เฉลยหน่วยที่ 7 ความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

ตอนที่ 1 จงทำเครื่องหมายกากบาท (X) ลงหน้าข้อที่ถูกต้องที่สุด

1. สภาพโทรคมนาคมระหว่างประเทศมีชื่อย่อว่าอะไร

ข. ITU

2. เทคโนโลยีใดที่ผู้ประกอบการนำมาช่วยวิเคราะห์ธุรกิจและภัยคุกคาม

ก. อนาไลติกส์

3. Network หมายถึงข้อใด

ค. เครือข่าย

4. การฝึกอบรมพนักงานเป็นการป้องกันด้านความปลอดภัยส่วนใด

ง. ระเบียบปฏิบัติ

5. การตรวจสอบว่าไฟล์นั้นถูกแก้ไขเปลี่ยนแปลงได้เป็นหลักในการรักษาความมั่นคงปลอดภัยข้อใด

จ. การรักษาความพร้อมใช้

6. แนวทางการบริหารจัดการความมั่นคงปลอดภัยแบ่งออกเป็นกี่ส่วน

ก. 2 ส่วน

7. Login หมายถึงข้อใด

ค. การเข้าสู่ระบบ

8. การใช้รหัสผ่านเมื่อเข้าใช้งานเป็นการรักษาความปลอดภัยแบบใด

ก. การระบุตัวตน

9. การเก็บรายงานการเข้าใช้งานเป็นการรักษาความปลอดภัยแบบใด

ง. การตรวจสอบได้

10. การลบไฟล์ข้อมูล เป็นภัยคุกคามด้านความมั่นคงปลอดภัยข้อใด

ค. การขัดจังหวะ

ตอนที่ 2 จงจับคู่ข้อความต่อไปนี้ให้สัมพันธ์กัน

1. ……**G**…… ความปลอดภัยทางไซเบอร์
2. ……**K**…… การรักษาความลับ
3. ……**I**……. การรักษาความครบถ้วนสมบูรณ์
4. ……**A**…… การป้องกัน
5. ……**M**……การตรวจสอบ
6. ……**B**…….การระบุตัวตน
7. ……**E**…… การตรวจสอบได้
8. ……**C**…… ภัยคุกคาม
9. ……**F**……. การดัดแปลงแก้ไข
10. … **L**……. วิทยาการรหัสลับ

A. Prevention
B. Identification
C. Threat
D. Fabrication
E. Accountability
F. Modification
G. Cyber Security
H. Interruption
I. Integrity
J. Authentication
K. Confidentiality

ตอนที่ 3 **จงตอบคำถามต่อไปนี้ให้ได้ใจความสมบูรณ์**

1. อธิบายปัจจัยที่สำคัญของ Digital Security

ตอบ ปัจจัยที่สำคัญของ Digital Security คือ

1. บุคลากร (Personal) องค์กรจะต้องมีบุคลากรที่มีประสบการณ์และมีความเชี่ยวชาญ มีความสามารถในด้านความปลอดภัยสูง โดยต้องอยู่ภายใต้การรับรองของหน่วยงานสากลหรือ Certificate

2. เครื่องมือ (Tool) การเลือกใช้อุปกรณ์ดิจิทัลและซอฟต์แวร์ที่ทันสมัยได้รับการยอมรับแล้วว่าสามารถป้องกันและมีความแม่นยำในการวิเคราะห์ภัยคุกคาม สามารถป้องกันการโจมตีเฟิร์มแวร์ ซึ่งเป็นภัยใหญ่ที่สุดในองค์กรได้อย่างมีประสิทธิภาพ

2. อธิบายโครงสร้างพื้นฐานระบบเครือข่าย

ตอบ

โครงสร้างพื้นฐานระบบเครือข่าย (Network) เป็นการทำธุรกรรมดิจิทัลในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่ายการรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และมักเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต แม้ว่าจะการเชื่อมต่อกันดังที่ได้กล่าวมาจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจากระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่าย ยิ่งมีขนาดมากเท่าไร ย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตี และเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้น

3. อธิบายความหมายของการรักษาความลับ

ตอบ

การรักษาความลับ (Confidentiality) หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะ ผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้น ๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญ เช่น ข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ข้อมูลส่วนบุคคลอื่น ๆ เช่น หมายเลขประจำตัวประชาชน กำหนดการของบุคคลสำคัญ รายชื่อผู้โดยสารของเที่ยวบินต่าง ๆ เป็นต้น

4. อธิบายความหมายของการรักษาความครบถ้วนสมบูรณ์

ตอบ **การรักษาความครบถ้วนสมบูรณ์ (Integrity)** หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของการทำธุรกรรมดิจิทัลที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความถูกต้องสมบูรณ์ และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้ เช่น หากมีการแก้ไขไฟล์ที่ถูกสร้างขึ้นแล้วมีการส่งผ่านไฟล์นั้นเข้าสู่เครือข่ายคอมพิวเตอร์ ผู้ที่เกี่ยวข้องจะต้องสามารถตรวจสอบได้ว่าไฟล์นั้นว่าถูกแก้ไขเปลี่ยนแปลงไประหว่างการส่งผ่านช่องทางการสื่อสารหรือไม่ เป็นต้น

5. อธิบายความหมายการรักษาความพร้อมใช้

ตอบ **การรักษาความพร้อมใช้ (Availability)** หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของข้อมูลในการทำธุรกรรมที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้น ๆ สามารถเข้าใช้งานได้ เช่น เมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์ อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น

6. อธิบายแนวทางบริหารจัดการความมั่นคงปลอดภัย

ตอบ

แนวทางบริหารจัดการความมั่นคงปลอดภัย ได้แก่

1. การป้องกัน (Prevention) การป้องกันนี้มีจุดมุ่งหมายคือ การรักษาข้อมูลมีให้ผู้ที่ไม่มีสิทธิในการใช้งานข้อมูล สามารถเข้ามาใช้ข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการป้องกันแบบนี้จะเป็นแบบการพิสูจน์ตัวตนก่อนการเข้าใช้งานในส่วนต่าง ๆ ของระบบ หรือข้อมูล ซึ่งวิธีการแบบนี้เป็นวิธีที่นิยมใช้กันอยู่ในลำดับต้น ๆ กฎการเข้าใช้งาน เมื่อเข้าใช้งานระบบ ต้องมีการเข้าสู่ระบบ (Login) ต้องใช้ชื่อผู้ที่มีอยู่ในระบบและรหัสผ่าน ถ้าผู้ใช้งานใดไม่มีสิทธิก็จะไม่สามารถเข้าใช้งานในส่วนนั้นได้

2. การตรวจสอบ (Detection) การตรวจสอบของข้อมูลนี้ เป็นการตรวจสอบข้อมูลต่าง ๆ ภายในระบบว่ามีการแก้ไขแล้วหรือไม่ ซึ่งข้อมูลที่มีการเปลี่ยนแปลงไปจากเดิม เช่น การแก้ไข การเพิ่ม ซึ่งถ้าตรวจสอบแล้วว่าข้อมูลนั้นถูกเปลี่ยนแปลงไปจะไม่มีความเชื่อถือของข้อมูล เมื่อจะนำมาวิเคราะห์ในเรื่องต่าง ๆ

7. อธิบายการรักษาความปลอดภัยของข้อมูลในการทำธุรกิจดิจิทัล

ตอบ

การรักษาความปลอดภัยของข้อมูลในการทำธุรกิจดิจิทัล ได้แก่

1. การระบุตัวตน (Identification) ภายในระบบสารสนเทศนั้นต้องมีการระบุตัวตนภายในตัวระบบได้ ในการระบุตัวตนนี้เป็นขั้นตอนแรกก่อนจะเข้าถึงข้อมูลชั้นความลับ และเป็นพื้นฐานขั้นตอนต่อไปในการพิสูจน์ตัวตน (Authentication) และการพิสูจน์สิทธิ์ (Authorization) เช่น การเข้าใช้งานเว็บไซต์ จะเห็นว่ามีการให้กรองชื่อผู้ใช้ และรหัสผ่านเข้าใช้งาน โดยสิทธิ์ในการเข้าถึงข้อมูลก็จะแตกต่างกันออกเป็นตามชื่อผู้ใช้งานนั้น ๆ

2. การพิสูจน์ทราบตัวตน (Authentication) การที่ระบบจะบอกได้ว่าเมื่อผู้ใช้งานนั้นทำการเข้าระบบมาแล้ว ว่าชื่อผู้ใช้งานนั้นมีรหัสผ่านตรงกับชื่อผู้ใช้งานภายในระบบหรือไม่ หรือจะเป็นคำถามเมื่อสมัครสมาชิกไว้แต่ตอนต้นแล้วเมื่อลืมรหัสผ่าน ระบบก็จะทำการให้ตอบคำถามซึ่งเป็นการระบุตัวตนได้เช่นกัน

3. การอนุญาตใช้งาน (Authorization) เมื่อผ่านขั้นตอนข้างต้นมาแล้ว ในส่วนนี้จะเป็นการที่ชื่อผู้ใช้งานแต่ละคนมีสิทธิในการเข้าถึงข้อมูลในส่วนต่าง ๆ โดยสิทธิการเข้าถึงข้อมูลนั้นจะแตกต่างกันออกไป เช่น สิทธิการเข้าใช้งานระบบฐานข้อมูล ผู้ใช้ธรรมดาย่อมมีสิทธิได้แค่ดูอย่างเดียว หรือเว้นแต่ผู้ดูแลระบบจะมอบสิทธิให้แต่ผู้ดูแลระบบจะสามารถสร้างลบ แก้ไขฐานข้อมูลได้

4. การตรวจสอบได้ (Accountability) โดยการตรวจสอบระบบได้นี้ในกรณีที่ผู้ใช้งานเข้าสู่ระบบแล้ว ทางระบบจะมีการเก็บการเข้าใช้งานภายในระบบ (logs) เพื่อตรวจสอบได้ว่าผู้ใดเข้ามาใช้งานภายในระบบบ้าง

8. อธิบายความหมายของการดักรับ

ตอบ

การดักรับ (Interception) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์อย่างถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (Sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง

9. อธิบายความหมายของไฟร์วอลล์

ตอบ

ไฟร์วอลล์ (Firewall) เป็นเทคโนโลยีที่ถูกสร้างขึ้นเพื่อป้องกันภัยคุกคามและการโจมตีทางเครือข่าย หลักทั่วไปของการใช้งานไฟร์วอลล์คือ การป้องกันภัยคุกคามที่มาจากภายนอก (ซึ่งอาจหมายถึงเครือข่ายภายนอก หรือเครือข่ายที่เครื่องคอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งเชื่อมต่อด้วยก็ได้) สามารถจำแนกชนิดของไฟร์วอลล์ตามลักษณะการใช้งานได้สองลักษณะ คือ ไฟร์วอลล์สำหรับเครือข่าย (Network firewall) และไฟล์วอลล์ส่วนบุคคล (Personal firewall)

10. อธิบายข้อควรระวังในการทำธุรกรรมดิจิทัล

ตอบ ข้อควรระวังในการทำธุรกรรมดิจิทัล ได้แก่

1. ความมั่นคงปลอดภัยออนไลน์ (Online Security) เมื่อตัดสินใจทำธุรกิจผ่านโลกออนไลน์ คุณต้องรอบรู้เรื่องภัยคุกคามต่าง ๆ ที่จะตามมาด้วยเช่นกัน ไม่ว่าจะเป็นมัลแวร์ ฟิชชิง การแฮก หรือสแปมเมล พร้อมหาวิธีป้องกันภัยคุกคามเหล่านี้ และตรวจสอบให้แน่ใจว่า คุณได้อัปเดตระบบปฏิบัติการของแพลตฟอร์มอย่างสม่ำเสมอ รวมทั้งใช้ SSL (Secure Sockets Layer) ที่แข็งแกร่งพอ

2. ความน่าเชื่อถือของระบบ (System Reliability) เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต (ISP) อาจล่ม ระบบเพย์เมนต์ออนไลน์อาจเกิดข้อผิดพลาด หรือโปรแกรมอีคอมเมิร์ซปลั๊กอินอาจเกิดข้อบกพร่องบางอย่าง แต่คุณสามารถอัปเดตระบบปฏิบัติการและ APIs ทั้งหมดของคุณได้ มีแค่บางสิ่งเท่านั้นที่อยู่นอกเหนือการควบคุมของคุณ

3. ประเด็นเรื่องความเป็นส่วนตัว ข้อมูลส่วนตัวของลูกค้าอาจถูกล้วง เพื่อนำไปใช้ประโยชน์ในทางที่มิชอบ เช่น การส่งสแปม การนำไปสวมรอย หรือการทำตลาดที่ไม่พึงประสงค์ ดังนั้น นอกจากมาตรการในเรื่องความมั่นคงปลอดภัยออนไลน์แล้ว ต้องมั่นใจด้วยว่าลูกค้าได้ใช้พาสเวิร์ดที่แข็งแกร่ง

4. ข้อพิพาทหรือร้องเรียนของลูกค้า เขาอาจไม่ได้รับสินค้า บัตรเครดิตถูกชาร์จเพิ่มเป็นสองเท่า หรือสินค้าที่ได้รับไม่ตรงตามรายละเอียดบนออนไลน์ ซึ่งไม่ว่าลูกค้าจะถูกหรือไม่ก็ตาม สิ่งสำคัญคือต้องให้บริการลูกค้าที่ดีเยี่ยมอยู่เสมอ ตลอดจนแก้ไขข้อผิดพลาดที่เป็นไปได้ทั้งหมดที่เกิดขึ้น เพื่อให้ลูกค้าของคุณรู้สึกพึงพอใจและกลับมาอุดหนุนคุณต่อไป

5. การฉ้อโกงบัตรเครดิต อาจมีโจรขโมยบัตรเครดิตมาใช้สั่งซื้อสินค้า หรือแฮกเกอร์อาจขโมยข้อมูลเครดิตลูกค้าในระบบของเราไป ไม่ว่ามาตรการรักษาความมั่นคงปลอดภัยของคุณจะดีเพียงใดก็ตาม ให้ระวังการทำธุรกรรมที่น่าสงสัยอยู่เสมอ

6. ทรัพย์สินทางปัญญา รูปภาพ คำอธิบายผลิตภัณฑ์ต่าง ๆ แม้กระทั่งโลโก้ คลิป ดนตรี รวมทั้งผลิตภัณฑ์ของคุณ อาจถูกคนอื่นก๊อปปี้ หรือคุณอาจไปละเมิดทรัพย์สินทางปัญญาของผู้อื่น ดังนั้น จึงควรตรวจสอบความถูกต้องอยู่เสมอ หากจำเป็นต้องใช้สิ่งต่าง ๆ ข้างต้น ต้องได้รับอนุญาตจากเจ้าของลิขสิทธิ์แล้วเท่านั้น

7. SEO (Search Engine Optimization) กูเกิลหรือแพลตฟอร์มอื่น ๆ สามารถปรับแต่งอัลกอริทึมได้ทุกเมื่อ และทำให้เกิดผลกระทบต่อทราฟฟิกในการเข้าถึงเว็บไซต์ของคุณ อาจทำให้เว็บไซต์ของคุณมีการเข้าถึงลดลงอย่างมีนัยสำคัญในชั่วข้ามคืน ดังนั้น การมีคอนเทนต์ที่แข็งแกร่งและอัปเดตเว็บไซต์ของคุณอย่างสม่ำเสมอจะช่วยคุณได้มาก

8. ภาษีอากร คุณอาจไม่ได้รวมภาษีการขายที่เหมาะสมกับยอดขายของคุณ หรือไม่ได้เผื่อค่าจัดส่งและภาษีนำเข้าตามสถานที่จัดส่งของคุณไป ดังนั้น จึงควรตรวจสอบเรื่องภาษีให้ดี เพราะหากเกิดข้อผิดพลาดอาจทำให้คุณต้องเสียภาษีรวบยอดยกใหญ่เลยทีเดียว

9. การคืนสินค้าและการรับประกัน เรื่องปวดเศียรเวียนเกล้าในการจัดการกับเรื่องการคืนสินค้า ซึ่งเพิ่มค่าใช้จ่ายในระบบจัดการซัปพลายเชน และไม่สามารถนำสินค้าที่รับคืนมาขายใหม่ในราคาเดิมได้ ดังนั้นคุณจึงต้องมีการคิดเผื่อต้นทุนของค่าใช้จ่ายส่วนนี้ที่อาจเพิ่มขึ้นด้วย

10. ระบบคลังสินค้าและโลจิสติกส์ สินค้าในสต๊อกของคุณอาจจะหมดในขณะที่คำสั่งซื้อเข้ามา จึงทำให้การจัดส่งผลิตภัณฑ์ล่าช้า หรือการส่งสินค้าไปยังผู้รับที่ไม่ถูกต้อง ดังนั้น จึงควรหมั่นตรวจสินค้าในสต๊อกและเช็กรายละเอียดในการจัดส่งอย่างถี่ถ้วนก่อนส่งสินค้าออกไป
