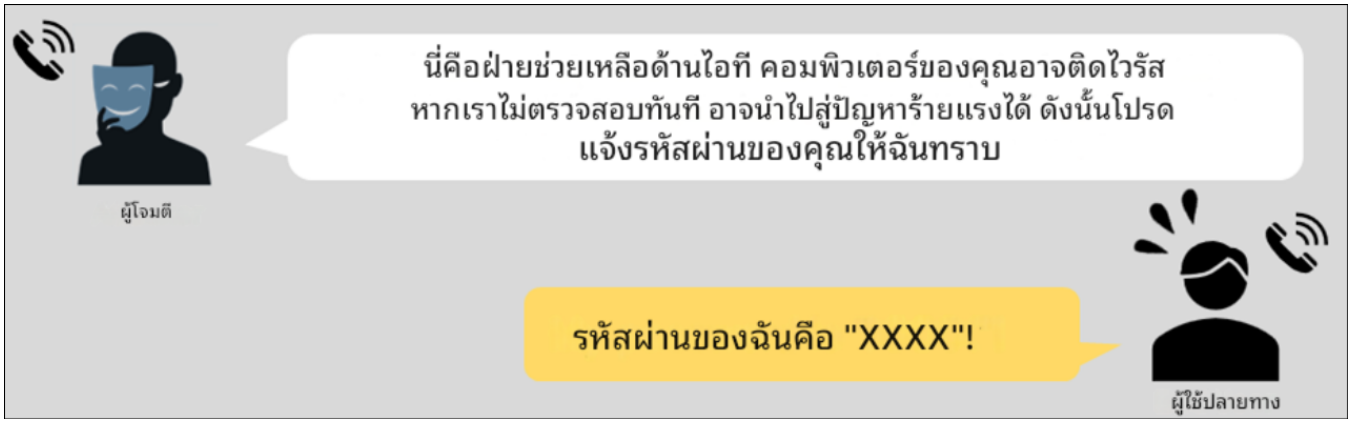
จดหมายข่าวความปลอดภัยของข้อมูล

Vol1 Social Engineering

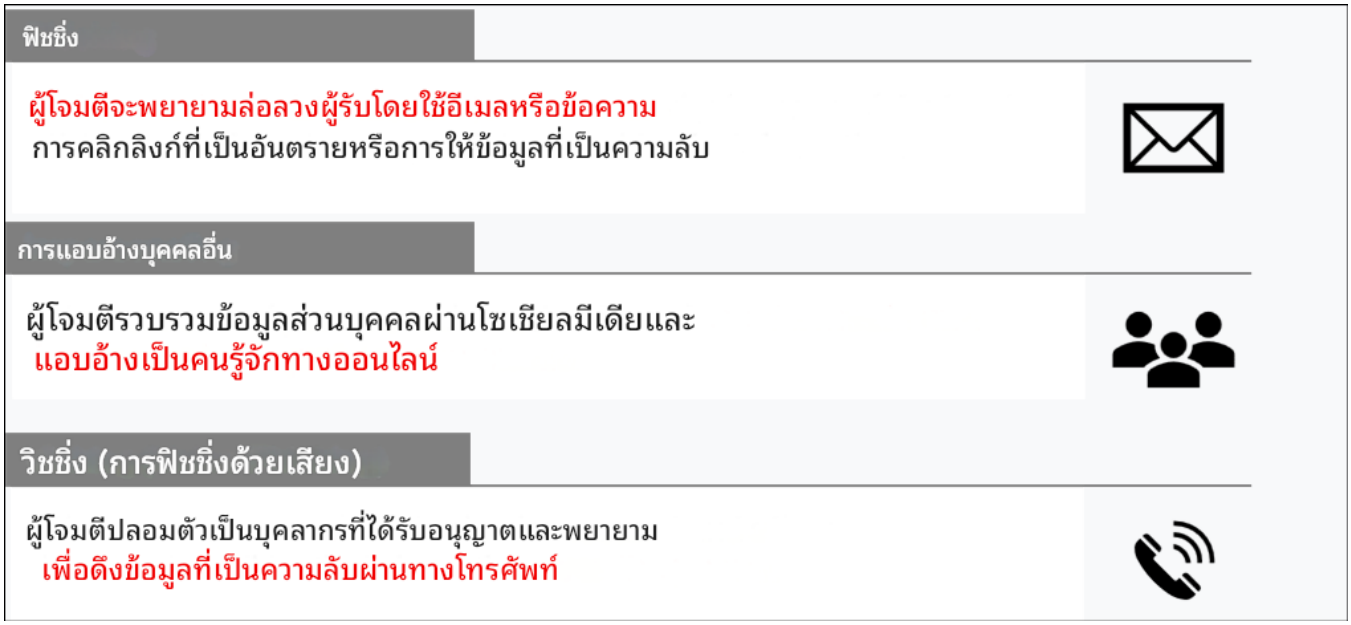


วิศวกรรมสังคม (Social Engineering) คืออะไร?

วิศวกรรมสังคม หมายถึง เทคนิคหลากหลายรูปแบบที่ใช้ในการหลอกลวงบุคคล หรือใช้ประโยชน์จากธรรมชาติและสัญชาตญาณของมนุษย์ วิธีการโจมตีแบบดั้งเดิมบางวิธีได้พัฒนาเป็นรูปแบบของ "อาชญากรรมไซเบอร์" ที่ดำเนินการผ่านแพลตฟอร์มออนไลน์ อีเมล หรือโซเชียลมีเดีย เนื่องจากวิศวกรรมสังคมไม่สามารถป้องกันได้ด้วยมาตรการทางเทคนิค เช่น ซอฟต์แวร์ป้องกันไวรัสหรือไฟร์วอลล์ จึงจำเป็นต้องใช้การป้องกันที่อาศัยบุคคลเป็นหลัก

กลยุทธ์ของผู้โจมตี

มีเทคนิคมากมายที่ใช้ในวิศวกรรมสังคม ตัวอย่างเช่น



วิศวกรรมสังคม

ผู้โจมตีจะเข้าเยี่ยมชมสถานที่ทำงานที่เป็นเป้าหมายและ
ปลอมตัวเป็นบุคคลที่มีตัวตนปลอม เช่น ผู้ขาย ผู้รับเหมาช่วง
ผู้หางาน พนักงาน หรือ นักท่องเที่ยว เพื่อขโมยข้อมูลที่เป็นความลับ

การตัดหาง

ผู้โจมตีพยายามหลบหนีผ่านทางเข้าที่ล็อกไว้โดยการ
ติดตามคนที่กำลังเข้ามา ตัวอย่างเช่น พวกเขาอาจ
แกล้งทำบัตรรักษาความปลอดภัยหายและขอให้ใครบางคนเปิด
ประตูให้

การแฮ็กไหล่

ผู้โจมตีแอบมองข้ามไหล่ของบุคคลเพื่อดูหน้าจอและ
ขโมยข้อมูลสำคัญ เช่น รหัสประจำตัวและรหัสผ่าน นอกจากการ
สังเกตด้วยตาแล้ว พวกเขายังอาจใช้กล้องเพื่อบันทึกและ
ขโมยข้อมูลอย่างลับๆ อีกด้วย

การทิ้งขยะ

ผู้โจมตีขโมยข้อมูลลับโดยการดึงบันทึกหรือกระดาษโน้ตที่
มีข้อมูลส่วนบุคคลจากถังขยะ มีกลยุทธ์หลากหลาย เช่น การ
ปลอมตัวเป็นภารโรงหรือพนักงานเก็บขยะ ดังนั้น แม้แต่เอกสารที่
ตั้งใจจะนำไปดำเนินการละลายก็อาจมีความเสี่ยงหากไม่ได้รับการจัดเก็บ
อย่างเหมาะสมก่อนการกำจัด

มาตรการส่วนบุคคล

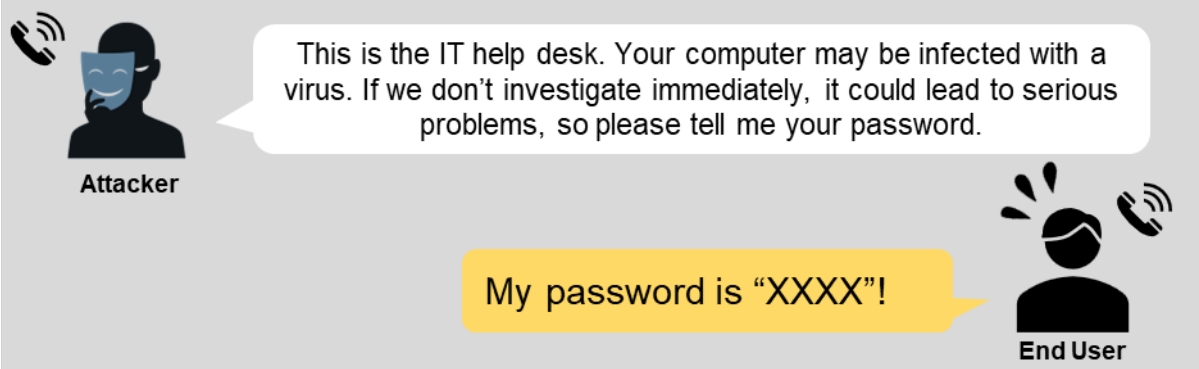
เพื่อป้องกันไม่ให้ตกเป็นเหยื่อของวิศวกรรมสังคม ทุกคนควรให้ความสำคัญกับประเด็นดังต่อไปนี้:

- อย่าเปิดไฟล์แนบหรือลิงก์ในอีเมลที่น่าสงสัย
- หากคุณได้รับสายโทรศัพท์ที่น่าสงสัยซึ่งพยายามจะดึงข้อมูล
  พนักงาน ให้วางสายทันทีและรายงานให้หัวหน้างานของคุณทราบ
- อย่าให้ยืมบัตรรักษาความปลอดภัยของคุณแก่ใครก็ตาม และอย่าเปิดประตูให้
  กับบุคคลที่ไม่มีบัตรรักษาความปลอดภัย
- เมื่อต้องทำงานนอกสำนักงาน ควรหลีกเลี่ยงการปฏิบัติงานในที่
  สาธารณะ
- เมื่อนำอุปกรณ์ออกไปนอกสำนักงาน ควรระวังความเสี่ยง เช่น การโจรกรรม
- กำจัดเอกสารลับโดยใช้กระบวนการละลายหรือเครื่องทำลายเอกสาร

【ข้อมูลติดต่อสอบถาม】
ฝ่ายเลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (กองเทคโนโลยีสารสนเทศ แผนกระบบสารสนเทศ ส่วนที่ 2)
อีเมล์ securitylearning@fanuc.co.jp

Information Security Newsletter

Vol1 Social Engineering



What is Social Engineering?

Social engineering refers to a wide range of techniques that deceive people or exploit human nature and instincts.
Some traditional attack methods have evolved into forms of "cybercrime" carried out through online platforms, email, or social media.
Since social engineering **cannot be prevented by technical measures such as antivirus software or firewalls**, human-based defense is required.

Attacker's Tactics

There are various techniques used in social engineering. Here are some examples.

Phishing

Using emails or text messages, attackers try to lure recipients into clicking malicious links or providing confidential information.

Impersonating

Attackers collect personal information through **social media and impersonate acquaintances online.**

Vishing (Voice-Phishing)

Attackers impersonate authorized personnel and attempt to extract confidential information **over the phone.**

Social Engineering

Attackers visit targeted workplaces and **pose as someone with a false identity**—such as a vendor, subcontractor, job seeker, employee, or tourist—to steal confidential information.

Tailgating

Attackers try to **slip through locked entrances by following someone** who is entering. For example, they may pretend to have lost their security card and ask someone to open the door for them to gain access.

Shoulder Hacking

Attackers **secretly look over a person's shoulder to view their screen** and steal sensitive information such as IDs and passwords. In addition to directly observing with their eyes, they may also use cameras to surreptitiously record and obtain the information.

Trashing

Attackers **steal confidential information** by retrieving memos or sticky notes containing personal information **from trash bins**. There are various tactics, such as impersonating janitors or waste collection staff, so even documents intended for dissolution processing can pose a risk if not properly stored before disposal.

Individual Measures

To prevent falling victim to social engineering, everyone should pay attention to the following points.

- Do not open suspicious email attachments or links.
- If you receive a suspicious phone call attempting to extract employee information, hang up immediately and report it to your supervisor.
- Do not lend your security card to anyone, and do not open doors for individuals who do not have a security card.
- When working outside the office, avoid performing tasks in public places.
- When taking a device outside the office, be cautious of risks such as theft.
- Dispose of confidential documents using dissolution processing or a shredder.

【Inquiry】
Information Security Committee Secretariat
(IT Division information System Department Section 2)
securitylearning@fanuc.co.jp