ภาคผนวก

ภาคผนวก ก.

แนวปฏิบัติเมื่อเกิดฟิชชิ่งกับ Web Server ขององค์กร

วัตถุประสงค์

๑. เพื่อกำหนดมาตรการในการแก้ไขปัญหาการเกิดฟิชชิ่ง (Phishing) ให้สามารถดำเนินการได้อย่างรวดเร็ว ไม่ให้เกิดความเสียหายและส่งผลกระทบต่อองค์กรทั้งภายในและภายนอกที่ใช้งานระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบ

ข้อ ๑ เมื่อผู้ดูแลระบบได้รับแจ้ง หรือตรวจพบว่า Web Server ขององค์กร ณ จุดผู้ใช้งานใดเป็นช่องทางทำให้ผู้ไม่หวังดีทำฟิชชิ่ง (Phishing) ผู้ดูแลระบบจะดำเนินการ ดังนี้

(๑) ดำเนินการบล็อค IP Address ของ Web Server ที่โดนฟิชชิ่งหรือแจ้งผู้ให้บริการเส้นทางเครือข่ายขององค์กรดำเนินการในส่วนที่เกี่ยวข้องโดยเร่งด่วน

(๒) แจ้งผู้ดูแล Web Server ขององค์กรที่ถูกทำฟิชชิ่ง ทางจดหมายอิเล็กทรอนิกส์ (e-Mail) หรือทางโทรศัพท์ เพื่อให้ดำเนินการแก้ไขปัญหา

ข้อ ๒ เมื่อองค์กรดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว ให้ประสานไปยังผู้ดูแลระบบเครือข่ายขององค์กรหรือผู้ให้บริการเส้นทางเครือข่ายขององค์กร เพื่อปลดบล็อค IP Address

ข้อ ๓ ผู้ดูแลระบบ Web Server ขององค์กร ต้องหมั่นตรวจสอบ Web Server และเว็บไซต์ รวมทั้งติดตั้งโปรแกรมปรับปรุงช่องโหว่ (Patch) อย่างสม่ำเสมอ เพื่อป้องกันผู้ที่ไม่หวังดีเข้ามาทำฟิชชิ่ง