

ภาคผนวก

ผนวก ก

การเล่นหุ้นผ่านทางระบบอิเล็กทรอนิกส์ให้ปลอดภัย

เป็นที่ทราบกันดีว่าความปลอดภัยในการทำธุรกรรมต่างๆ บนอินเทอร์เน็ตเป็นเรื่องสำคัญเรื่องหนึ่ง ที่ทำให้หลายคนลังเลหรือไม่กล้าเข้ามาทำธุรกรรมรูปแบบนี้ การซื้อขายหุ้นผ่านทางระบบอิเล็กทรอนิกส์ก็เช่นเดียวกัน ซึ่งอันที่จริงแล้วสามารถคลายความกังวลดังกล่าวลงได้ถ้าได้รู้ว่าบริษัทหลักทรัพย์มีระบบรักษาความปลอดภัยอะไร และผู้ลงทุนเอง จะมีวิธีป้องกัน และตรวจสอบในเรื่องนี้อย่างง่ายๆ ได้อย่างไรบ้าง ดังนี้

1. การตรวจสอบบริษัทหลักทรัพย์ว่ามีระบบตรวจสอบผู้ใช้งานก่อนเข้าระบบและก่อนส่งคำสั่งซื้อขายหุ้นหรือไม่

ในการสั่งซื้อขายหุ้นแต่ละวิธี บริษัทหลักทรัพย์จะต้องมีการตรวจสอบก่อนว่าคำสั่งซื้อขายหลักทรัพย์นั้นมาจากเจ้าของบัญชีที่แท้จริงหรือไม่ เช่น ดูจากลายเซ็น ฟังเสียง หรือดูหน้าตา ซึ่งการซื้อขายหุ้นผ่านอินเทอร์เน็ตก็เช่นเดียวกัน โดยเครื่องมือหลักอันหนึ่งที่ทุกบริษัทหลักทรัพย์ใช้ในการตรวจสอบตัวตนของผู้ใช้งานก่อนเข้าระบบ คือ การให้ป้อนชื่อผู้ใช้งาน และรหัสผ่านก่อนเข้าระบบ โดยชื่อผู้ใช้งานเป็นตัวที่บอกกับระบบว่า ท่านคือใคร และรหัสผ่านจะเป็นตัวยืนยันว่า ท่านคือคนที่อ้างนั้นจริง ซึ่งหลังจาก ผู้ใช้งานเข้าระบบแล้ว หากจะทำการส่งคำสั่งซื้อขายหุ้น ทุกบริษัทหลักทรัพย์ ก็มักจะให้ลูกค้าป้อนรหัสผ่านอีกครั้งหนึ่งเพื่อตรวจสอบให้แน่ใจก่อนว่าคนที่ป้อนคำสั่งดังกล่าว เป็นลูกค้ารายที่ถูกต้อง

ดังนั้น รหัสผ่านจึงเป็นปราการด่านแรกที่จะช่วยทำให้การซื้อขายหุ้นผ่านอินเทอร์เน็ตมีความปลอดภัยมากขึ้น และเป็นเรื่องสำคัญอย่างมาก ที่ผู้ลงทุนควรเรียนรู้ วิธีการใช้รหัสผ่านที่ถูกต้อง เพื่อป้องกันไม่ให้ผู้ไม่หวังดีคาดเดารหัสผ่าน แล้วแอบอ้างว่าเป็นตัวนักลงทุนเองเข้าไปในระบบเพื่อดูหรือแก้ไขข้อมูลสำคัญ หรือแอบส่งคำสั่งซื้อขายทำให้นักลงทุนได้รับความเสียหายได้

เทคนิคง่ายๆ ในการใช้รหัสผ่านอย่างถูกต้อง มีดังนี้

1. ควรเปลี่ยนรหัสผ่านทันทีที่ได้รับจากบริษัทหลักทรัพย์ เนื่องจากในช่วงก่อนที่รหัสผ่านจะถึงมือนักลงทุน อาจมีผู้อื่นรู้รหัสผ่านและลักลอบเข้ามาในระบบได้

2. ควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น ทุกๆ 3 เดือน เพื่อลดโอกาสที่คนอื่นอาจรู้รหัสผ่านแล้วเข้ามาในระบบของนักลงทุนได้
3. รหัสผ่านต้องยากในการคาดเดา โดยมีเทคนิค ดังนี้
 - ควรมีความยาวอย่างน้อย 6 ตัวอักษร
 - ควรเลือกรหัสผ่านที่มีตัวเลข ตัวอักษร หรือตัวอักขระพิเศษผสมกัน
 - ไม่ควรใช้รหัสผ่านตัวเดียวกับ User ID หรือใช้ชื่อ-นามสกุลของนักลงทุนเพราะอาจทำให้ผู้อื่นคาดเดาได้ง่าย
4. ไม่ควรบอกรหัสผ่านให้ผู้อื่นทราบ เพราะอาจมีผู้ไม่หวังดีแอบอ้างเป็นนักลงทุนเข้ามาในระบบ
5. ไม่ควรกำหนดให้เครื่องคอมพิวเตอร์จำรหัสผ่านไว้ เพราะหากคนอื่นมาใช้เครื่องคอมพิวเตอร์นั้น ก็จะสามารถเข้าไปในระบบของนักลงทุนได้ อย่างง่ายดาย
6. หากพบข้อสังเกตใดผิดปกติ หรือสงสัยว่ามีคนอื่นแอบเข้าระบบ เช่น ถ้าข้อมูลการเข้าระบบครั้งสุดท้าย (Last Login) ไม่ตรงกับวันเวลาที่นักลงทุนเข้าระบบครั้งล่าสุด เป็นต้น ให้นักลงทุนรีบเปลี่ยนรหัสผ่านทันทีเพื่อป้องกันมิให้ บุคคลนั้นเข้ามาในระบบอีก และแจ้งเจ้าหน้าที่บริษัทหลักทรัพย์ ให้ทำการตรวจสอบ
7. Log out ทันที ที่ลุกออกจากหน้าจอคอมพิวเตอร์ เพื่อป้องกันมิให้คนอื่นแอบเข้ามาดูหรือแก้ไขข้อมูล ที่อาจเปิดค้างที่หน้าจอ นั้น

2. ตรวจสอบบริษัทหลักทรัพย์ว่ามีการป้องกันข้อมูลสำคัญที่ส่งผ่านเครือข่ายหรือไม่

ในการส่งข้อมูลสำคัญผ่านเครือข่าย เช่น ข้อมูลรหัสผ่าน ข้อมูลเกี่ยวกับการซื้อขายหุ้น เป็นต้น บริษัทหลักทรัพย์ส่วนใหญ่จะมีการใช้เทคโนโลยีที่เรียกว่า Secure Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีการรักษาความปลอดภัยในการรับส่งข้อมูลผ่านอินเทอร์เน็ตที่ได้มาตรฐาน โดย SSL จะมีเครื่องมือที่ใช้ในการเข้ารหัสข้อมูลที่ส่งผ่านอินเทอร์เน็ต เพื่อป้องกันมิให้คนอื่นลักลอบดูข้อมูล และเครื่องมือที่ใช้ในการตรวจสอบว่าข้อมูลที่ส่งมาถูกแก้ไขเปลี่ยนแปลงระหว่างทางหรือไม่ด้วย ดังนั้น หากเว็บไซต์ใดใช้ SSL ก็จะทำให้มั่นใจมากขึ้นว่าข้อมูลที่ส่งผ่านระบบนั้นจะมีความปลอดภัย ซึ่งนักลงทุนก็สามารถใช้เป็นข้อมูลในการตัดสินใจเลือกใช้บริการจากบริษัทหลักทรัพย์ได้ โดยวิธีการดูง่ายๆ ว่าเว็บไซต์ไหนใช้เทคโนโลยี SSL มีดังนี้

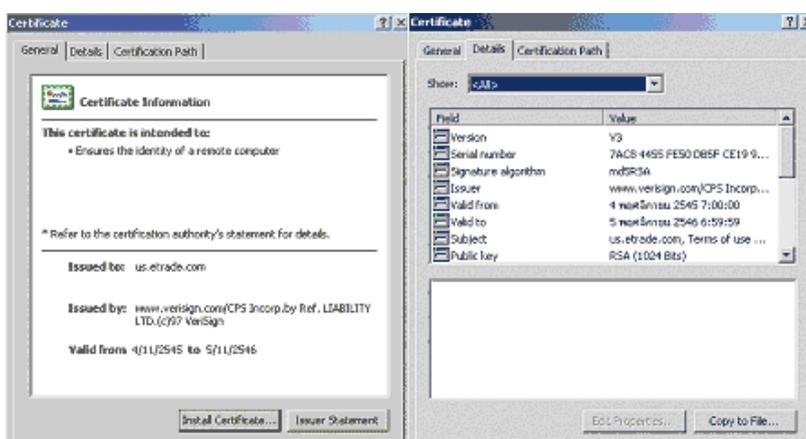
- 1) ที่บริเวณชื่อที่อยู่ของเว็บไซต์ (URL) ต้องมีคำว่า “ https:// ” ดังรูป



2) ที่ Task bar ซึ่งอยู่บริเวณมุมขวาล่างของหน้าจอต้องมีรูปแม่กุญแจปรากฏอยู่



โดยเมื่อคลิกที่รูปแม่กุญแจจะปรากฏหน้าจอแสดงข้อมูลใบรับรองอิเล็กทรอนิกส์ (Certificate Information) ซึ่งมีข้อมูลเกี่ยวกับการรับรองตัวตนของเครื่องคอมพิวเตอร์ ที่นักลงทุนกำลังติดต่ออยู่ เช่น ชื่อผู้ออกใบรับรองซึ่งต้องเป็นหน่วยงานที่น่าเชื่อถือ (ตัวอย่างคือ verisign.com) ชื่อเว็บไซต์ ที่ได้รับการรับรอง ซึ่งต้องเป็นชื่อเว็บไซต์เดียวกัน กับที่นักลงทุนกำลังติดต่ออยู่ และช่วงเวลาใบรับรองมีผลบังคับซึ่งต้องครอบคลุมช่วงเวลาให้นักลงทุนกำลังเข้าเว็บไซต์นั้นอยู่ เป็นต้น ดังภาพ



3) การตรวจสอบว่าเว็บไซต์ที่เราากำลังติดต่ออยู่เป็นเว็บไซต์จริงของบริษัทหลักทรัพย์หรือไม่

เนื่องจากการทำธุรกรรมผ่านอินเทอร์เน็ตในต่างประเทศเคยพบกรณีผู้ประสงค์ร้ายปลอมแปลง เว็บไซต์โดยทำหน้าตาและชื่อเว็บไซต์คล้ายคลึงกับเว็บไซต์จริง ซึ่งแม้ว่าเหตุการณ์แบบนี้อาจยังไม่ปรากฏแน่ชัดว่าเคยเกิดขึ้นในเมืองไทย แต่หากเกิดขึ้นและมีนักลงทุนรายใดหลงเข้าไป Log in ที่เว็บไซต์ปลอมดังกล่าวก็อาจถูกผู้ประสงค์ร้ายลักลอบดูและสำเนาข้อมูลสำคัญต่างๆ เช่น Username รหัสผ่าน เลขที่บัตรเครดิต เป็นต้น และนำข้อมูลดังกล่าวไปใช้ประโยชน์ต่อ

ได้ ดังนั้น เพื่อความไม่ประมาท ผู้ลงทุนก็ควรเรียนรู้วิธีป้องกันและตรวจสอบเรื่องดังกล่าวในเบื้องต้นซึ่งมีวิธีการง่ายๆ ดังนี้

- ก่อนจะ Log in เพื่อเข้าระบบทุกครั้ง นักลงทุนควรตรวจสอบว่าชื่อเว็บไซต์ของบริษัทหลักทรัพย์ ว่าถูกต้องหรือไม่ เช่น ปกติชื่อเว็บไซต์ของบริษัทหลักทรัพย์ XYZ เป็น www.xyz.co.th แต่ถ้าปรากฏว่า ชื่อเปลี่ยนไปเป็น www.xyz.com ให้รีบตรวจสอบข้อมูลกับบริษัทหลักทรัพย์ทันทีเพราะนั่นอาจเป็น สัญญาณเตือนว่าเป็นเว็บไซต์ปลอม
- หากนักลงทุนได้รับจดหมาย หรือ e-mail แจ้งการเปลี่ยนแปลงชื่อเว็บไซต์ รวมถึงพบ ข้อมูลหรือบริการใดที่มีข้อความเกินจริงหรือมีลักษณะผิดปกติ อย่าเพิ่งหลงเชื่อ ให้ติดต่อสอบถาม บริษัทหลักทรัพย์เพื่อยืนยันความถูกต้องก่อน
- นักลงทุนควรจดจำลักษณะสำคัญของเว็บไซต์ที่ตนเองเข้าไปทำธุรกรรมอยู่เป็นประจำ หากมีการเปลี่ยนแปลงใดที่มีนัยสำคัญเกิดขึ้นก็ควรติดต่อสอบถามกับบริษัทหลักทรัพย์ก่อน

ในกรณีที่เว็บไซต์ใดใช้ SSL หากนักลงทุนพบเครื่องหมายตกใจ  ในหน้าจอเตือนเกี่ยวกับระบบรักษาความปลอดภัย (ดูตัวอย่าง) ให้กดปุ่ม “No” และติดต่อสอบถามข้อมูลกับบริษัทหลักทรัพย์ เพราะนั่นหมายถึงว่า SSL ได้ตรวจพบข้อมูลที่ไม่ถูกต้องเกี่ยวกับใบรับรองอิเล็กทรอนิกส์ เช่น ใบรับรองนั้น อาจไม่ได้มาจากหน่วยงานรับรองที่เชื่อถือได้หรือหมดอายุแล้ว หรือชื่อเว็บไซต์ที่ถูกค้ำกำลังติดต่ออยู่ อาจไม่ตรงกับที่ระบุในใบรับรอง เป็นต้น



ข้อเตือนใจ ผู้ลงทุนต้องตรวจสอบความถูกต้องครบถ้วนของข้อมูลต่างๆ เช่น ข้อมูลรายการซื้อขายหลักทรัพย์ (Portfolio) ข้อมูลวงเงินคงเหลือ เป็นต้นควบคู่กับการใช้เทคนิคต่างๆ ที่ได้กล่าวไปข้างต้น และหากพบข้อมูลใดที่ผิดสังเกต ก็ต้องติดต่อเจ้าหน้าที่ของบริษัทหลักทรัพย์ เพื่อตรวจสอบทันที เพราะนั่นเป็นสัญญาณเตือนว่าอาจมีผู้ไม่หวังดีแอบเข้ามาในระบบ และทำการแก้ไขหรือส่งคำสั่งซื้อขายแทนนักลงทุนได้

ที่มา : สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)