HOW TO PREVENT SOCIAL ENGINEERING ATTACKS

When we think about cyber-security, most of us think about defending ourselves against hackers who use technological weaknesses to attack data networks. But there is another way into organizations and networks, and that's taking advantage of human weakness. This is known as social engineering, which involves tricking someone into divulging information or enabling access to data networks.

There are several types of social engineering attacks. So it's important to understand the definition of social engineering, as well as, how it works. Once the basic modus operandi is understood, it's much easier to spot social engineering attacks.

Social engineering attacks are particularly difficult to counter because they're expressly designed to play on natural human characteristics, such as curiosity, respect for authority, and the desire to help one's friends.

Put simply, social engineering is the use of deception to manipulate individuals into enabling access or divulging information or data.

Check the Source

Take a moment to think about where the communication is coming from; do not trust it blindly. A USB stick turns up on your desk and you do not know what it is. An out of the blue phone call says you've inherited $5 million. An email from your CEO asking for a load of information on individual employees. All of these sound suspicious and should be treated as such.

Checking the source isn’t difficult. For instance, with an email, look at the email header and check against valid emails from the same sender. Look at where the links go - spoofed hyperlinks are easy to spot by simply hovering your cursor over them (Do not click the link though!). Check the spelling: banks have whole teams of qualified people dedicated to producing customer communications, so an email with glaring errors is probably a fake.

If in doubt, go to the official website and get in contact with an official representative, as they will be able to confirm if the email/message is official or fake.

Don't Go Too Fast

Be particularly wary when you feel a sense of urgency coming into a conversation. This is a standard way for malicious actors to stop their targets from thinking the issue through. If you're feeling pressured, slow the whole thing down. Say you need time to get the information, you need to ask your manager, you don't have the right details with you right now — anything to slow things down and give yourself time to think.

Most of the time, social engineers will not push their luck if they realize they've lost the advantage of surprise. Social engineering often depends on a sense of urgency. Attackers hope their targets will not think too hard about what is going on. So just taking a moment to think can deter these attacks or show them for what they are; fakes.

Secure Your Devices

It's also important to secure devices so that a social engineering attack, even if successful, is limited in what it can achieve. The basic principles are the same, whether it's a smartphone, a basic home network or a major enterprise system.

- **Keep your anti-malware and anti-virus software up to date**. This can help prevent malware that comes through phishing emails from installing itself. Use a package like Kaspersky's Antivirus to keep your network and data secure.
- **Keep software and firmware regularly updated**, particularly security patches.
- **Don't run your phone rooted, or your network or PC in administrator mode**. Even if a social engineering attack gets your user password for your "user" account, it won't let them reconfigure your system or install software on it.
- **Don't use the same password for different accounts.** If a social engineering attack gets the password for your social media account, you don't want them to be able to unlock all of your other accounts too.
- **For critical accounts, use two-factor authentication** so that just having your password isn't enough to access the account. That might involve voice recognition, use of a security device, fingerprinting, or SMS confirmation codes.
- **If you just gave away your password to an account** and think you may have been "engineered," change the password right away.
- **Keep yourself informed about new cybersecurity risks** by becoming a regular reader of our Resource Center. You'll then know all about new methods of attack as they emerge, making you much less likely to become a victim.

Think About Your Digital Footprint

You might also want to give some thought to your digital footprint. Over-sharing personal information online, such as through social media, can help attackers. For instance, many banks have “name of your first pet” as a possible security question — did you share that on Facebook? If so, you could be vulnerable! In addition, some social engineering attacks will try to gain credibility by referring to recent events you may have shared on social networks.

We recommend you turn your social media settings to “friends only” and be careful what you share. You don't need to be paranoid, just be careful.

Think about other aspects of your life that you share online. If you have an online resumé, for instance, you should consider redacting your address, phone number and date of birth - all useful information for anyone planning a social engineering attack. While some social engineering attacks don't engage the victim deeply, others are meticulously prepared - give these criminals less information to work with.

Social engineering is very dangerous because it takes perfectly normal situations and manipulates them for malicious ends. However, by being fully aware of how it works, and taking basic precautions, you'll be far less likely to become a victim of social engineering.