

13 Click&Go with Technology: Encryption and Password Security in Medical School Examinations



ดร.ศุภกิจ บุญเอกพัฒน์
ศูนย์ความเป็นเลิศด้านการศึกษาวิทยาศาสตร์สุขภาพ
คณะแพทยศาสตร์ศิริราชพยาบาล

พบกันอีกครั้งกับ Click&Go with Technology วารสารฉบับนี้ กลับมาเป็นรูปแบบเดิมที่ทุกท่านคุ้นเคย เกี่ยวกับการนำเสนอ technology หรือ application ที่น่าสนใจมาให้ทุกท่านได้ศึกษา คราวนี้เป็นเรื่องวิธีการรักษาความปลอดภัยของ file ข้อสอบ เพื่อป้องกันการรั่วไหลของ file ข้อสอบ ซึ่งถือเป็นเรื่องที่สำคัญอย่างมาก แต่บางท่านอาจจะยังไม่ทราบถึงวิธีการปฏิบัติที่แท้จริง ผู้เขียนหวังว่าผู้อ่านทุกท่านที่ได้อ่านบทความฉบับนี้ จะนำแนวคิด วิธีการที่ได้ไปประยุกต์ใช้ได้อย่างเหมาะสมในบริบทการทำงาน และการเรียนการสอนครับ

ในยุค digital ที่ข้อมูลสามารถถูกเข้าถึง แก้ไข หรือรั่วไหลได้อย่างรวดเร็ว ความมั่นคงของข้อมูลข้อสอบในระดับอุดมศึกษา โดยเฉพาะในโรงเรียนแพทย์ที่มีลักษณะของการประเมินผลที่เข้มงวดและมีความสำคัญสูง จึงเป็นประเด็นที่ไม่อาจมองข้าม การรั่วไหลของข้อสอบ ไม่เพียงส่งผลต่อความยุติธรรมในการสอบ แต่ยังบั่นทอนความน่าเชื่อถือของระบบการศึกษา กระทบต่อชื่อเสียงของสถาบัน และที่สำคัญที่สุดคือ ส่งผลต่อคุณภาพของผู้สำเร็จการศึกษา

บทความนี้มีวัตถุประสงค์เพื่อให้คณาจารย์และบุคลากรในโรงเรียนแพทย์สามารถป้องกันข้อสอบของตนเองจากการถูกเข้าถึงโดยมิชอบ ด้วยแนวทางและเครื่องมือที่สามารถ นำไปใช้ได้จริงในบริบทของการทำงานประจำวัน โดยเนื้อหาจะครอบคลุมใน 3 หัวข้อสำคัญ ได้แก่

1. การเข้ารหัส file (File Encryption)
2. การแบ่งปันหรือส่งต่อ file อย่างปลอดภัย (Secure File Sharing)
3. การจัดการรหัสผ่านอย่างมีวินัย (Password Management)

การเข้ารหัส file (File Encryption)

แนวคิดของการเข้ารหัส file (File Encryption) คือกระบวนการแปลงข้อมูลให้กลายเป็นรูปแบบที่อ่านไม่ได้ เว้นแต่จะมีรหัสผ่านที่ถูกต้องในการถอดรหัส เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึง file สามารถเปิดดู หรือแก้ไขเนื้อหาภายในได้ สำหรับการจัดสอบในโรงเรียนแพทย์ การเข้ารหัส file ข้อสอบ PDF ถือเป็นมาตรการพื้นฐานที่จำเป็นอย่างยิ่ง โดยเฉพาะในสถานการณ์ที่ต้องส่งต่อ file ระหว่างคณาจารย์ ผู้ประสานงาน หรือเจ้าหน้าที่ด้านการศึกษา การตั้งรหัสผ่านให้กับ file สามารถช่วยป้องกันไม่ให้ file ถูกเปิดโดยบุคคลอื่น แม้ว่าจะมีการเข้าถึง file จาก e-mail หรือ cloud โดยไม่ได้ตั้งใจ

ตัวอย่างการใช้งานการเข้ารหัส file ในบริบทของการสอบ เช่น เมื่อคณาจารย์จัดทำข้อสอบเสร็จในรูปแบบ file PDF ก่อนจะส่งต่อไปยังเจ้าหน้าที่หรือผู้ประสานงาน ควรดำเนินการเข้ารหัส file โดยตั้งรหัสผ่านเพื่อป้องกันไม่ให้ผู้อื่นสามารถเปิดดูเนื้อหาได้โดยไม่ได้รับอนุญาต โดยผู้ที่ได้รับ file จะต้องทราบรหัสผ่านจึงจะสามารถเปิดใช้งาน file ข้อสอบได้ ทั้งนี้ เพื่อความปลอดภัย รหัสผ่านควรส่งผ่านช่องทางที่ปลอดภัยและแยกจากช่องทางการส่ง file เช่น ส่งข้อความส่วนตัวทาง Line แทนการแนบรหัสผ่านไว้ใน e-mail ฉบับเดียวกับ file

ในโอกาสนี้ผู้เขียนจึงอยากนำเสนอเครื่องมือการเข้ารหัส file คือ website [ilovepdf](https://www.ilovepdf.com/protect-pdf) ซึ่งเป็นเครื่องมือที่ใช้งานได้ง่าย ไม่เสียค่าใช้จ่าย ไม่ต้องติดตั้ง program และใช้ได้จากทุกเครื่องมือที่เชื่อมต่อ internet โดยมีขั้นตอนการใช้งานดังนี้

1. เข้าเว็บไซต์ <https://www.ilovepdf.com/protect-pdf>
2. เลือก “Select PDF file” และเลือก file ที่ต้องการเข้ารหัส

CONVERT PDF ▾

ALL PDF TOOLS ▾

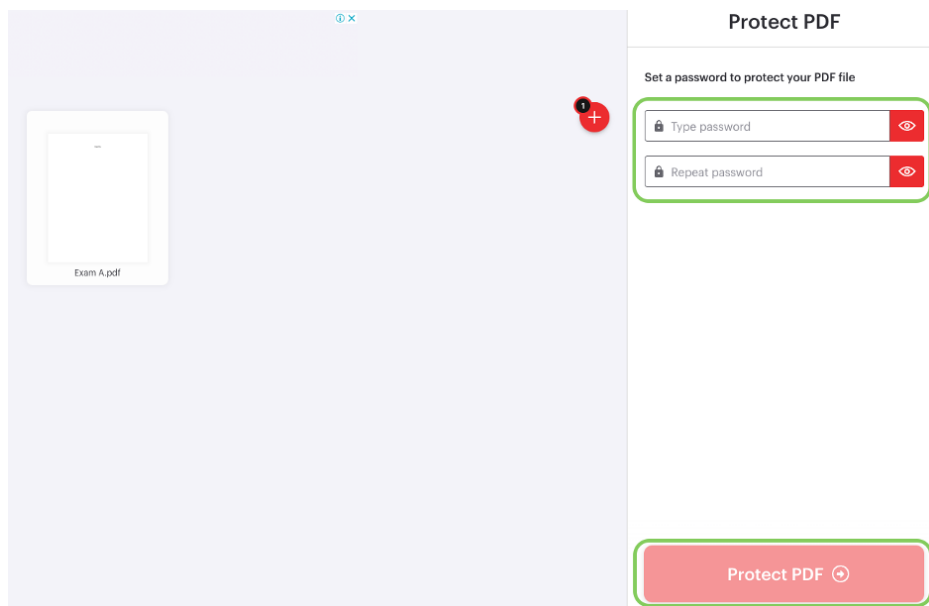
Protect PDF file

Encrypt your PDF with a password to keep sensitive data confidential.

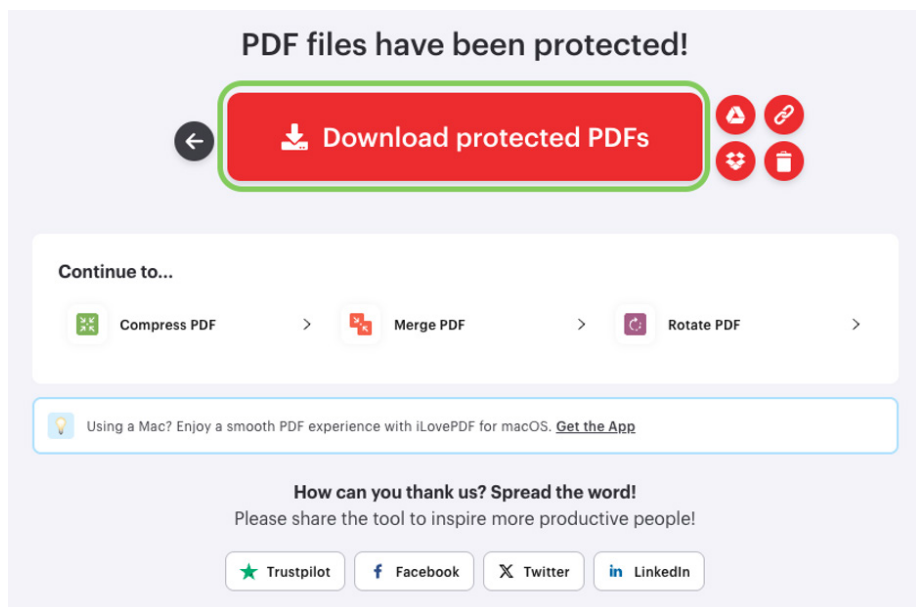
Select PDF file

or drop PDF here

3. ตั้งรหัสและยืนยันรหัส จากนั้นกดปุ่ม “Protect PDF”



4. กดปุ่ม “Download Protected PDFs” เพื่อ download file ที่เข้ารหัสแล้ว



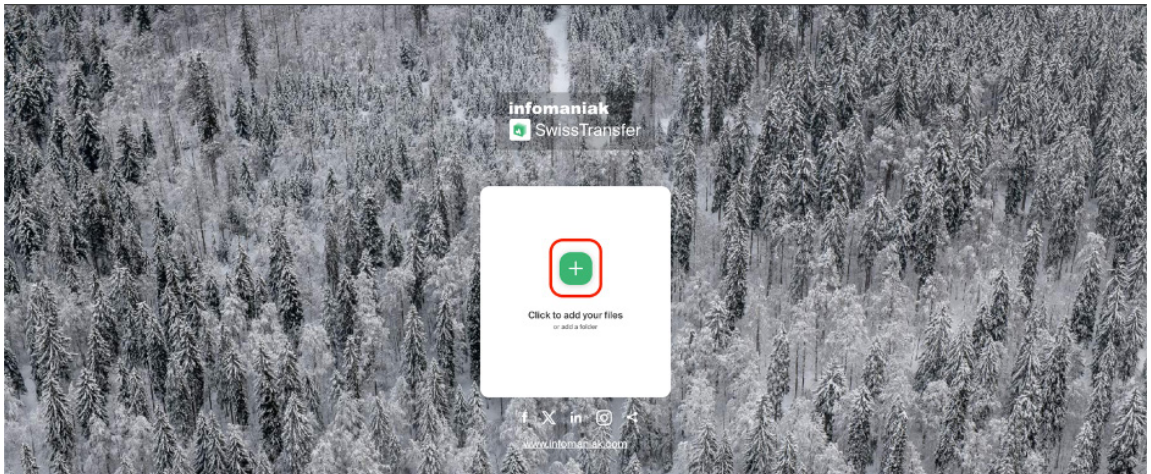
การแบ่งปัน file อย่างปลอดภัย (Secure File Sharing)

การแบ่งปัน file อย่างปลอดภัย (Secure File Sharing) หมายถึงกระบวนการส่งต่อข้อมูลหรือ file ผ่านช่องทางที่มีการป้องกันความปลอดภัย เช่น การเข้ารหัส file การกำหนดสิทธิ์เข้าถึง และการควบคุมระยะเวลาในการเปิดใช้งาน file เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ในบริบทของการบริหารจัดการข้อสอบในโรงเรียนแพทย์ การเลือกใช้ระบบแบ่งปัน file ที่ปลอดภัยมีความสำคัญ

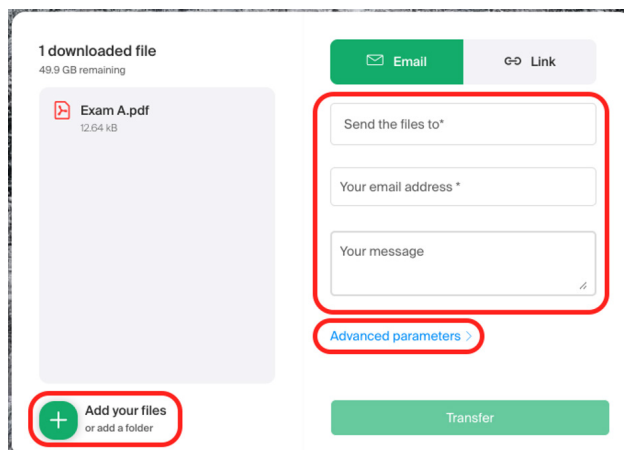
อย่างยิ่ง เนื่องจากการส่ง file ผ่าน e-mail โดยตรงมีความเสี่ยงต่อการรั่วไหลของข้อมูล e-mail ทั่วไป มักไม่ได้มีระบบการเข้ารหัสแบบครบวงจรสำหรับ file แนบ (end-to-end encryption) และหากบัญชีผู้ใช้ e-mail ถูกโจมตี file ที่แนบไว้ก็สามารถถูกเข้าถึงได้โดยง่าย นอกจากนี้ file แนบใน e-mail ยังขาดคุณสมบัติการควบคุมสิทธิ์การเข้าถึง เช่น การตั้งวันหมดอายุของ file หรือการจำกัดจำนวนครั้งในการ download ซึ่งเป็นมาตรการสำคัญในการป้องกันการเผยแพร่ข้อมูลข้อสอบอย่างไม่เหมาะสม

ในบทความนี้ ผู้เขียนขอแนะนำเสนอแนวทางการใช้บริการ Secure File Sharing ผ่าน website SwissTransfer ซึ่งช่วยให้ผู้ส่งสามารถเพิ่มระดับการป้องกันข้อมูลได้หลายชั้น ทั้งการกำหนดรหัสผ่านในการเปิด file การตั้งค่ารระยะเวลาในการ download และการจำกัดจำนวนการเข้าถึง นอกจากนี้จะช่วยลดความเสี่ยงจากการรั่วไหลของข้อมูลแล้ว ยังช่วยเสริมสร้างมาตรฐานการจัดการข้อมูลที่ปลอดภัยในกระบวนการสอบได้อย่างเป็นระบบ

1. เข้าเว็บไซต์ <https://www.swisstransfer.com/>
2. กด icon เครื่องหมาย “+” เพื่อเพิ่ม file ที่ต้องการ share



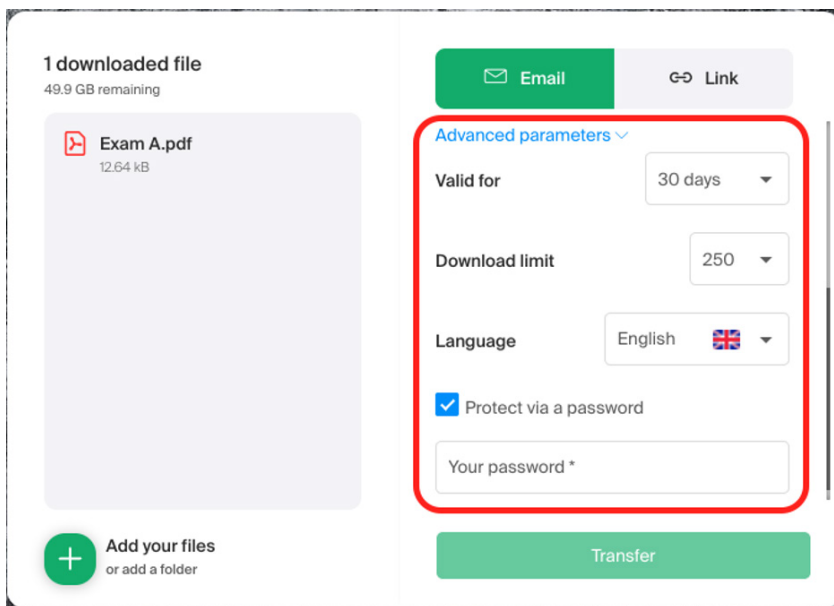
3. หากเลือกส่ง file ผ่าน e-mail ให้ระบุ e-mail ผู้รับและ e-mail ผู้ส่งให้ครบถ้วน หากต้องการส่งหลาย file พร้อมกัน สามารถกด icon “+” เพื่อเพิ่ม file เพิ่มเติมได้



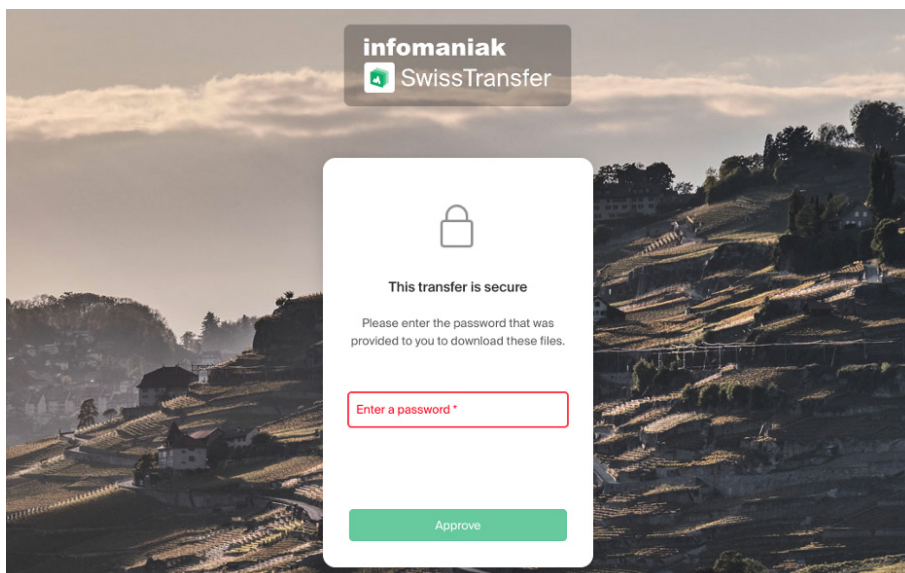
4. ผู้เขียนแนะนำให้เลือกใช้ตัวเลือก Advanced parameters เพื่อเพิ่มความปลอดภัยในการ share file โดย click ที่ menu dropdown Advanced parameters จากนั้นสามารถกำหนด

- ระยะเวลาที่ file จะสามารถ download ได้ (Valid for)
- จำนวนครั้งสูงสุดที่สามารถ download file ได้ (Download limit)
- การตั้งรหัสผ่านสำหรับป้องกันการเข้าถึง file (เลือก ✓ ที่ Protect via a password)

เมื่อกำหนดค่าต่าง ๆ เรียบร้อยแล้ว ให้กดปุ่ม Transfer



5. ผู้รับจะได้รับ e-mail จาก SwissTransfer แจ้งว่ามี file ถูกส่งมาให้ เมื่อ click ที่ link download ผู้รับจะถูกนำไปยัง website SwissTransfer และต้องกรอกรหัสผ่านที่ผู้ส่งกำหนดไว้ จึงจะสามารถ download file ทั้งหมดได้



การจัดการรหัสผ่าน (Password Management)

การจัดการรหัสผ่าน (Password Management) คือแนวทางในการสร้าง เก็บรักษา และใช้รหัสผ่านอย่างปลอดภัย โดยมีกรรมถึงการใช้เครื่องมือช่วยจำรหัสผ่าน (password manager) เพื่อหลีกเลี่ยงการใช้รหัสผ่านซ้ำ หรือการตั้งรหัสผ่านที่คาดเดาได้ง่าย ขณะที่ วินัยด้านรหัสผ่าน (Password Discipline) หมายถึงพฤติกรรมของผู้ใช้งานที่ส่งผลต่อความปลอดภัยของข้อมูล เช่น การเปลี่ยนรหัสผ่านเป็นระยะ การไม่บันทึกรหัสผ่านไว้ในที่เปิดเผย และการไม่ส่งรหัสผ่านผ่านช่องทางที่ไม่ปลอดภัย

สำหรับคณาจารย์และบุคลากรในโรงเรียนแพทย์ที่ต้องรับผิดชอบข้อมูลสำคัญ เช่น ข้อสอบ file ประเมินผล หรือข้อมูลนักศึกษา การมีระบบจัดการรหัสผ่านที่ดีถือเป็นมาตรการพื้นฐานในการรักษาความปลอดภัยของข้อมูล การใช้รหัสผ่านที่คาดเดายากแต่ไม่ต้องจดจำเองทุกตัว และสามารถแชร์ได้อย่างปลอดภัยกับทีมที่เกี่ยวข้อง ช่วยลดความเสี่ยงจากการรั่วไหลของข้อมูล โดยเฉพาะในสถานการณ์ที่ต้องใช้งานระบบ e-mail platform เก็บ file ระบบข้อสอบ online หรือเครื่องมือสื่อสารต่าง ๆ หลายระบบพร้อมกัน แม้ว่าปัจจุบัน browser หลายตัว เช่น Chrome, Safari หรือ Microsoft Edge จะมีระบบบันทึกรหัสผ่านในตัว แต่เครื่องมือเหล่านี้มักไม่สามารถจัดการรหัสผ่านข้ามอุปกรณ์หรือ share กับผู้อื่นได้อย่างปลอดภัย และไม่มีระบบควบคุมความปลอดภัยที่เข้มงวดเท่ากับ software จัดการรหัสผ่านโดยเฉพาะ

ดังนั้นผู้เขียนขอแนะนำให้พิจารณาใช้ platform จัดการรหัสผ่าน ที่มีความน่าเชื่อถือ โดยในตารางด้านล่างเป็นการเปรียบเทียบ software 4 รายการที่ได้รับความนิยม

เครื่องมือ	ข้อดี	ข้อเสีย
Bitwarden (ฟรี/มีค่าใช้จ่าย)	• มี version ฟรีใช้งานได้ครบพอสมควร • รองรับหลายอุปกรณ์ • มีระบบ share รหัสผ่านผ่านองค์กร (Team/Org vault) • Open-source ปลอดภัย ตรวจสอบได้	• หน้าตาอาจจะไม่สวยหรือใช้งานเท่าคู่แข่ง • การตั้งค่าบางส่วนอาจซับซ้อนสำหรับมือใหม่
1Password (มีค่าใช้จ่าย)	• User interface ใช้งานง่าย • รองรับ features ที่หลากหลาย • Share รหัสผ่านในทีมได้อย่างปลอดภัย	• ไม่มี version ฟรี • ราคาค่อนข้างสูงเมื่อเทียบกับคู่แข่ง
KeePassXC (ฟรี, offline)	• ฟรี 100% และไม่ต้องเชื่อมต่อ internet • เหมาะสำหรับผู้ที่ไม่ไว้ใจ cloud • เก็บข้อมูลทั้งหมดไว้ในเครื่อง (local vault)	• ต้องจัดการ file ฐานข้อมูลเอง • ไม่สามารถ share รหัสผ่านกับผู้อื่นได้สะดวก • ไม่มี mobile app อย่างเป็นทางการ
NordPass (ฟรี/มีค่าใช้จ่าย)	• มี version ฟรีใช้งานง่าย • User interface ทันสมัย • มี features ตรวจสอบรหัสผ่านรั่วไหล	• Version ฟรีจำกัดการใช้งานข้ามอุปกรณ์ • Features ข้นสูงน้อย

สำหรับคณาจารย์ที่ทำงานร่วมกับผู้อื่นในการจัดการข้อสอบ ผู้เขียนแนะนำให้เลือกใช้ Bitwarden (<https://bitwarden.com/>) หรือ 1Password (<https://1password.com/>) เพื่อสร้าง vault กลางสำหรับ share รหัสผ่านระบบต่าง ๆ (เช่น file ที่ถูกเข้ารหัส, ระบบ learning management system, หรือระบบข้อสอบ online) อย่างปลอดภัย โดยควรกำหนดสิทธิ์การเข้าถึงให้เหมาะสม และเปลี่ยนรหัสผ่านเป็นระยะ