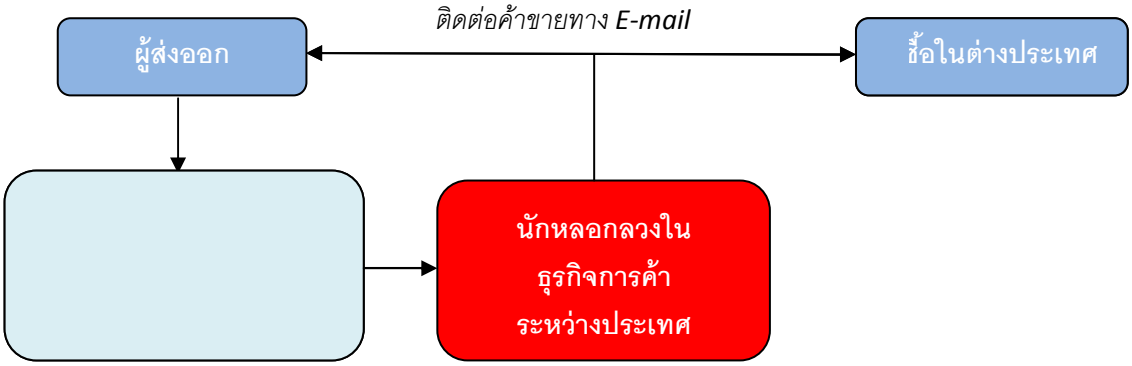
SMEs กับกลโกงของคู่ค้าในต่างประเทศ (2)

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



"**อยากรู้อะไร อยากหาอะไร หาได้จากในอินเทอร์เน็ต**" เป็นประโยคที่เป็นความจริงสำหรับทุกคนในปัจจุบัน และเป็นที่ยอมรับอย่างชัดเจนว่า "**อินเทอร์เน็ต**" เป็นส่วนสำคัญที่ขาดไม่ได้สำหรับชีวิตประจำวันของนักธุรกิจในยุคไซเบอร์นี้ นักธุรกิจรุ่นใหม่ใช้อินเทอร์เน็ตสำหรับค้นหาข้อมูล ติดต่อสื่อสารในทางธุรกิจการค้า หรือแม้แต่ใช้คลิกเดียวเพื่อชอปปิงซื้อสินค้าส่วนตัว ด้วยความเคยชินจึงอาจลืมไปว่า แม้ว่าอินเทอร์เน็ตจะช่วยอำนวยความสะดวกและสร้างประโยชน์ทางธุรกิจแก่ผู้ใช้ แต่อาจเป็น "**ภัยร้าย**" ที่แทรกซึมตามมาโดยที่ผู้ใช้ไม่ทันได้ระวังตัว

ปัจจุบันการติดต่อทำธุรกิจการค้าผ่านทางอินเทอร์เน็ตเป็นที่นิยมแพร่หลายมาก โดยเฉพาะอย่างยิ่งการทำการค้าระหว่างประเทศ ทั้งที่คู่ค้าอาจไม่รู้จักหน้าตากันมาก่อน หรืออาจจะเป็นคู่ค้าที่มีความสนิทสนมและไว้เนื้อเชื่อใจกันเนื่องจากติดต่อกันมาเป็นเวลานาน ซึ่งในการติดต่อสื่อสารมักจะใช้อีเมลเป็นสื่อกลางในการเจรจาตกลงทางธุรกิจ การสั่งซื้อสินค้า หรือแม้กระทั่งการยืนยันชำระเงินค่าสินค้า จนอาจเป็นช่องทางให้บุคคลกลุ่มหนึ่งใช้โลกอินเทอร์เน็ตเป็นเครื่องมือในการทำมาหากิน โดยอาศัยเทคนิคความสามารถทางคอมพิวเตอร์พัฒนาตัวเป็น "**แฮกเกอร์**" ทำหน้าที่ล้วงลับข้อมูลทางธุรกิจ หรือปลอมตัวเป็นกิจการใหญ่ในต่างประเทศหลอกลวงคู่ค้าโดยตรง เพื่อแสวงหาผลประโยชน์ (เงิน) เข้าสู่ตนเอง

หลายๆ ท่านอาจคิดว่าตนเองรู้เรื่องการหลอกลวงผ่านอินเทอร์เน็ตดีอยู่แล้ว เพราะว่ามีเรื่องราวประสบการณ์ของผู้ประสบเหตุการณ์จริงถ่ายทอดให้เห็นอยู่ทั่วไป แต่ท่านทั้งหลายก็ไม่ควรประมาท เนื่องจากการแข่งขันทางการค้ารุนแรงมากขึ้นและมีความต้องการขยายธุรกิจเป็นแรงขับสำคัญในการหาลูกค้าใหม่ๆ เพิ่มมากขึ้น ในขณะเดียวกันก็ทำให้ผู้ไม่ประสงค์ดีมีโอกาสมากขึ้นในการหลอกลวงทางอินเทอร์เน็ต และที่สำคัญ อย่าลืมว่า ทุกวันนี้ผู้ร้ายทางอินเทอร์เน็ตสามารถพัฒนากลเม็ดหลอกลวงผู้อื่นอย่างไม่หยุดยั้งได้เช่นกัน

ในช่วงครึ่งปีแรกที่ผ่านมา มีผู้ส่งออกหลายรายขอให้ทางธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย หรือ EXIM BANK ช่วยตรวจสอบข้อมูลคู่ค้าซึ่งส่วนใหญ่จะเป็นผู้นำเข้าจากประเทศในทวีปแอฟริกา เนื่องจากได้รับการติดต่อโดยตรงจากต่างประเทศทางอีเมลว่าสนใจจะสั่งซื้อสินค้าจำนวนมาก ขณะที่ผู้ส่งออกไม่มีความมั่นใจว่าผู้ที่ติดต่อมานั้นมีตัวตนจริงหรือไม่ จึงขอใช้**บริการประเมินความเสี่ยงผู้ซื้อ/ธนาคารผู้ซื้อกับ** EXIM BANK ซึ่งผลจากการตรวจสอบข้อมูลผู้นำเข้าหลายสิบรายดังกล่าว พบว่าผู้ที่แสดงความประสงค์จะซื้อสินค้าทั้งหมดเป็นนักหลอกลวง หากผู้ส่งออกไม่ได้ตรวจสอบกับ EXIM BANK ก่อนและหลงกลเชื่อนักหลอกลวงเหล่านี้ เมื่อทำการติดต่อกลับและแสดงท่าทีว่าสนใจจะทำธุรกิจด้วย นักหลอกลวงเหล่านั้นจะเริ่มดำเนินการขั้นต่อๆ ไป เช่น ขอเงินล่วงหน้าในการติดต่อและดำเนินการนำเข้าในประเทศนั้นๆ และเมื่อมีการส่งมอบสินค้า นักหลอกลวงขั้นเซียนก็จะเชิดสินค้าไปในที่สุด ทั้งนี้ ไม่เพียงเฉพาะผู้ส่งออกเท่านั้นที่ต้องระมัดระวัง ท่านที่เป็นผู้นำเข้าก็ควรตระหนักในเรื่องเหล่านี้ด้วยเช่นกัน

นอกจากการโกงแบบตรงๆ ดังกล่าวแล้ว การโกงทางอินเทอร์เน็ตที่เป็นกรณีคลาสสิก คือ การที่บุคคลที่สามเข้าแฮกอีเมลของคู่ค้า และใช้กลวิธีปลอมตัวเป็นผู้ส่งออกไทย โดยที่ผู้นำเข้าในต่างประเทศคาดไม่ถึง เพื่อหลอกให้คู่ค้าที่เป็นผู้นำเข้าต่างประเทศโอนเงินค่าสินค้าเข้าบัญชีธนาคารเลขที่ใหม่แทนบัญชีเดิม ซึ่งโดยส่วนใหญ่กรณีนี้มักเกิดกับคู่ค้าที่ติดต่อธุรกิจกันมาพอสมควร และผู้ไม่หวังดีเหล่านี้ติดตามข้อมูลของคู่ค้ามาระยะหนึ่งจนรู้พฤติกรรมของคู่ค้า และเมื่อสบโอกาสก็จะแฮกอีเมลในขั้นตอนการชำระเงินค่าสินค้า

กรณีแบบนี้ก็เกิดขึ้นต่อเนื่องเป็นประจำ ผมขอยกตัวอย่างที่เกิดขึ้นในปีนี้ คือ บริษัทส่งออกเครื่องประดับอัญมณีไทยทำการค้ากับผู้นำเข้าในยุโรปมานานหลายปี โดยใช้อีเมลในการเจรจาตกลงธุรกิจเสมอมาและการค้าราบรื่นมาโดยตลอด ไม่เคยเกิดปัญหาหรืออุปสรรคใด ๆ แต่เมื่อต้นปีที่ผ่านมาบริษัทผู้นำเข้าในยุโรปได้รับอีเมลซึ่งมีชื่ออีเมลและชื่อผู้ส่งในตอนท้ายของอีเมลเป็นชื่อเดียวกันกับคนไทยที่เคยติดต่อค้าขายกันเป็นประจำ แจ้งว่าให้โอนเงินค่าสินค้าตามงวดที่ต้องชำระเข้าบัญชีธนาคารที่เปิดใหม่ โดยอ้างว่าบริษัทผู้ส่งออกอยู่ระหว่างการตรวจสอบบัญชีภายใน และไม่สะดวกที่จะตรวจสอบเงินที่โอนเข้ามาในบัญชีเก่าได้ จึงขอให้ใช้บัญชีใหม่ในการโอนเงินแทน ซึ่งบริษัทผู้นำเข้าก็ได้ขอการยืนยันผ่านอีเมล ซึ่งเมื่ออีเมลโดนแฮกแล้วก็ได้รับคำยืนยันจากผู้ร้ายนั่นเอง จึงได้ดำเนินการโอนเงินเข้าบัญชีใหม่ดังกล่าว เมื่อเวลาผ่านไประยะหนึ่ง เมื่อผู้ส่งออกฝ่ายไทยยังไม่ได้รับเงินค่าสินค้า และไม่ได้รับการติดต่อทางอีเมลอีกเลย จึงได้โทรศัพท์สอบถามผู้นำเข้า ทั้งสองฝ่ายจึงได้รู้ว่ามีบุคคลที่สามปลอมแปลงอีเมลของบริษัทผู้ส่งออกไทยเพื่อใช้สนทนาลวงหลอกให้บริษัทผู้นำเข้าโอนเงินเข้าในบัญชีของแฮกเกอร์ และเมื่อตรวจสอบกลับไปยังธนาคารนั้นก็ทราบว่าได้ปิดบัญชีไปแล้ว

หลายคนคงคิดว่าเหตุการณ์ลักษณะนี้ไม่น่าจะเกิดขึ้นได้ง่าย จะเป็นไปได้หรือที่จะมีใครมาแอบใช้อีเมลของเราไปสนทนากับคนอื่น? ในเมื่อนี่คืออีเมลส่วนตัวที่เราใช้เองเป็นประจำทุกวัน สำหรับการติดต่อธุรกิจการค้าทางอีเมลหากได้รับการติดต่อขอเปลี่ยนแปลงข้อมูลใดๆ โดยเฉพาะอย่างยิ่งข้อมูลที่สำคัญ เช่น การส่งมอบสินค้า การชำระเงิน ควรมีการโทรศัพท์ตรวจสอบกับคู่ค้าเพื่อยืนยันความถูกต้องทุกครั้งก่อนทำการโอนชำระเงินต่างๆ อย่างน้อยก็เป็นการยืนยันว่าได้ทราบการเปลี่ยนแปลงข้อมูล และควรมีการเปลี่ยนรหัสผ่าน (Password) อย่างสม่ำเสมอ เพื่อความปลอดภัยในการใช้งานอีเมลในการค้า รวมทั้งเมื่อเกิดปัญหาแล้วผู้ส่งออกไม่ควรยอมรับกับผู้ซื้อว่ามีผู้แฮกอีเมลของตนและควรรีบแจ้งความกับตำรวจเพื่อดำเนินการร่วมกับผู้นำเข้า และเพื่อรักษาสถานะหนี้ที่ผู้นำเข้าต่างประเทศต้องชำระค่าสินค้าให้คงอยู่ต่อไป

เส้นทางทุกสายไม่ได้ราบเรียบเสมอไป โดยเฉพาะ “เส้นทางแห่งธุรกิจการค้า” นั้นมีอุปสรรคและความท้าทายที่รอคอยผู้ที่จะคว้าชัยชนะในวงการธุรกิจ การก้าวเดินไปข้างหน้าด้วยความระมัดระวังเป็นสิ่งที่ไม่ควรละเลยแต่อย่างใด ประสบการณ์ของตนเองและผู้อื่นจะเสริมสร้างให้นักธุรกิจเติบโตอย่างแข็งแกร่ง และสามารถยืนหยัดได้ในเส้นทางแห่งธุรกิจการค้าสายนี้อย่างมั่นคง หากเกิดความประมาทก็จะส่งผลให้ธุรกิจเกิดความเสียหายเสมอ