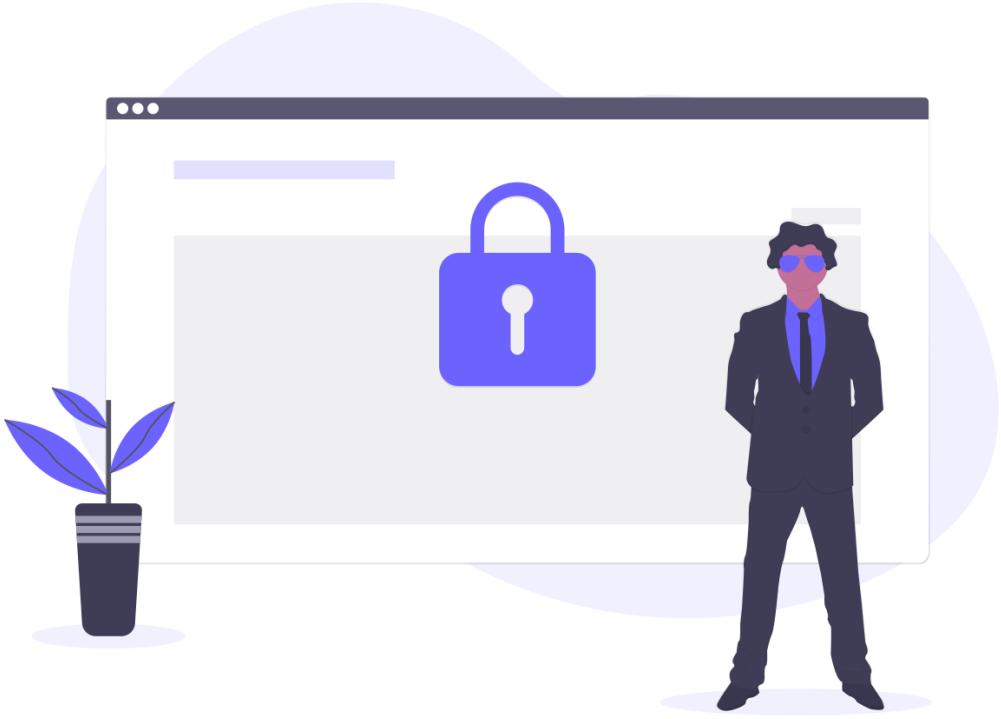
somyos.jin@kmutt.ac.th
5/3/21

ปกป้องเว็บไซต์และผู้ใช้ของคุณให้ปลอดภัยด้วย HTTPS



HTTPS

Hypertest Transfer Protocol Secure

HTTPS (Hypertext Transfer Protocol Secure) คือโปรโตคอลการสื่อสารอินเทอร์เน็ตที่ช่วยรักษาความสมบูรณ์ถูกต้องของข้อมูลผู้ใช้และเก็บข้อมูลไว้เป็นความลับระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์ ผู้ใช้คาดหวังประสบการณ์ออนไลน์ที่มีความปลอดภัยและเป็นส่วนตัวระหว่างที่ใช้เว็บไซต์ เราขอแนะนำให้คุณใช้ HTTPS เพื่อปกป้องการเชื่อมต่อของผู้ใช้กับเว็บไซต์ ไม่ว่าเนื้อหาในเว็บไซต์จะเป็นรูปแบบใดก็ตาม ข้อมูลที่ส่งด้วย HTTPS จะได้รับการรักษาความปลอดภัยผ่านโปรโตคอลความปลอดภัยชั้นการรับส่งข้อมูล (TLS) ซึ่งให้การปกป้องหลัก 3 ชั้น ดังนี้

1. การเข้ารหัส หมายถึง การเข้ารหัสข้อมูลที่แลกเปลี่ยนเพื่อรักษาความปลอดภัยจากผู้ลักลอบดูข้อมูล ซึ่งหมายความว่าขณะที่ผู้ใช้เรียกดูเว็บไซต์ จะไม่มีใครสามารถ "ฟัง" การสนทนาของพวกเขา ติดตามกิจกรรมของพวกเขาไปตลอดหลายหน้า หรือขโมยข้อมูลของพวกเขาได้

2. ความถูกต้องสมบูรณ์ของข้อมูล หมายถึง จะไม่สามารถแก้ไขหรือทำให้ข้อมูลเสียหายในช่วงที่ถ่ายโอนข้อมูลไม่ว่าจะมีเจตนาหรือไม่ก็ตาม โดยที่ไม่มีการตรวจพบ

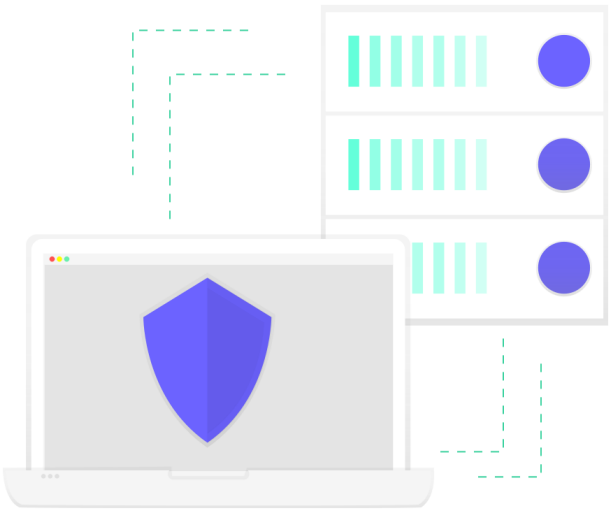
3. การตรวจสอบสิทธิ์ หมายถึง การพิสูจน์ว่าผู้ใช้สื่อสารกับเว็บไซต์ที่เขาต้องการ โดยจะป้องกันการโจมตีจากบุคคลที่อยู่ตรงกลางและทำให้ผู้ใช้เกิดความเชื่อมั่น ซึ่งทำให้เกิดผลประโยชน์อื่นๆ ในทางธุรกิจตามมา

ต้นฉบับ : https://support.google.com/webmasters/answer/6073543?hl=th

somyos.jin@kmutt.ac.th
5/3/21

ทำอย่างไร

3 ขั้นตอน เพื่อให้รองรับ HTTPS



ขั้นตอนที่ 1 เว็บไซต์ใช้ระบบชื่อโดเมน (DNS) แบบใด

A. http://**aaa**.kmutt.ac.th

ตัวอย่าง http://global.kmutt.ac.th

โปรดข้ามไปอ่านรายละเอียด **หน้าที่ 4**

B. http://**bbb.aaa**.kmutt.ac.th

ตัวอย่าง http://www.gloal.kmutt.ac.th

โปรดข้ามไปอ่านรายละเอียด **หน้าที่ 5**

เว็บไซต์ใช้แบบ A (http://aaa.kmutt.ac.th)

ดูแลเครื่องแม่ข่าย (Server) และระบบชื่อโดเมน (DNS) โดยหน่วยงาน/ตนเอง หรือไม่ ?

(a) ดูแลโดยหน่วยงาน/ตนเอง มี 2 ทางเลือก คือ

1) ผู้ดูแลดำเนินการสร้างไฟล์ CSR ส่งถึงสำนักคอมพิวเตอร์ทางอีเมล ccsupport@kmutt.ac.th เพื่อดำเนินการออก SSL Certifcate ให้กับผู้ดูแลนำไปดำเนินการติดตั้งบนเครื่องแม่ข่าย (Server)

อ่านขั้นตอนการสร้างไฟล์ CSR และการติดตั้ง SSL Certifcate ได้ที่ https://www.alphassl.com/support/index.html

หมายเหตุ SSL Certificate มีอายุการใช้งาน 1 ปี เมื่อหมดอายุ โปรดอย่าลืมดำเนินการใหม่อีกครั้ง

2) ผู้ดูแลดำเนินการตั้งค่าระบบชื่อโดเมน (DNS) มาใช้งาน Reverse proxy ที่หมายเลข IP ที่ **202.44.11.178** และติดต่อสำนักคอมพิวเตอร์ในขั้นตอน (b)

กรณีหน่วยงานใช้บริการระบบชื่อโดเมน (DNS) จากทางสำนักคอมพิวเตอร์ หรือไม่ทราบ โปรดใช้ขั้นตอนในคำตอบ **(b)** เพิ่มเติม

(b) ดูแลโดยสำนักคอมพิวเตอร์ หรือ ไม่ทราบ

ติดต่อสำนักคอมพิวเตอร์ ที่ช่องทางชื่อ “ICT Service Desk For Staff” บน Microsoft Teams และค้นหา Channel ชื่อ “Websites” เพื่อดำเนินการตรวจสอบเพิ่มเติม

เว็บไซต์ใช้แบบ B (http://bbb.aaa.kmutt.ac.th)

เนื่องจากระบบชื่อโดเมน (DNS) ในแบบ B (http://bbb.aaa.kmutt.ac.th) ไม่สามารถใช้ SSL Certifcate ร่วมกับส่วนกลางมหาวิทยาลัยที่สำนักคอมพิวเตอร์ให้บริการได้ และ SSL Certifcate มีค่าใช้จ่ายรายปี หน่วยงานจึงต้องดำเนินการจัดหาหรือจัดซื้อเพิ่มเติมเอง

หมายเหตุ SSL Certificate มีค่าใช้จ่ายรายปี ประมาณ 1,600 บาท อ้างอิงจากที่เลือกสำนักคอมพิวเตอร์ใช้งาน

ดูแลเครื่องแม่ข่าย (Server) และระบบชื่อโดเมน (DNS) โดยหน่วยงาน/ตนเอง หรือไม่ ?

(a) ดูแลโดยหน่วยงาน/ตนเอง

ผู้ดูแลจัดหาหรือจัดซื้อ SSL Certificate และดำเนินการติดตั้ง SSL Certificate ตามคำแนะนำของผู้ให้บริการ

(b) ดูแลโดยสำนักคอมพิวเตอร์ หรือ ไม่ทราบ

ผู้ดูแลจัดหาหรือจัดซื้อ SSL Certificate และติดต่อสำนักคอมพิวเตอร์ ที่ช่องทางชื่อ “ICT Service Desk For Staff” บน Microsoft Teams และค้นหา Channel ชื่อ “Websites” เพื่อดำเนินการตรวจสอบเพิ่มเติม

หากสามารถเปลี่ยนมาใช้ระบบชื่อโดเมน (DNS) เป็นแบบ A (https://aaa.kmutt.ac.th) จะสามารถใช้ SSL Certifcate ร่วมกับส่วนกลางมหาวิทยาลัยได้โดยไม่มีค่าใช้จ่าย สำหรับการดำเนินการขอเปลี่ยนระบบชื่อโดเมน (DNS) โปรดติดต่อสำนักคอมพิวเตอร์ ที่ช่องทางชื่อ “ICT Service Desk For Staff” บน Microsoft Teams และค้นหา Channel ชื่อ “Websites”

กรณีดูแลระบบชื่อโดเมน (DNS) โดยหน่วยงาน/ตนเอง อาจไม่สามารถดำเนินการเปลี่ยนระบบชื่อโดเมน (DNS) เป็นแบบ A (https://aaa.kmutt.ac.th) ได้ โปรดประเมินผลกระทบที่อาจเกิดขึ้นกับระบบอื่นๆ ที่เกี่ยวข้องก่อน

ขั้นตอนที่ 2 ตรวจสอบ/ทดสอบเว็บไซต์รองรับ HTTPS หรือยัง ?

1. เปิดโปรแกรมเว็บบราวเซอร์ พิมพ์ https://<ชื่อโดเมน>.kmutt.ac.th ในช่อง URL Address

2. ตรวจสอบรูปไอคอนกุญแจ Lock หรือคำว่า “Secure” ด้านหน้า ชื่อโดเมน ในช่อง URL Address ในทุกหน้าเว็บเพจ

3. หากรูปไอคอนกุญแจ Lock หรือคำว่า “Secure” ไม่ขึ้นแสดง หรือ ไม่สามารถใช้งานได้ หรือ ใช้งานได้ไม่เหมือนเดิม โปรดตรวจสอบ URL Address ของไฟล์ต่าง ๆ อาจยังอ้างอิงระบบชื่อโดเมน (DNS) เดิมหรือไม่ เช่น http://www.<ชื่อโดเมน>.kmutt.ac.th หรือ http://<ชื่อโดเมน>.kmutt.ac.th

4. ดำเนินการแก้ไขตามความเหมาะสม จนแน่ใจว่าเว็บไซต์สามารถใช้งานได้ปกติแล้ว (โปรดอ่านขั้นตอนการปรับแก้ไขเว็บไซต์ในแต่ละระบบที่ใช้ หน้าที่ 8)

สำหรับผู้ดูแลที่ได้รับคำแนะนำจากสำนักคอมพิวเตอร์ให้ทำการตั้งค่าเครื่องคอมพิวเตอร์ของตัวเองเพื่อทดสอบเว็บไซต์ เมื่อเลือกใช้วิธี Reverse proxy ก่อนเริ่มขั้นตอนตรวจสอบ/ทดสอบด้านบน โปรดอ่านขั้นตอนเพิ่มเติม หน้าที่ 10

ขั้นตอนที่ 3 การปรับแก้ไขเว็บไซต์ในแต่ละระบบที่ใช้

Static website / Website generators / Framework

ตรวจสอบลิงก์ในไฟล์ต่าง ๆ และดำเนินการแก้ไขเป็นชื่อโดเมน (DNS) ใหม่ให้ถูกต้อง

Wordpress

จัดเตรียมก่อนดำเนินการ

1. สิทธิในการเข้าไปแก้ไข wp-config ในเครื่องแม่ข่าย (Server)
2. สิทธิในการเข้าถึง Database ของ WP
3. ดำเนินการ Backup file และ Database ไว้

ดำเนินการแก้ไข

1. แก้ไขไฟล์ wp-config.php บนเครื่อง Server โดยเพิ่มบรรทัดเหล่านี้ ไว้ด้านบน

```
define('WP_HOME','https://<ชื่อโดเมน>.kmutt.ac.th');
define('WP_SITEURL','https://<ชื่อโดเมน>.kmutt.ac.th');
$_SERVER['HTTPS'] = 'on';
$_SERVER['SERVER_PORT'] = 443;
```

2. Login เข้าใช้ Wordpress Admin และทำการติดตั้ง Search and Replace plugins (https://wordpress.org/plugins/search-and-replace/)

3. ใช้ Plugin เพื่อค้นหา และแก้ไขชื่อโดเมน (DNS) ให้ถูกต้องด้วยความระมัดระวัง ตัวอย่างข้อมูลที่ต้องแก้ไขให้ถูกต้อง เช่น

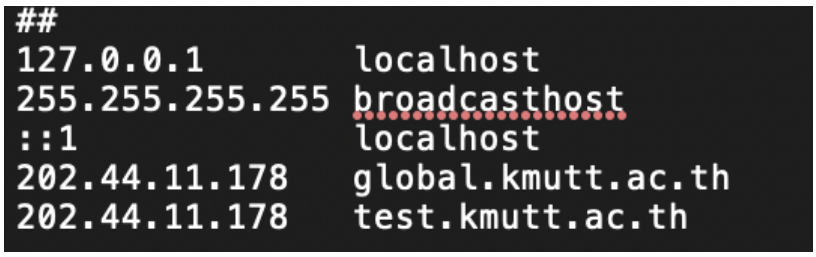
ชื่อโดเมนเก่า	เปลี่ยนเป็นชื่อโดเมนใหม่
http://www.aaa.kmutt.ac.th	https://aaa.kmutt.ac.th
http://aaa.kmutt.ac.th	https://aaa.kmutt.ac.th
www.aaa.kmutt.ac.th	aaa.kmutt.ac.th

การเริ่มแก้ไขบนเครื่องแม่ข่าย (Server) ที่ใช้งานจริง อาจทำให้เว็บไซต์ไม่สามารถใช้งานได้ชั่วขณะในเวลาสั้น ๆ จนกว่าผู้ดูแลจะดำเนินการเสร็จสิ้น

ขั้นตอนเพิ่มเติม

การตั้งค่าเครื่องคอมพิวเตอร์ของตัวเองเพื่อทดสอบ เมื่อเลือกใช้วิธี Reverse proxy โปรดดำเนินการขั้นตอนนี้

1. ตั้งค่าไฟล์ host โดยเพิ่ม “202.44.11.178 <ชื่อโดเมน>.kmutt.ac.th” เป็นหนึ่งบรรทัด และทำการบันทึก (อ่านเพิ่มเติมการตั้งค่าที่ https://en.wikipedia.org/wiki/Hosts_(file)) เช่น



2. ตรวจสอบว่าเว็บไซต์สามารถใช้งานได้เป็นปกติ ตามขั้นตอนในหน้าที่ 6

3. ติดต่อสำนักคอมพิวเตอร์ เพื่อดำเนินการย้ายหรือเปลี่ยนระบบชื่อโดเมน (DNS)

4. ลบข้อมูลที่เพิ่ม จากข้อ 1 ออกจากไฟล์ host

5. สำนักคอมพิวเตอร์ติดต่อกลับเพื่อทดสอบอีกครั้ง และเริ่มใช้งานจริง

การอัพเดทระบบชื่อโดเมน (DNS) อาจใช้เวลาภายในไม่กี่ชั่วโมง จนถึง 48 ชั่วโมง จนกว่าการอัพเดทจะเสร็จสิ้น อาจทำให้เว็บไซต์ไม่สามารถใช้งานจากบางสถานที่ได้ชั่วขณะ