



จดหมายข่าวความปลอดภัยของข้อมูล



Vol1 Social Engineering



ผู้โจมตี

นี่คือฝ่ายช่วยเหลือด้านในอีก คอมพิวเตอร์ของคุณอาจติดไวรัส หากเราไม่ตรวจสอบกันที่อาจนำไปสู่ปัญหาร้ายแรงได้ ดังนั้นโปรดแจ้งรหัสผ่านของคุณให้ฉันทราบ



ผู้ใช้ปลายทาง

รหัสผ่านของฉันคือ "XXXX"!

วิศวกรรมลังแคม (Social Engineering) คืออะไร?

วิศวกรรมลังแคม หมายถึง เทคนิคหลอกลวงแบบที่ใช้ในการหลอกลวงบุคคล หรือใช้ประโยชน์จากการชรุ่มชาติและสูญชาตญาณของมนุษย์ วิธีการโจรกรรมแบบดังเดิมบางวิธีได้พัฒนาเป็นรูปแบบของ "อาชญากรรมไซเบอร์" ที่ดำเนินการผ่านแพลตฟอร์มออนไลน์ อีเมล หรือโซเชียลมีเดีย เป็นต้น จุดประสงค์ของการลังแคมไม่สามารถบังคับได้ด้วยมาตรการทางเทคนิค เช่น ซอฟต์แวร์บังคับกันไวรัสหรือไฟร์วอลล์ จึงจำเป็นต้องใช้การบังคับกันที่อาศัยบุคคลเป็นหลัก

กลยุทธ์ของผู้โจมตี

มีเทคนิคமากมายที่ใช้ในวิศวกรรมลังแคม ตัวอย่างเช่น

พิชชิ่ง

ผู้โจมตีจะพยายามล่อลงผู้รับโดยใช้อีเมลหรือข้อความ



การคลิกลิงก์ที่เป็นอันตรายหรือการให้ข้อมูลที่เป็นความลับ

การแอบอ้างบุคคลอื่น

ผู้โจมตีรวมข้อมูลส่วนบุคคลผ่านโซเชียลมีเดียและ
แอบอ้างเป็นคนรู้จักทางออนไลน์



วิชชิ่ง (การพิชชิ่งด้วยเสียง)

ผู้โจมตีปลอมตัวเป็นบุคลากรที่ได้รับอนุญาตและพยายาม
เพื่อดึงข้อมูลที่เป็นความลับผ่านทางโทรศัพท์



วิศวกรรมสังคม

ผู้โจนตีจะเข้าเยี่ยมชมสถานที่ทำงานที่เป็นเป้าหมายและ
ปลอมตัวเป็นบุคคลที่มีตัวตนปลอม เช่น ผู้ขาย ผู้รับเหมาช่าง
ผู้ทำงาน พนักงาน หรือ นักท่องเที่ยว เพื่อบโนยข้อมูลที่เป็นความลับ



การตัดทาง

ผู้โจนตีพยาามหลบหนีผ่านทางเข้าที่ล็อกไว้โดยการ
ติดตามคนที่กำลังเข้ามา ตัวอย่างเช่น พวกรabeาอาจ
กลังทำบัตรรักษาความปลอดภัยหายและขอให้ครบรากคนเปิด
ประตูให้



การแยกไฟล์

ผู้โจนตีแอบนมองข้ามไฟล์ของบุคคลเพื่อดูหน้าจอและ
บโนยข้อมูลสำคัญ เช่น รหัสประจำตัวและรหัสผ่าน นอกจากรา
สังเกตด้วยตาแล้ว พวกรabeาอาจใช้กล้องเพื่อบันทึกและ
บโนยข้อมูลอย่างลับๆ อีกด้วย



การทิ้งขยะ

ผู้โจนตีบบโนยข้อมูลลับโดยการดึงบันทึกหรือกระดาษโน๊ตที่
มีข้อมูลส่วนบุคคลจากถังขยะ มีกลยุทธ์หลากหลาย เช่น การ
ปลอมตัวเป็นภรรยาพนักงานเก็บขยะ ดังนั้น แม้แต่เอกสารที่
ตั้งใจจะนำไปดำเนินการละลายก็อาจมีความเสี่ยงหากไม่ได้รับการจัดเก็บ
อย่างเหมาะสมก่อนการกำจัด



มาตรการส่วนบุคคล

เพื่อป้องกันไม่ให้ตกเป็นเหยื่อของวิศวกรรมสังคม ทุกคนควรให้ความสำคัญกับประเด็นดังต่อไปนี้:

- อย่าเปิดไฟล์แนบหรือลิงก์ในอีเมลที่น่าสงสัย
- หากคุณได้รับสายโทรศัพท์ที่น่าสงสัยซึ่งพยายามจะดึงข้อมูล
พนักงาน ให้ห่วงสายทันทีและรายงานให้หัวหน้างานของคุณทราบ
- อย่าให้ยืมบัตรรักษาความปลอดภัยของคุณแก่ใครก็ตาม และอย่าเปิดประตูให้
กับบุคคลที่ไม่มีบัตรรักษาความปลอดภัย
- เมื่อต้องทำงานนอกสำนักงาน ควรหลีกเลี่ยงการปฏิบัติงานในที่
สาธารณะ
- เมื่อนำอุปกรณ์ออกไปนอกสำนักงาน ควรระมัดระวังความเสี่ยง เช่น การโจรมรร
- กำจัดเอกสารลับโดยใช้กระบวนการลบรากหรือเครื่องกำลากเอกสาร

【ข้อมูลติดต่อสอบถาม】

ผู้เลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (กองเทคโนโลยีสารสนเทศ แผนกรระบบสารสนเทศ ส่วนที่ 2)

อีเมล securitylearning@fanuc.co.jp



Vol1 Social Engineering



Attacker

This is the IT help desk. Your computer may be infected with a virus. If we don't investigate immediately, it could lead to serious problems, so please tell me your password.



My password is “XXXX”!

End User

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】

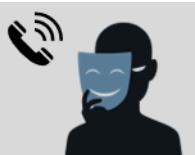
Information Security Committee Secretariat
(IT Division information System Department Section 2)
securitylearning@fanuc.co.jp



情報セキュリティ定期注意喚起



第1回 ソーシャルエンジニアリング



ITヘルプデスクです。
あなたのパソコンがウイルス感染した可能性があります。
今すぐ調査しないと大変な事になるのでパスワードを教えてください。

ハッカー/攻撃者



パスワードは「XXXX」です！

ユーザ

ソーシャルエンジニアリングとは？

人を騙したり、人の性質や本能に付け込む様々な手法全体を指します。

昔からある攻撃手法をオンライン、メール、ソーシャルメディア上で行う「サイバー犯罪」になっているものもあります。ソーシャルエンジニアリングは、ウイルス対策ソフトやファイアウォールといった技術的な対策で防ぐことができないため、人による防御が必要です。

攻撃者の手口

ソーシャルエンジニアリングには様々な手口があります。いくつか例をご紹介します。

フィッシング

メールやテキストメッセージを使って、悪意のあるリンクをクリックさせたり、機密情報を提供させるよう受信者を誘導します。



なりすまし

ソーシャルメディアを使って個人の情報を収集し、オンライン上で知り合いになります。



音声でのフィッシング（ビッシング）

関係者になりすまして電話で機密情報を聞き出そうとします。



対面での詐欺

標的とした職場などを訪問して、偽の身分（例えばベンダ、下請け業者、就職希望者、従業員、観光客など）を装い、機密情報を盗もうとします。



共連れ

中に入ろうとしている人の後ろについて、ロックのかかった入口を通り抜けようとしています。
例えばセキュリティカードを失くしたふりをして、ドアを開けてもらい侵入しようとします。



ショルダーハッキング

背後から画面をこっそり覗いたり、動きを観察してIDやパスワードなどの重要な情報を盗み見ます。
直接目で見るだけでなく、カメラで盗撮して間接的に盗み見ることもあります。



ゴミ箱あさり（トラッシング）

ゴミ箱から個人情報が書かれたメモや付箋などを拾い機密情報を盗みます。
清掃員やゴミの回収業者になりますなど多様な手口があるので、
溶解処理をする書類も、適切な保管下にないと機密情報を盗まれるリスクがあります。



個人の注意点

ソーシャルエンジニアリングの被害を防ぐため、個人個人が以下のことに注意しましょう。



不審なメールのファイルやリンクは開かない



社員情報を聞き出そうとする不審な電話が掛かってきた場合、
すぐに電話を切って上司に報告をする



セキュリティカードを誰かに貸したり、
セキュリティカードを持たない人の代わりにドアを開けたりしない



ショルダーハッキングの懸念がある場所では、
パソコンに覗き見防止フィルター^{*1}を装着する



機密書類は、溶解処分やシュレッダーで処分する

*1 覗き見防止フィルタは、IT本部から支給をしていますが、在庫状況によってはすぐに配布できない場合があります

【お問い合わせ先】

IT本部 情報システム部 二課

情報セキュリティ委員会事務局

[事務局へのお問合せ](#)