อันตรายที่ต้องระวังในการค้าขายระหว่างประเทศ

จารุพัฒน์ พานิชยิ่ง
ผู้อำนวยการฝ่ายรับประกันการส่งออก
ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย (EXIM BANK)
jarupatp@exim.go.th

จากฉบับที่แล้ว ผมพูดถึง “การส่งออกด้วย Letter of Credit” แต่เนื่องจากได้รับทราบข่าวว่า ในช่วงปีนี้ผู้ส่งออกไทยหลายรายโดน Hack E-mail โกงค่าสินค้า ผมจึงขอพูดถึงเรื่อง E-mail และวิธีป้องกันความเสี่ยงในการใช้ E-mail ติดต่อค้าขายระหว่างประเทศในฉบับนี้นะครับ

Electronic mail **หรือ** “E-mail” เป็นการติดต่อแลกเปลี่ยนข่าวสารระหว่างเครื่องคอมพิวเตอร์ โดยผ่านระบบโทรคมนาคม โดย E-mail เป็นสิ่งที่ใช้กันอย่างกว้างขวางและเป็นสัดส่วนใหญ่ของ Traffic บนอินเทอร์เน็ต รวมทั้งเป็นที่ยอมรับกันว่า E-mail เป็นส่วนสำคัญที่ขาดไม่ได้สำหรับชีวิตประจำวันของนักธุรกิจในยุคไซเบอร์นี้ ทั้งในการเรื่องติดต่อสื่อสารทางธุรกิจการค้าและการติดต่อส่วนตัว ซึ่งประโยชน์ของ E-mail มีอยู่มากมาย ทั้งช่วยอำนวยความสะดวกให้สามารถติดต่อสื่อสารระหว่างกันได้ในทุกสถานที่ ประหยัดค่าใช้จ่าย และเป็นช่องทางการสื่อสารที่รวดเร็ว ทำให้ E-mail เป็นปัจจัยสำคัญในการสร้างประโยชน์ทางธุรกิจให้แก่ผู้ใช้ แต่ในอีกด้านหนึ่ง E-mail อาจเป็น *“**อันตราย**”* ใกล้ตัวที่ผู้ใช้ไม่ทันได้ระวังตัว ด้วยความเคยชินและความสะดวกของการใช้ E-mail นี้เอง

ปัจจุบันการติดต่อสื่อสารในธุรกิจการค้าระหว่างประเทศมักจะใช้ E-mail เป็นสื่อกลางในการเจรจาตกลงทางธุรกิจ การสอบถามความต้องการต่างๆ การสั่งซื้อสินค้า การยืนยันการจัดส่งสินค้า จนกระทั่งการยืนยันการชำระเงินค่าสินค้า การใช้ E-mail ในการสื่อสารธุรกิจตั้งแต่เริ่มต้นจนจบกระบวนการการค้าอาจเป็นช่องทางให้บุคคลกลุ่มหนึ่งสามารถใช้อินเทอร์เน็ตเป็นเครื่องมือในการทำมาหากินในทางทุจริต โดยอาศัยเทคนิคความสามารถทางคอมพิวเตอร์และกลเม็ดหลอกลวงผู้อื่น พัฒนาตัวเป็น **“แฮกเกอร์”** มาล้วงความลับข้อมูลทางธุรกิจและเปลี่ยนแปลงข้อมูลที่สื่อสารกันระหว่างคู่ค้า เพื่อแสวงหาผลประโยชน์ (เงิน) เข้าสู่ตนเอง เช่น การนำข้อมูลทางธุรกิจไปขายให้คู่แข่ง การขโมยสินค้า หรือการหลอกให้โอนเงินไปยังบัญชีของวายร้ายเหล่านี้ เป็นต้น

ตั้งแต่ต้นปีที่ผ่านมา มีลูกค้าและผู้นำเข้าส่งออกหลายรายเข้ามาขอคำแนะนำจากธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทยหรือ EXIM BANK ให้ช่วยตรวจสอบเนื่องจากสงสัยว่าทำไมผู้ซื้อไม่ชำระเงินค่าสินค้าและถูก Hack Email หรือไม่ ซึ่งคำตอบส่วนใหญ่คือ “ถูกต้อง” โดยแฮกเกอร์เหล่านี้เมื่อสามารถเข้ามาใช้ E-mail ของผู้ส่งออกได้แล้ว ก็จะติดต่อผู้นำเข้าในต่างประเทศโดยผู้ส่งออกตัวจริงไม่รู้และคาดไม่ถึงเพราะไม่สามารถใช้ E-mail นั้นได้อีกต่อไป และหลอกให้ผู้นำเข้าในต่างประเทศโอนเงินค่าสินค้าเข้าบัญชีธนาคารเลขที่ใหม่ที่อาจเปิดในประเทศไทยหรือเปิดในต่างประเทศแทนบัญชีเดิมที่เคยทำธุรกรรมกันอยู่โดยอ้างเหตุผลร้อยแปดพันเก้า โดยวายร้ายเหล่านี้จะติดตามข้อมูลข่าวสารของคู่ค้ามาระยะหนึ่งจนรู้พฤติกรรมของคู่ค้าและเมื่อสบโอกาสเหมาะก็จะ Hack Email ของผู้ส่งออกซึ่งส่วนใหญ่จะเกิดกับคู่ค้าที่ติดต่อธุรกิจกันมานานพอสมควรและมีพฤติกรรมและข้อความในการติดต่อทาง E-mail ในแต่ละธุรกรรมซ้ำๆ กัน

ตัวอย่างที่เกิดขึ้นล่าสุด คือ ผู้ส่งออกสินค้าพลาสติกทำการค้ากับผู้นำเข้าในยุโรปมานานหลายปี โดยใช้ E-mail ของบริษัทในการติดต่อสื่อสารเป็นประจำ และการค้าขายเป็นไปด้วยความราบรื่นมาโดยตลอด ไม่เคยเกิดปัญหาหรืออุปสรรคใดๆ เลย แต่เมื่อเดือนที่แล้ว บริษัทผู้นำเข้าในยุโรปได้รับ E-mail ซึ่งมีรูปแบบและชื่อผู้ส่งเป็นคนเดียวกันกับพนักงานของผู้ส่งออกที่เคยติดต่อกันเป็นประจำ แจ้งให้ผู้นำเข้าโอนเงินค่าสินค้าตามงวดที่ต้องชำระเข้าเลขที่บัญชีธนาคารใหม่ในประเทศอื่นโดยอ้างว่า บริษัทผู้ส่งออกอยู่ระหว่างถูกหน่วยงานราชการตรวจสอบบัญชี และไม่สะดวกที่จะตรวจสอบเงินที่โอนเข้ามาเพิ่มในบัญชีเก่าได้ จึงขอใช้บัญชีใหม่ในการรับโอนเงินแทน ซึ่งบริษัทผู้นำเข้าก็ได้ขอให้ผู้ส่งออกยืนยันการเปลี่ยนแปลงดังกล่าวผ่าน E-mail อีกครั้ง ซึ่งในทางปฏิบัติแล้วเมื่อ E-mail ชื่อนั้นโดน Hack แล้ว ผู้นำเข้าก็ได้รับคำยืนยันจากวายร้ายนั่นเอง จึงได้ดำเนินการโอนเงินเข้าบัญชีใหม่ดังกล่าว เมื่อเวลาผ่านไประยะหนึ่งเมื่อผู้ส่งออกไทยยังไม่ได้รับเงินค่าสินค้าและไม่ได้รับการติดต่อทาง E-mail เลย จึงได้โทรศัพท์สอบถามไปยังผู้นำเข้าทั้งสองฝ่ายจึงได้ทราบว่ามีบุคคลที่สาม Hack E-mail และปลอมแปลงข้อความของผู้ส่งออกไทย เพื่อใช้สนทนาลวงหลอกให้บริษัทผู้นำเข้าโอนเงินเข้าในบัญชีของแฮกเกอร์ และเมื่อตรวจสอบกลับไปยังธนาคารนั้นก็ทราบว่าได้ปิดบัญชีไปแล้ว

หลายคนคงคิดว่าเหตุการณ์ลักษณะนี้ไม่น่าจะเกิดขึ้นได้ง่าย คิดว่าเป็นไปไม่ได้ที่จะมีใครมาแอบใช้ E-mail ของเราไปสนทนากับคนอื่น ในเมื่อการใช้ E-mail ของบริษัทมีความเป็นส่วนตัวสูง (Privacy) และเป็นการใช้งานของพนักงานบริษัทเราเอง

ดังนั้น ในการติดต่อธุรกิจการค้าทาง E-mail หากได้รับการติดต่อขอเปลี่ยนแปลงข้อมูลใดๆ โดยเฉพาะอย่างยิ่งการดำเนินการที่สำคัญ เช่น การส่งมอบสินค้า การชำระเงิน ควรมีการโทรศัพท์ตรวจสอบกับคู่ค้าเพื่อความชัดเจนทุกครั้งก่อนทำการโอนชำระเงินต่าง ๆ อย่างน้อยก็เป็นการเน้นย้ำว่ามีการเปลี่ยนแปลงจริงตามที่ได้รับแจ้ง และผู้ใช้ควรมีการเปลี่ยน Password อย่างสม่ำเสมอ เพื่อความปลอดภัยในการทำธุรกรรมต่างๆ รวมทั้ง เมื่อเกิดปัญหาแล้วผู้ส่งออกไม่ควรยอมรับกับผู้ซื้อว่ามีผู้ Hack E-mail ของตน ควรรีบแจ้งความกับตำรวจเพื่อดำเนินการร่วมกับผู้นำเข้าและเพื่อรักษาสถานะหนี้ที่ผู้นำเข้าต่างประเทศต้องชำระค่าสินค้าให้คงอยู่ รวมทั้งควรรีบติดต่อผู้ให้บริการอินเทอร์เน็ตหรือ Domain ของบริษัท เพื่อหาวิธีป้องกันในอนาคต

สิ่งสำคัญในเรื่องนี้คงจะอยู่ที่**การป้องกัน** ผมจึงรวบรวมคำแนะนำเรื่องการป้องกันการโดน Hack E-mail ในเบื้องต้นได้ดังนี้

- ควรตั้งรหัสผ่านให้ยากต่อการคาดเดา เช่น หากใช้เบอร์โทร อาจมีตัวอักษรปิดหัวปิดท้าย เช่น e0812345678w เป็นต้น
- ควรเปลี่ยนรหัสผ่านเป็นระยะๆ ไม่ควรใช้ Password เดียวตลอด เพราะมีความเสี่ยงสูงที่จะถูก Hack ข้อมูล
- การเช็ก E-mail ควรมองตำแหน่ง URL ให้ดี หากมีความผิดปกติ ไม่ควรใส่รหัสผ่าน
- ไม่ควรใช้ E-mail ของบริษัทในการลงทะเบียนเว็ปไซต์สาธารณะและไม่น่าไว้วางใจ
- หากเป็น E-mail ในเรื่องที่สำคัญ ควรแยกออกจาก E-mail ที่ใช้สื่อสารเป็นประจำ จะทำให้สามารถลดความเสี่ยงไปได้อีกระดับหนึ่ง

และสุดท้ายที่สำคัญที่สุด คือ **อย่าประมาท** เพราะความประมาทอาจส่งผลให้ธุรกิจเกิดความเสียหายได้เสมอ