความปลอดภัยของเว็บไซต์?

รายได้:

การที่เว็บไซต์ไม่มีการป้องกันใดๆ จะถูกจัดอยู่ในบัญชีดำของ Google ซึ่งส่งผลให้เว็บไซต์ถูกระงับการใช้งานได้

ความน่าเชื่อถือและความไว้วางใจ:

หากเว็บไซต์ไม่มีการใช้ SSL certificate ผู้ใช้งานเว็บไซต์อาจลังเลในการซื้อสินค้าและทำให้ลูกค้าคิดวาทกรรมการจัดการที่ดี

ผลการจัดอันดับของ Search Engine:

หากในกรณีที่เว็บไซต์ของคุณไม่ปลอดภัย เว็บไซต์ของคุณจะไม่ปรากฏในรายการค้นหา และถูกจัดอยู่ในบัญชีดำเป็นเวลา 6 สัปดาห์หลังจากที่ถูกตรวจสอบ แม้ว่าเว็บไซต์ไม่ได้ถูกจัดอยู่ในบัญชีดำ ผู้ใช้งานเว็บไซต์จะเข้าถึงน้อยลงหากมีการเตือนว่าเว็บไซต์ไม่ปลอดภัย ซึ่งทำให้อันดับของเว็บไซต์ต่ำลงด้วยเช่นกัน

ข้อมูลเพิ่มเติม:

<https://www.symantec.com/connect/blogs/types-ssl-certificates-choose-right-one>

<http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html>

<https://www.scmagazine.com/whitehat-security-release-website-security-statistics-report/article/536252/>

<https://www.techopedia.com/definition/24747/cybersecurity>

<http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/>