การใช้อินเทอร์เน็ตให้ปลอดภัยสำหรับผู้ใช้งานในองค์กร

(How to Use Internet Safely for Users in Organization)

นายนรินทร์ พนาวาส

(ผู้ช่วยอธิการบดีฝ่ายบริหาร มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี)

e-Mail: narin.pa@east.spu.ac.th

ในปัจจุบันทุกองค์กรมีการใช้บริการต่างๆ บนระบบเครือข่ายอินเทอร์เน็ตเพิ่มมากขึ้นเป็นลำดับทั่วโลก เพื่อเป็นช่องทางในการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว รวมถึงการทำธุรกิจออนไลน์และการพาณิชย์ในด้านต่างๆ ซึ่งช่วยในเรื่อง การลดระยะเวลาและต้นทุนในการติดต่อสื่อสาร รวมไปถึงการศึกษาหาความรู้ จากระบบอินเทอร์เน็ต แต่อย่างไรก็ตาม ผู้ใช้งานโดยทั่วไปในองค์กรต่างๆ ยังไม่เห็นความสำคัญ ของการใช้งานอินเทอร์เน็ตที่ปลอดภัยเท่าที่ควร เนื่องจากขาดความรู้ ในการใช้งาน และวิธีป้องกันที่ถูกวิธีหรืออาจคิดว่าคงไม่มีปัญหาอะไรมาก แต่เมื่อเกิดปัญหาขึ้นกับตนเองแล้ว ก็ทำให้ตนเองและองค์กรเดือดร้อน หรือการใช้งานอินเทอร์เน็ตที่ผิดวิธี เช่น การโพสข้อความลงกระทู้ (Webboard) ที่ส่งผลให้ผู้อื่นเสียหาย โดยคิดว่าจะไม่มีใครรู้ว่าตนเองเป็นใคร การถูกขโมย Account อินเทอร์เน็ตไปใช้งาน การถูกขโมยเลขที่บัตรเครดิตไปใช้งาน การถูกลบข้อมูลบนเครื่องคอมพิวเตอร์ และการถูกปล่อยไวรัสมาไว้บนเครื่องคอมพิวเตอร์ หรือการได้รับอีเมล์ขยะ (Junk Mail) เป็นจำนวนมาก รวมไปถึงการส่งอีเมล์แบบหลอกลวง (Phishing) ให้ผู้รับอี-เมล์ เข้าไปในเว็บไซต์นั้น เพื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ เช่น ข้อมูลของหมายเลขบัตรเครดิต เลขที่บัญชีผู้ใช้ (Username) รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ ที่มีความสำคัญ เพื่อที่บุคคลผู้ไม่หวังดีเหล่านั้น จะนำข้อมูลที่ได้ไปดำเนินการทำธุรกรรมต่างๆ ต่อไปบนระบบอินเทอร์เน็ต การเข้าเว็บไซต์ลามกหรือเว็บไซต์ที่มีไวรัส และการดาวน์โหลดข้อมูลประเภท P2P เช่น ภาพยนตร์ เพลง วีดีโอ ที่ไม่จำเป็น เป็นต้น

ซึ่งปัญหาต่างๆ เหล่านี้ในหลายองค์กรอาจประสบปัญหากันบ้างแตกต่างกันออกไป ดังนั้นเพื่อเป็นการป้องกันหรือลดความเสียหายต่างๆ ที่อาจจะเกิดขึ้นในอนาคต องค์กรควรมีแนวทางและวิธีการป้องกันที่ดี รวมไปถึงการแนะนำหรือฝึกอบรมให้ผู้ใช้งานในองค์กร รู้ถึงกฎระเบียบ ข้อกำหนด และวิธีการใช้งานอินเทอร์เน็ตอย่างไรให้ปลอดภัย อาทิเช่น

1. องค์กรควรติดตั้งระบบรักษาความปลอดภัย สำหรับเครือข่ายอินเทอร์เน็ตอย่างสมบูรณ์และพอเพียง ทั้งระบบโปรแกรม หรืออุปกรณ์ประเภทที่สามารถตรวจสอบไวรัส และป้องกันการใช้งานประเภทต่างๆ ที่ไม่พึงประสงค์ ทางเข้า-ออก ของการใช้งานอินเทอร์เน็ต เช่น ตรวจสอบไวรัส และเมล์ขยะในขณะรับ-ส่งอีเมล์ ป้องกันการเปิดเข้าเว็บไซต์ที่มีไวรัส

2. ป้องกันการเข้าเว็บไซต์ลามก หรือเว็บไซต์ที่ ไม่พึงประสงค์ และป้องกันโปรแกรมดาวน์โหลดข้อมูล หรือควบคุมการใช้งานที่ไม่จำเป็นประเภท P2P, Multimedia, FTP เป็นต้น

3. ควรทำการตรวจสอบ และอัพเดตระบบความปลอดภัย ของซอฟต์แวร์ที่ใช้งานอินเทอร์เน็ต บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน เช่น Windows Internet Explorer และ Outlook Express จากเว็บไซต์ www.microsoft.com และ www.cert.org เป็นต้น

4. ทำการติดตั้งโปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์ โดยเป็นโปรแกรมประเภท ที่ต้องจ่ายเงินค่าใช้บริการ เช่น Mcafee VirusScan , Norton Antivirus และ NOD32 เป็นต้น หรือโปรแกรมประเภทที่ใช้งานฟรีโดยสามารถ Download โปรแกรมป้องกันไวรัสฟรี ได้ที่เว็บไซต์ www.free-av.com , http://free.grisoft.com และ www.avast.com เป็นต้น และควรหมั่นอัพเดตโปรแกรมป้องกันไวรัสอย่างน้อยสัปดาห์ละครั้ง

5. ทำการติดตั้งโปรแกรมตรวจสอบและกำจัดโปรแกรมประเภทมัลแวร์ (Malware) บนเครื่องคอมพิวเตอร์ โดยสามารถ Download โปรแกรมกำจัด Malware ฟรี ได้ที่เว็บไซต์ www.spybot.info และ www.lavasoft.com เป็นต้น

6. การตั้งกระทู้ หรือตอบกระทู้ตามเว็บไซต์ต่างๆ ควรใช้คำที่สุภาพไม่ขัดต่อศีลธรรม และจริยธรรมอันดี ไม่ควรนำข้อมูลที่เป็นเรื่องส่วนตัวของผู้อื่น ไปเผยแพร่ก่อนได้รับอนุญาต และก่อให้เกิดความเดือดร้อนให้กับผู้อื่น

7. ไม่ควรให้ Account อินเทอร์เน็ตกับบุคลอื่นไปใช้งาน และควรเปลี่ยน password อย่างน้อย เดือนละครั้ง การตั้ง password ใหม่ ควรตั้งให้มีความยาว

ของอักษรไม่ต่ำกว่า 7-8 ตัวโดยใช้ ตัวเลขผสมตัวอักษรและอักขระพิเศษ เช่น 255w$cit&1 ถ้าในกรณีที่รู้ว่า Account ตนเองมีปัญหาในการใช้งาน ให้ติดต่อหน่วยงานที่ให้บริการทันที

8. ระวังการจ่ายเงินสั่งซื้อสินค้าผ่านระบบอินเทอร์เน็ต เพราะอาจจะมีผู้อื่น คอยดักจับเลขที่บัตรเครดิต ดังนั้น ควรตรวจสอบระบบความปลอดภัยของเว็บไซต์นั้นๆ ว่ามีระบบความปลอดภัยหรือไม่ ก่อนทำการสั่งซื้อ และพิจารณาให้รอบคอบเกี่ยวกับข้อมูลที่ได้รับทางอีเมล์ ที่ให้เข้าไปกรอกข้อมูลด้านการเงิน ต้องพิจารณาเว็บไซต์ดังกล่าวว่ามีตัวตนจริง หากไม่แน่ใจ ควรติดต่อไปยังเจ้าของเว็บไซต์ หรือเจ้าของสถาบันการเงินดังกล่าว เพื่อสอบถามข้อมูล

9. ไม่ควร Download โปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือ

10. ไม่ควรรับโปรแกรมหรือเปิดไฟล์ต่างๆ จากบุคคลที่ไม่รู้จัก ผ่านทางระบบ e-Mail และการใช้งานโปรแกรมประเภท Chat ต่างๆ เช่น ICQ , MSN Messenger, Yahoo Messenger, Pirch และ Skype เป็นต้น

11. ไม่ควรนำ e-Mail ของตนเองไปลงทะเบียนตามเว็บไซต์ต่างๆ เพราะจะทำให้ได้รับจดหมายขยะ จากเว็บไซต์โฆษณาสินค้าหรือเว็บไซต์ที่มีไวรัส

เครื่องคอมพิวเตอร์ของผู้ใช้งาน หากต้องการความปลอดภัยที่สูงขึ้น ในการใช้งานอินเทอร์เน็ต สามารถติดตั้งโปรแกรม Personal Firewall บนเครื่องคอมพิวเตอร์เพื่อป้องกันผู้บุกรุกจากภายนอกเข้าสู่เครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยสามารถ Download โปรแกรมฟรีมาทดลองใช้งานได้ที่เว็บไซต์ www.zonelabs.com , www.sygate.com และ www.kerio.com เป็นต้น

จะเห็นได้ว่า ถ้าองค์กรต่างๆ ให้ความสำคัญกับวิธีการใช้งานอินเทอร์เน็ต ให้ปลอดภัยและถูกวิธีกับผู้ใช้งานภายในองค์กร ก็จะสามารถลดปัญหา การใช้งานอินเทอร์เน็ตของผู้ใช้งานลงได้อย่างมาก และส่งผลดีทางด้านภาพลักษณ์ให้กับองค์กร รวมไปถึง ยังสามารถลดการลงทุนทางด้านไอที ในแต่ละปีเพื่อการแก้ไขปัญหาดังกล่าวลงได้ ถ้าองค์กรได้รับความร่วมมือที่ดี จากผู้ใช้งานทุกคน