Social Engineering

Cyber attackers have learned that the easiest way to take control of your computer or steal your information is to simply ask. Use common sense. If a person or a message seems suspicious or too good to be true, it may be an attack.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES

Social Engineering

One of the main techniques cyber attackers use to compromise your computers and steal your information is called social engineering, also known as the art of human manipulation. This is when attackers pretend to be someone or something you know or trust, such as your bank, a government organization or even a friend or coworker. They then leverage that trust to get what they want, often by simply asking for it. Let's take a look at several examples of real social engineering attacks.

Email

You receive an email from a shipping company saying that they tried to deliver a package to you but had the wrong address. The email looks official; it has professional-looking graphic designs and a real company logo. The email informs you that if you do not respond in the next 24 hours, your package will be returned to sender. It then provides you with a link to click on or an email attachment to fill out so you can receive your package. The problem is this is an attack. A cyber criminal has created an email that looks just like a real shipping company; however, the email is designed to fool you. If you click on the link, you will be taken to a website that the attacker controls. Once your browser connects to the attacker's website, it attempts to silently hack into your browser. If you were to open the attachment, it would silently infect your computer. Be suspicious of any unexpected emails that urge you to click on links or open attachments.

Tech Support Scam

You receive a phone call from someone claiming to be from a computer support company. They believe your computer is infected and have been tasked with investigating the issue and helping you secure your computer.   They then ask you if there are specific files on your computer and tell you how to find them. When you locate the files on your computer, the caller confirms your computer is infected. This is really all a lie and your computer is not infected. These files are standard files that every computer has. Once they have you fooled into believing your computer is infected, they will then pressure you into buying their security software. However, this software is really a virus that gives them total control of your computer. In the end, not only has the caller tricked you into infecting your computer for them, but you just paid them to do it.

Social Media

Your friend posts on her Facebook page that she is on vacation in London and has just been mugged. She needs someone to send her money right away so she can get back home. However, this is a lie. Your friend has not been mugged. In fact, she is not even in London. Instead, a cyber attacker has hacked into and taken over her Facebook account, then posted this fake message in an attempt to scam money from her friends. In this case, the best way to protect yourself would be to call your friend on the phone and confirm if she really does need help.

Remember, social engineering is nothing more than an attacker building trust with you, then abusing that trust to get what they want. If you get an email, message or phone call that seems odd, suspicious or too good to be true, it may be an attack. Common indicators of a social engineering attack include people asking for information they should not have access to, using a lot of confusing or technical terms or creating a sense of urgency. If you believe someone is attempting to trick or fool you, simply hang up the phone or ignore the email and immediately contact the help desk or information security team.

You Won the Lottery

You receive a text message on your smartphone announcing you have won the lottery. To collect your winnings, you must call the number in the message and provide them your banking information. When you call the phone number, a person explains that you must pay a transaction fee or taxes before you receive your lottery winnings. Once you provide them your financial information and pay the required fees, the cyber criminals disappear with your money and information, never to be seen again. The simplest way to protect yourself against these types of attacks is to be suspicious of any message that sounds too good to be true. In this case, how could you win a lottery that you never even entered or heard of before?

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES