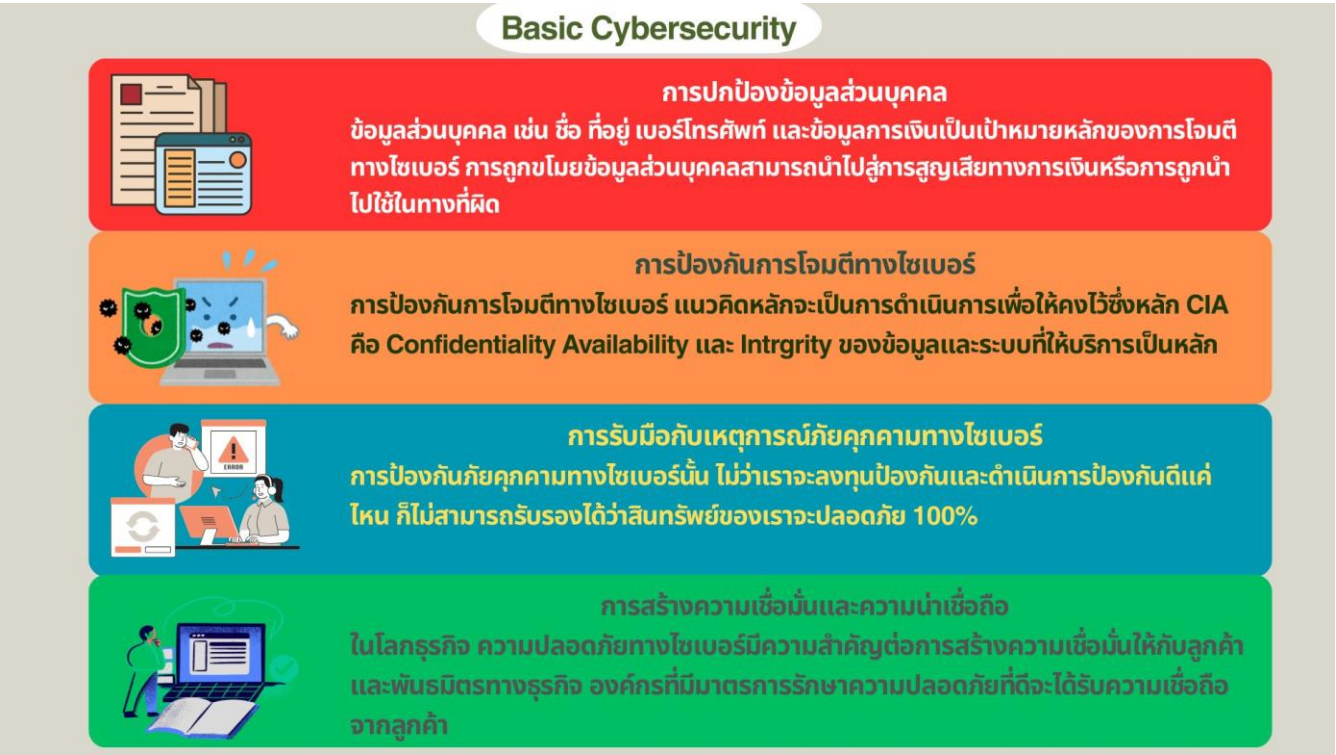
ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

Basic Cybersecurity Series

น.ส.อิสริยา มีสิงห์

นักวิชาการเกษตรชำนาญการพิเศษ

กลุ่มวิจัยและพัฒนาการใช้ประโยชน์หญ้าแฝกในการจัดการดิน กองวิจัยและพัฒนาการจัดการที่ดิน



ในยุคที่เทคโนโลยีและอินเตอร์เน็ตเข้ามามีบทบาทสำคัญในชีวิตประจำวันของเรานั้น ความปลอดภัยทางไซเบอร์ไม่สามารถมองข้ามได้ แม้ว่าจะเป็นในองค์กรขนาดใหญ่หรือบุคคลทั่วไป การรักษาความปลอดภัยของข้อมูลถือเป็นหัวใจสำคัญที่ช่วยป้องกันความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นได้ในหลาย ได้แก่

1.การปกป้องข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และข้อมูลการเงิน เป็นเป้าหมายหลักของการโจมตีทางไซเบอร์ การถูกขโมยข้อมูลส่วนบุคคล สามารถนำไปสู่การสูญเสียทางการเงินหรือการถูกนำไปใช้ในทางที่ผิด การมีพื้นฐานของความมั่นคงปลอดภัยทางไซเบอร์ เช่น การใช้งานรหัสผ่านที่เข้มแข็งและไม่ซ้ำกัน การเปิดการใช้งานการยืนยันตัวตนแบบสองขั้น และการรักษาความลับข้อมูลส่วนบุคคล จะช่วยลดความเสี่ยงในการถูกโจมตี

2. การป้องกันการโจมตีทางไซเบอร์

การป้องกันการโจมตีทางไซเบอร์ แนวคิดหลักจะเป็นการดำเนินการเพื่อให้คงไว้ซึ่งหลัก CIA คือ Confidentiality Availabiliity และ Integrity คือการรักษาความลับของข้อมูล การทำให้ข้อมูลพร้อมใช้อยู่เสมอ และแน่ใจว่าข้อมูลมีความถูกต้อง โดยในการดำเนินการเพื่อให้ระบบนั้นมีความมั่นคงปลอดภัยควรดำเนินการตามหลักการประเมินความเสี่ยงเพื่อให้แน่ใจได้ว่าจะปกป้องสินทรัพย์ได้อย่างปลอดภัยด้วยการลงทุนที่เหมาะสม และต้องดำเนินการป้องกันให้รอบด้านเพื่อให้แน่ใจว่าได้จัดแนวทางการป้องกันสินทรัพย์ต่างๆ โดยเฉพาะข้อมูลตลอดไปจนถึงข้อมูลส่วนบุคคลให้ปลอดภัยจากการโจมตีจากผู้ไม่หวังดีในโลกไซเบอร์ยุคปัจจุบัน

3. การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์

การป้องกันภัยคุกคามทางไซเบอร์นั้น ไม่ว่าจะป้องกันดีแค่ไหนก็ไม่สามารถรับรองได้ว่าสินทรัพย์ของเราจะปลอดภัย ดังนั้นในปัจจุบันจะเน้นการป้องกันให้เหมาะสมตามแนวทางการประเมินความเสี่ยงและทำการป้องกันตามแนวปฏิบัติที่เป็นมาตรฐานเพื่อให้แน่ใจว่าเราได้ทำการป้องกันสินทรัพย์ได้ดีเพียงพอ และสิ่งที่สำคัญต่อจากนั้นคือการพร้อมรับมือหากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยจะเริ่มจากการตรวจสอบเฝ้าระวังตลอดเวลาเพื่อให้รับรู้ถึงภัยคุกคามที่จะเกิดขึ้นได้อย่างรวดเร็วที่สุด ตามด้วยการมีแผนรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเพื่อที่จะสามารถระงับเหตุไม่ให้เกิดความเสียหายมากกว่าที่เป็นอยู่ และสุดท้ายเป็นแผนในการฟื้นฟูบริการให้สามารถกลับมาให้บริการได้ตามปกติอย่างเร็วที่สุด

4. การสร้างความเชื่อมั่นและความน่าเชื่อถือ

การสร้างความเชื่อมั่นและความน่าเชื่อถือในโลกธุรกิจ ความปลอดภัยทางไซเบอร์มีความสำคัญต่อการสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรทางธุรกิจ องค์กรที่มีมาตรการรักษาความปลอดภัยที่ดีจะได้รับความเชื่อถือจากลูกค้า เนื่องจากลูกค้ารู้สึกมั่นใจว่าข้อมูลของตนจะไม่ถูกละเมิด นอกจากนี้ความปลอดภัยทางไซเบอร์ที่เข้มแข็งยังช่วยป้องกันความเสียหายทางธุรกิจที่อาจจะเกิดจากการโจมตีทางไซเบอร์ได้ เช่น การถูกเรียกค่าไถ่ข้อมูลหรือการสูญเสียความสามารถในการดำเนินธุรกิจ

สรุปการมีความรู้พื้นฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น เป็นสิ่งจำเป็นสำหรับทุกคนในยุคดิจิทัลนี้ ไม่เพียงแต่ป้องกันข้อมูลส่วนบุคคลและระบบคอมพิวเตอร์ของเราเอง แต่ยังเพื่อสร้างความมั่นคงให้กับองค์กรและสร้างความเชื่อมั่นให้ลูกค้าและพันธมิตรทางธุรกิจ การลงทุนในความรู้และการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ควรทำ เพื่อเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นในอนาคต แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถนำไปปรับใช้ สามารถศึกษาได้จากมาตรฐานสากล เช่น ISO/IEC 27001 Version 2022 และ NIST Cybersecurity Framework Version 2.0 เป็นต้น

กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน

วุฒิบัตรฉบับนี้ให้ไว้เพื่อแสดงว่า

นายเกษมสุข ศรีแย้ม

ได้ผ่านการฝึกทักษะออนไลน์

เรื่อง หลักสูตร Basic Cybersecurity

จำนวนชั่วโมงการฝึกอบรม 1.30 ชั่วโมง

ให้ไว้ ณ วันที่ 18 กุมภาพันธ์ พ.ศ. 2569

(นายสมาสภ์ ปัทมะสุคนธ์)

อธิบดีกรมพัฒนาฝีมือแรงงาน

กรมพัฒนาฝีมือแรงงาน

ETDA

กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน

ร่วมกับ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วุฒิบัตรฉบับนี้ให้ไว้เพื่อแสดงว่า

นายเกษมสุข ศรีแย้ม

ได้ผ่านการฝึกทักษะออนไลน์

การสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต ETDA Digital Citizen Plus

จำนวนชั่วโมงการฝึกอบรม 3 ชั่วโมง 00 นาที

ให้ไว้ ณ วันที่ 18 กุมภาพันธ์ พ.ศ. 2569

(นายสมาสภ์ ปัทมะสุคนธ์)
อธิบดีกรมพัฒนาฝีมือแรงงาน

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สรุปบทเรียนเรื่อง Basic Cybersecurity

นายเกษมสุข ศรีแย้ม นักวิชาการเกษตรชำนาญการพิเศษ

เรื่อง Basic Cybersecurityความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ เป็นหลักสูตรและช่องทางการเรียนรู้ แบบ e - Learning เพื่อพัฒนาทักษะด้านดิจิทัล Cybersecurity ซึ่งสาระการเรียนรู้ในหลักสูตรถูกแบ่งออกเป็น 6 หัวข้อ มีรายละเอียดโดยสรุป ดังนี้

1. Basicsecurityการใช้งานบัญชีรายชื่อบุคคล

บัญชีรายชื่อบุคคล คือ ฐานข้อมูลที่สร้างขึ้นมาเพื่อจัดเก็บชื่อบุคคลที่จะเข้าไปใช้งานระบบและรหัสผ่าน สิ่งสำคัญที่สุดคือการใช้บัญชีแยกเฉพาะบุคคล ไม่ใช้ร่วมกัน ตั้งรหัสผ่านที่คาดเดาได้ยาก ไม่บอกผู้อื่น และต้องล๊อกเอาต์ (Log out) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่หน้าเครื่องเพื่อป้องกันการสวมสิทธิ์และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. Basicsecurityการป้องกันภัยคุกคามทางด้านไซเบอร์

การป้องกันภัยคุกคามทางไซเบอร์พื้นฐาน (Basicsecurity) คือการสร้างเกราะป้องกันข้อมูลและอุปกรณ์จากการโจมตี โดยเน้นที่การตั้งรหัสผ่านที่ซับซ้อนและไม่ซ้ำกัน การเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MFA) การอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ การติดตั้งโปรแกรมป้องกันไวรัส (Anti-malware) และความระมัดระวังในการใช้งานอินเทอร์เน็ตหรือคลิก link ที่น่าสงสัย

3. Basicsecurityป้องกันมัลแวร์

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่ายมีลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภทตัวอย่างเช่น

- Virus: มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- Worm: สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์
- Trojan: หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย
- Backdoor: เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว
- Rootkit: เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)
- Spyware: แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย
- Ransomware: ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

ข้อแนะนำในการป้องกันการติดมัลแวร์

1.อัพเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ

2.ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์

3.ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น USB ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน

4.ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ

5.ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่

6.หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใดๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

4. Basicsecurityการใช้อินเตอร์เน็ตอย่างปลอดภัย

คือการป้องกันข้อมูลส่วนบุคคลและอุปกรณ์จากภัยคุกคามไซเบอร์ โดยตั้งรหัสผ่านที่เดายากและไม่ซ้ำกัน, เปิดการยืนยันตัวตนแบบหลายปัจจัย (MFA), อัปเดตซอฟต์แวร์/Antivirus สม่ำเสมอ, หลีกเลี่ยง Wi-Fi สาธารณะ, ไม่คลิกลิงก์น่าสงสัย และตรวจสอบ URL เว็บไซต์ก่อนกรอกข้อมูลสำคัญ

5. Basicsecurityการใช้อินเตอร์เน็ตอย่างถูกต้อง

คือการป้องกันข้อมูลส่วนบุคคลและการใช้งานอุปกรณ์อย่างรู้เท่าทันภัยไซเบอร์ หลักปฏิบัติพื้นฐานประกอบด้วยการตั้งรหัสผ่านที่รัดกุม, อัปเดตซอฟต์แวร์สม่ำเสมอ, ระวังลิงก์แปลกปลอม (Phishing), ไม่เผยแพร่ข้อมูลส่วนตัว บนโซเชียล และตรวจสอบความน่าเชื่อถือของเว็บไซต์ก่อนทำธุรกรรม

6. Basicsecurityการป้องกันตนเองจากการฉ้อฉลจากไซเบอร์

แนวทางปฏิบัติเพื่อความปลอดภัยไซเบอร์ (Basic Security Tips)

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานการของแต่ละบุคคล
2. ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti Malware และมีการอัพเดทอย่างสม่ำเสมอ
4. มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดีและไม่บอก Password แก่ผู้อื่น

Password

1. การใช้ Password ที่ดีคือหนึ่งมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ตัวเลข และอักขระ พิเศษ
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. ความหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดา ได้ง่าย เช่น Password 1,2,3,4,5,6 วันเกิด และหมายเลขโทรศัพท์
4. มีการเปลี่ยน password อย่างสม่ำเสมอ

อีเมล์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เปิด Gmail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
3. ไม่คลิกลิงค์ใน E-mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆควรมีการเช็คผ่านเข้าทางอื่นๆเพิ่มเติม

เว็บไซต์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ได้เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจนเช่นการใช้งานช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆบนบราวเซอร์
3. เว็บไซต์สำหรับทำธุรการที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน https
4. ควรมีการอัพเดทเวอร์ชั่นของเราสม่ำเสมอ
5. ในกรณีเครื่องคอมพิวเตอร์ที่ไม่ใช่เรื่องส่วนตัวควรใช้งาน Browser ในโหมดเซฟเว็บ Save Web browsing
6. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น Google Chrome , mozilla Firefox เป็นต้น

Message สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง
3. มีความตระหนักก่อนเปิดลิงก์หรือฝ่ายต่างๆที่ได้รับมา
4. มีการ update Version ของโปรแกรมอย่างสม่ำเสมอ
5. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล Fake News ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมา เผยแพร่ดูมีความน่าเชื่อถือ ทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็ว มากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

1. มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกมาแนวการโฆษณา Conference

สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร์ข้อมูลต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ update Version ของโปรแกรม Conference อย่างสม่ำเสมอ Cloud storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าสู่ไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
5. มีการ update Version ในโปรแกรมอย่างสม่ำเสมอ 6. มีการตั้ง Password ที่ดีและมันบอก Password แก่ผู้อื่น

สรุปบทเรียน เรื่อง Basic Cybersecurity

นางสาวปานิสรา ทองท้วม นักวิชาการเกษตรชำนาญการ

เรื่อง Basic Cybersecurity ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ เป็นหลักสูตรและช่องทางการเรียนรู้ แบบ e - Learning เพื่อพัฒนาทักษะด้านดิจิทัล ที่จัดทำโดย กรมพัฒนาฝีมือแรงงาน จัดอยู่ในหมวดหมู่ Cybersecurity ซึ่งสาระการเรียนรู้ในหลักสูตรถูกแบ่งออกเป็น 6 หัวข้อ มีรายละเอียดโดยสรุป ดังนี้

1. Basicsecurity การใช้งานบัญชีรายชื่อบุคคล

บัญชีรายชื่อบุคคล คือ ฐานข้อมูลที่สร้างขึ้นมาเพื่อจัดเก็บชื่อบุคคลที่จะเข้าไปใช้งานระบบและรหัสผ่าน สิ่งสำคัญที่สุดคือการใช้บัญชีแยกเฉพาะบุคคลไม่ใช้ร่วมกัน ตั้งรหัสผ่านที่คาดเดาได้ยาก ไม่บอกผู้อื่น และต้องล๊อกเอาต์ (Log out) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่หน้าเครื่องเพื่อป้องกันการสวมสิทธิ์และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2. Basicsecurity การป้องกันภัยคุกคามทางด้านไซเบอร์

การป้องกันภัยคุกคามทางไซเบอร์พื้นฐาน (Basicsecurity) คือการสร้างเกราะป้องกันข้อมูลและอุปกรณ์จากการโจมตี โดยเน้นที่การตั้งรหัสผ่านที่ซับซ้อนและไม่ซ้ำกัน การเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MFA) การอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเสมอ การติดตั้งโปรแกรมป้องกันไวรัส (Anti-malware) และความระมัดระวังในการใช้งานอินเทอร์เน็ตหรือคลิก link ที่น่าสงสัย

3. Basicsecurity ป้องกันมัลแวร์

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย มีลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท ตัวอย่างเช่น

Virus: มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

Worm: สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

Trojan: หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย

Backdoor: เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว

Rootkit: เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่องพร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

Spyware: แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย

Ransomware: ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

ข้อแนะนำในการป้องกันการติดมัลแวร์

- อัพเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
- ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
- ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น USB ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
- ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
- ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่
- หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใดๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

4. Basicsecurity การใช้อินเตอร์เน็ตอย่างปลอดภัย

คือการป้องกันข้อมูลส่วนบุคคลและอุปกรณ์จากภัยคุกคามไซเบอร์ โดยตั้งรหัสผ่านที่เดายากและไม่ซ้ำกัน, เปิดการยืนยันตัวตนแบบหลายปัจจัย (MFA), อัปเดตซอฟต์แวร์/Antivirus สม่ำเสมอ, หลีกเลี่ยง Wi-Fi สาธารณะ, ไม่คลิกลิงก์น่าสงสัย และตรวจสอบ URL เว็บไซต์ก่อนกรอกข้อมูลสำคัญ

5. Basicsecurity การใช้อินเตอร์เน็ตอย่างถูกต้อง

คือการป้องกันข้อมูลส่วนบุคคลและการใช้งานอุปกรณ์อย่างรู้เท่าทันภัยไซเบอร์ หลักปฏิบัติพื้นฐานประกอบด้วย การตั้งรหัสผ่านที่รัดกุม, อัปเดตซอฟต์แวร์สม่ำเสมอ, ระวังลิงก์แปลกปลอม (Phishing), ไม่เผยแพร่ข้อมูลส่วนตัว บนโซเชียล และตรวจสอบความน่าเชื่อถือของเว็บไซต์ก่อนทำธุรกรรม

6. Basicsecurity การป้องกันตนเองจากการฉ้อฉลจากไซเบอร์

แนวทางปฏิบัติเพื่อความปลอดภัยไซเบอร์ (Basic Security Tips)

- จัดการรหัสผ่าน: ใช้รหัสผ่านที่เข้มแข็ง
- ระวังการคลิก/ดาวน์โหลด: ไม่คลิกลิงก์ (Link) หรือดาวน์โหลดไฟล์แนบจากอีเมล, SMS หรือแชทที่ไม่รู้จักหรือไม่น่าเชื่อถือ เพราะอาจเป็นฟิชชิ่ง (Phishing) หรือมัลแวร์
- อัปเดตเสมอ: อัปเดตระบบปฏิบัติการ (OS) และแอปพลิเคชันให้เป็นเวอร์ชันล่าสุด
- ยืนยันตัวตน 2 ขั้นตอน (2FA/MFA): ด้วยการล็อกอินร่วมกับรหัส OTP หรือแอปยืนยันตัวตน
- ปกป้องข้อมูล
  ส่วนตัว: ไม่เปิดเผยข้อมูลส่วนตัวแก่บุคคลที่ไม่จำเป็นหรือแอบอ้างเป็นเจ้าหน้าที่
- ป้องกันอุปกรณ์: ติดตั้งโปรแกรมป้องกันไวรัส ล็อคหน้าจออุปกรณ์และใช้รหัสผ่าน/PIN ในการเข้าใช้งานเสมอ
- สำรองข้อมูล: ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอเพื่อป้องกัน Ransomware หรือข้อมูลสูญหาย
- ปลอดภัยจากการเชื่อมต่อ: หลีกเลี่ยงการใช้ Wi-Fi สาธารณะ (Free Wi-Fi) ในการทำธุรกรรมการเงิน