S&T Bank | Zelle®

How Scammers Use Social Engineering to Steal Money and How You Can Spot Them

As scams become more prevalent, they are also more sophisticated, making them harder to detect. Scammers employ what is known as “social engineering” to manipulate people into revealing sensitive information.

It’s all about the psychology of persuasion. These scammers take advantage of human nature, aiming to lower your defenses so you’ll act on impulse rather than reason.

Let’s look at some examples of how social engineering uses the powers of persuasion to steal personal information and money:

Pretexting

Building a solid pretext or a fabricated scenario is an important aspect of social engineering. Hackers often research their victims in advance to get a sense of the victim's personal and professional life to help establish the right pretext with which to approach a victim. This information can easily be found by a simple internet search or reviewing social media activities.

Pretexting is typically the first step in a broader scheme to steal from you. The scammer then pretends to be someone you trust, possibly a representative from your financial institution or a government worker offering loan forgiveness. It often starts with a friendly “hello” and a convincing story that leads the victim to hand over sensitive information that can be used to steal money or commit identify theft.

Baiting

Baiting uses the false promise of an enticing item, such as a monetary reward or free movie download, to trick the unsuspecting consumer into opening a file or providing sensitive information, like their login credentials. Instead of the attached file being the movie or other reward, it is actually infected with malware that will encrypt or take control of the individual’s data, allowing the attacker access to personal information.

Phishing

Phishing is one of the most common types of social engineering attacks, typically in the form of emails or text messages that look like they are from a reputable source, like your financial institution, informing you of an urgent matter that needs your immediate attention. The message may include a link to a fake website that looks legitimate and suggests that you must provide personal information in order to remedy the urgent issue. This can result in the scammers gaining access to your accounts or learning important details about your identity.

How to Combat this Psychological Manipulation

Knowledge is key. Now that you know what to look for, follow these tips to help protect yourself.

1. Delete requests for personal information or passwords. No one should contact you for your personal information. Not even your financial institution.
2. Disregard offers for help or requests of help from those you don’t know. Especially if unsolicited.
3. Avoid tempting offers. Though it may be difficult to pass on what appears to be a great offer, don’t just dive in. If it seems too good to be true, it probably is. If you’re really interested, take a step back and do some research. Confirm that the company is legitimate by researching reviews. If they are reputable, call the company allegedly offering the deal to ensure the offer came from them and not a scammer pretending to be them.
4. Verify contacts. Scammers usually imitate legitimate companies by mimicking their names in emails or using caller ID spoofing. You can check their authenticity by looking at the domain name of an email address or hanging up on an unsolicited caller, verifying the legitimate phone number and calling back.

If you detect suspicious activity, contact the alleged company directly. If you have received something that appears to have come from S&T Bank, but seems suspicious, contact us at **800.325.2265**.

To learn about scams and ways to protect yourself, visit zellepay.com/pay-it-safe.