

SecurityAwarenessNews

the security awareness newsletter for security aware people

WARNING SIGNS:

IDENTIFYING ATTACKS

**Anatomy of Social
Engineering**

Why the Urgency?

**When Attackers Play
on Fear**



ANATOMY OF SOCIAL ENGINEERING

Consider this scenario:

An employee receives a call from someone claiming to be from IT support. They say there's an urgent security issue with the account, and they need the password to fix it. The employee is busy, and the caller sounds important and seems to need help. Without thinking, the employee shares the data.

This is social engineering in action.



What is Social Engineering?

Social engineering is the art of convincing an individual to give up sensitive information or take actions that can lead to a security breach. It's a form of psychological manipulation that exploits human nature rather than technical vulnerabilities.

A Persistent Threat

Although technology has improved, social engineering remains one of the most effective methods for cybercriminals. While technology can block many attacks, social engineering targets human interaction. These attacks try to bypass technical security measures by manipulating people directly. Staying alert and following security protocols can help you avoid falling for most social engineering attempts.

Common Techniques

Recognizing the warning signs and understanding the techniques used to strengthen your defenses are crucial in the fight against social engineering. It uses methods such as:



Phishing: Sending fraudulent emails or messages to trick recipients into revealing sensitive information or executing malicious content. For example, an email that appears to be from your bank asking you to “verify” your account details.



Pretexting: Creating a false scenario to obtain information or access. This could involve someone calling you, pretending to be a co-worker from another department, and asking for confidential data.



Baiting: Using a false promise or offer to lure people into a trap. An instance of this could be a USB drive labeled “Confidential Salary Information” left in a public area, tempting people to plug it in and unknowingly install malware.



Tailgating: Following an authorized person into a restricted area. For example, someone might wait by a secure door and follow an employee inside, bypassing security measures.

WHEN TIME PRESSURE STRIKES

In social engineering attacks, urgency is often used as a powerful manipulation tool. When attackers create a sense of time pressure, they aim to bypass rational thinking and push people into hasty decisions.

Real-World Example

In 2020, Twitter (now X) was targeted by a social engineering attack that compromised high-profile accounts. The attackers used phone phishing techniques to gain access to Twitter's internal support systems. They then took over accounts of celebrities and politicians, posting messages like **'Send \$1,000 in Bitcoin now and I'll return \$2,000! Limited time offer - only accepting the first 1,000 transactions!'** The artificial time constraint ('limited time offer') and exclusivity ('only first 1,000') created urgency that led many followers to act quickly without verifying, resulting in substantial financial losses.

Quick Decisions, High Stakes

When someone feels rushed, their ability to process information critically is diminished. This can lead to impulsive actions and increased vulnerability to manipulation.



Tips for Handling Urgent Requests

- **Take a breath:** Pause and give yourself time to think.
- **Verify independently:** Reach out to the supposed sender through a different, trusted channel.
- **Follow protocols:** Don't bypass established procedures, even under pressure.
- **Ask for guidance:** Consult a colleague or supervisor about the request if you are unsure.

As a general rule, remember that legitimate requests rarely require immediate and unrestricted action. When in doubt, it's better to check than to take hasty actions that you'll regret later.

WHEN ATTACKERS PLAY ON FEAR

Scare Tactics

Fear is a primal emotion that can override logical thinking. Social engineers often exploit this by using scare tactics to manipulate targets into hasty actions.

The Robinhood Data Breach Example

The popular trading app Robinhood experienced a significant data breach affecting approximately 7 million customers in November 2021. The attack began with a phone call to a customer service employee. The scammer used social engineering tactics, including fear and urgency, to convince the employee to grant access to certain customer support systems.

Posing as a member of the company's IT security team, the attacker convinced the employee that immediate action was necessary to address a critical threat. This manufactured fear and urgency led the employee to bypass normal security protocols, granting the attacker access to millions of users' personal information.

The Psychology of Fear in Decision-Making

When someone is afraid, the brain's fight-or-flight response kicks in, reducing their capacity for critical thinking. This makes them more susceptible to manipulation and poor decision making.

Strategies for Maintaining Composure

Similar to urgency-based tactics, fear can also push people into hasty actions. Building on our earlier tips, here are additional strategies to combat fear-based manipulation:



Recognize emotional triggers:

Be aware of content designed to provoke fear or anxiety.



Question the source:

Verify the legitimacy of threatening messages independently.



Report suspicious activity:

Alert your IT security team to potential threats immediately.

A real organization will rarely use fear or threats in its communication. If a message seems designed to scare you into taking action, it is probably an attempted attack.