บริษัทหลักทรัพย์ ไอ วี โกลบอล จำกัด (มหาชน) ขอขอบพระคุณที่ท่านให้ความไว้วางใจ บริษัท ฯ ขอแนะนำการใช้งานบัญชีซื้อขายหลักทรัพย์ทางอินเทอร์เน็ตอย่างปลอดภัยดังนี้

ข้อแนะนำในการตั้งรหัสผ่าน และการใช้งานระบบ

- รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร
- มีการกำหนดให้ใช้ร่วมกับตัวเลข และ อักขระพิเศษ เช่น !@#%$>
- รหัสผ่านต้องถูกเลือกอย่างระมัดระวัง หลีกเลี่ยงคำหรือตัวเลขที่คาดเดาได้ง่าย หรือง่ายเกินไป เช่น 123
- ไม่ใช้คำในพจนานุกรม
- ไม่เปลี่ยนรหัสผ่านซ้ำของเดิม
- ให้ทำการเปลี่ยนรหัสผ่านสม่ำเสมอ อย่างน้อย ทุกๆ 3 เดือน หรือเมื่อสงสัยว่ารหัสผ่านรั่วไหลหรืออาจถูกคาดเดาได้
- รหัสผ่านต้องถูกเก็บเป็นความลับ ถือเป็นความรับผิดชอบของผู้ใช้ ไม่ควรบอกรหัสผ่านให้กับบุคคลอื่นๆ
- ควร log out ออกจากระบบเมื่อเลิกใช้งาน หรือ เมื่อต้องห่างจากเครื่องเป็นเวลานาน
- หมั่นตรวจสอบรายการเคลื่อนไหวและหุ้นคงเหลืออย่างสม่ำเสมอ เพื่อป้องกันการนำหุ้นของท่านไปใช้ประโยชน์
- หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์สาธารณะ และระมัดระวังการเชื่อมต่อกับเครือข่าย WiFi สาธารณะหรือเครือข่ายที่ไม่ปลอดภัย เช่น ในอินเทอร์เน็ตคาเฟ่
- ระบบจะกำหนดให้ผู้ใช้เปลี่ยนรหัสผ่าน เมื่อมีการเข้าใช้งานในครั้งแรก
- เมื่อเปลี่ยนรหัสผ่านแล้ว ผู้ใช้ต้องทำการกำหนด PIN เพื่อใช้ในการส่งคำสั่ง

ข้อแนะนำในการปฏิบัติเพื่อป้องกันการทุจริต ดังต่อไปนี้

ไม่เปิดเผยข้อมูลส่วนบุคคลใดๆ ของตนเอง อาทิ รหัสประจำตัว (User ID) รหัสผ่าน (Password) หรือรหัสส่งคำสั่ง (PIN CODE) หมายเลขบัญชี หมายเลขบัตรเครดิต หรือข้อมูลส่วนบุคคลใดๆ ผ่านทาง e-mail หรือในระหว่างทำรายการผ่านบริการของบริษัท ฯ เนื่องจากบริษัท ฯ ไม่มีนโยบายในการดำเนินการสอบถามข้อมูลส่วนบุคคลใดๆ ของผู้ใช้บริการผ่านช่องทางดังกล่าว ตรวจสอบความถูกต้องของรายการธุรกรรม และตรวจสอบยอดหุ้นคงเหลือในบัญชีของท่านอย่สม่ำเสมอ เพื่อป้องกันรายการผิดปกติที่อาจจะเกิดขึ้นเมื่อได้รับอีเมล์ล่อลวง อย่าตอบกลับอีเมล์ใดๆ ที่ขอให้เปิดเผยข้อมูลส่วนบุคคล โปรดตั้งข้อสงสัยไว้เมื่อพบว่ามีอีเมลจากธุรกิจหรือบุคคลใดที่พยายามให้ผู้ใช้บริการเปิดเผยรหัสผ่าน หมายเลขบัญชีหรือข้อมูลใดๆ ที่เป็นความลับ หรืออีเมล์ใดที่ส่งข้อมูลส่วนบุคคลของผู้ใช้บริการมาเพื่อให้ปรับปรุงข้อมูลหรือยืนยันความถูกต้อง กรุณาลบอีเมล์นั้นทันทีหากพบความผิดปกติของหน้าจอขณะทำรายการ โปรดหยุดทำรายการทันที ไม่ต้องปฏิบัติตามคำแนะนำใดๆ ทั้งสิ้น และกรุณาออกจากเว็บไซต์ที่น่าสงสัยทันที ควรตรวจสอบโปรแกรมป้องกันไวรัสและอัพเดทฐานข้อมูลไวรัสให้เป็นเวอร์ชั่นล่าสุดเสมอ

ข้อแนะนำการใช้งานอินเทอร์เน็ตทั่วไป

ทุกครั้งที่เชื่อมต่ออินเทอร์เน็ต ขอให้ท่านตระหนักถึงความเสี่ยงที่ท่านอาจจะดาวน์โหลดไวรัสหรือมัลแวร์เข้าเครื่องคอมพิวเตอร์โดยไม่ตั้งใจ และซอฟท์แวร์เหล่านี้อาจเป็นเครื่องมือที่มิจฉาชีพใช้โจรกรรมข้อมูลส่วนตัวของท่าน พฤติกรรมการใช้อินเทอร์เน็ตบางอย่างอาจนำมาซึ่งความเสี่ยง เช่น การเปิดอีเมลที่ไม่รู้จัก การเข้าเว็บไซต์ที่ไม่น่าไว้ใจ หรือการดาวน์โหลดโปรแกรม ไฟล์หรือไฟล์ภาพและเสียงจากเว็บไซต์ที่ไม่น่าเชื่อถือ

ดังนั้น บริษัท ฯ ขอแนะนำให้ท่านรักษาความปลอดภัยสำหรับตัวท่านเองด้วยการปฏิบัติตามข้อแนะนำง่ายๆ ดังนี้

- ติดตั้งซอฟท์แวร์ป้องกันไวรัสและสปายแวร์อย่างน้อย 1 โปรแกรม และทำการอัพเดทอยู่เสมอ
- อัพเดทโปรแกรมปรับปรุงระบบ (Patches) ของซอฟท์แวร์บนคอมพิวเตอร์และอินเทอร์เน็ตของท่าน เพื่อปิดช่องโหว่ที่ไวรัสหรือมัลแวร์อาจใช้เป็นช่องทางบุกรุกเข้าสู่ระบบ
- ล้างค่าต่างๆ และประวัติการใช้งานของบราวเซอร์หลังจากเสร็จสิ้นการใช้งานในแต่ละครั้ง เพื่อลบข้อมูลบัญชีของท่านทั้งหมด
- ระวังการชำระเงินในการสั่งซื้อสินค้าผ่านระบบอินเทอร์เน็ต เพราะอาจจะมีผู้อื่น คอยดักจับเลขที่บัตรเครดิตขณะที่กำลังใช้งานได้ ดังนั้นควรตรวจสอบระบบความปลอดภัยของเว็บไซต์นั้นๆ ว่ามีระบบความปลอดภัยหรือไม่ ก่อนทำการสั่งซื้อสินค้าทางออนไลน์
- ควรทำการตรวจสอบระบบความปลอดภัยของซอฟต์แวร์ที่ใช้งานอินเทอร์เน็ตอย่างสม่ำเสมอ เช่น Windows, Firefox, Chrome เป็นต้น
- ไม่ควรดาวน์โหลดโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือ
- ไม่ควรคลิกรับโปรแกรม หรือเปิดไฟล์ต่าง ๆ จากบุคคลอื่นที่ไม่รู้จักผ่านการใช้งานโปรแกรมแชทหรือโปรแกรมแชร์ไฟล์ต่างๆ รวมทั้งทางอีเมล์ และไม่ควรรับไฟล์ใด ๆ แม้จากคนที่เรารู้จักหากไม่ได้รับการยืนยันจากผู้ส่งว่าได้ส่งไฟล์มา เพราะปัจจุบันมีไวรัสหรือมัลแวร์ที่สามารถปลอมตัวหรือใช้โปรแกรมของผู้ส่งไปยังผู้รับได้ เมื่อรับมาก็คือการรับไวรัสเข้ามายังเครื่องคอมพิวเตอร์นั่นเอง

- ควรระมัดระวังในการใช้อีเมล์ของตนเองลงทะเบียนตามเว็บไซต์ต่าง ๆ เพราะอาจจะทำให้ได้รับจดหมายขยะจากเว็บไซต์โฆษณาสินค้าหรือเว็บไซต์ที่มีไวรัส
- ถ้าต้องการความปลอดภัยสูงขึ้นในการใช้งานอินเทอร์เน็ต สามารถติดตั้งโปรแกรมไฟร์วอลล์ บนเครื่องคอมพิวเตอร์เพื่อป้องกันผู้บุกรุกจากภายนอกเข้าสู่เครื่องผู้ใช้

การใช้งานอินเทอร์เน็ตผ่านจุดเชื่อมต่อสาธารณะอย่างปลอดภัย

- ผู้ใช้งานเครื่องคอมพิวเตอร์ หรือโทรศัพท์มือถือควรมีการติดตั้งโปรแกรมป้องกันล่าสุด และอัพเดทโปรแกรมหรือฐานข้อมูลไวรัสอยู่เสมอทันทีที่มีการแจ้งเตือน เพื่อป้องกันไวรัสชนิดใหม่ๆ ที่อาจทำอันตรายกับอุปกรณ์ของคุณ
- ควรติดตั้งโปรแกรมไฟร์วอลล์ เพื่อป้องกันการเข้าถึงคอมพิวเตอร์และโทรศัพท์มือถือของคุณโดยผู้ไม่ได้รับอนุญาต และควรมั่นใจว่ามีการอัพเดทโปรแกรมอยู่เสมอ
- หลีกเลี่ยงการดาวน์โหลดข้อมูลต่างๆ เนื่องจากอาจมีซอฟท์แวร์สอดแนม (Spyware) แฝงมากับไฟล์ด้วย
- หลีกเลี่ยงการทำรายการที่ใช้ข้อมูลบัตรเครดิต การทำธุรกรรมเกี่ยวกับการเงิน เนื่องจากซอฟท์แวร์สอดแนมสามารถแอบดักข้อมูลและเข้าถึงรหัสผ่าน หมายเลขบัตรเครดิต และบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึงได้
- ซอฟท์แวร์สอดแนม เป็นซอฟท์แวร์ที่ออกแบบเพื่อสังเกตการณ์หรือดักจับข้อมูลการใช้อินเทอร์เน็ต โดยจะถูกติดตั้งไว้ในเครื่องคอมพิวเตอร์ (ด้วยความยินยอมจากผู้ใช้หรือไม่ก็ตาม) เมื่อมีการดาวน์โหลดไฟล์ ซอฟท์แวร์ เกม หรือสกรีนเซฟเวอร์ จากเว็บไซต์ต่างๆ มายังอุปกรณ์ของเรา ซึ่งจะทำให้การใช้งานบนคอมพิวเตอร์ล่าช้า เนื่องจากการใช้ทรัพยากรระบบที่สูงเกินปกติ ส่งผลไปถึงความเสียหายของเครื่องคอมพิวเตอร์ได้

การใช้งานอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์สาธารณะ

- ให้ปิดเว็บบราวเซอร์ทั้งหมดที่เปิดใช้งานหลังจากที่ใช้งานเสร็จแล้ว
- ล้างหน่วยความจำคอมพิวเตอร์ (Cache) ในเว็บบราวเซอร์หลังจากที่ใช้งานเสร็จแล้ว ซึ่งจะช่วยลดโอกาสที่ผู้อื่นจะสามารถเขาถึงข้อมูลส่วนตัวของท่านได้
- ให้ล้างบันทึกประวัติการใช้งาน (History settings) ในเว็บบราวเซอร์หลังจากที่ใช้งานเสร็จแล้ว
- ไม่อนุญาตให้เครื่องคอมพิวเตอร์จำรหัสผ่านให้ เช่น จะต้องคลิกตัวเลือกการจำรหัสผ่านออก
- ไม่ป้อนข้อมูลลับหรือส่วนตัวที่เป็นความลับใดๆ โดยผ่านทางเครื่องคอมพิวเตอร์สาธารณะ