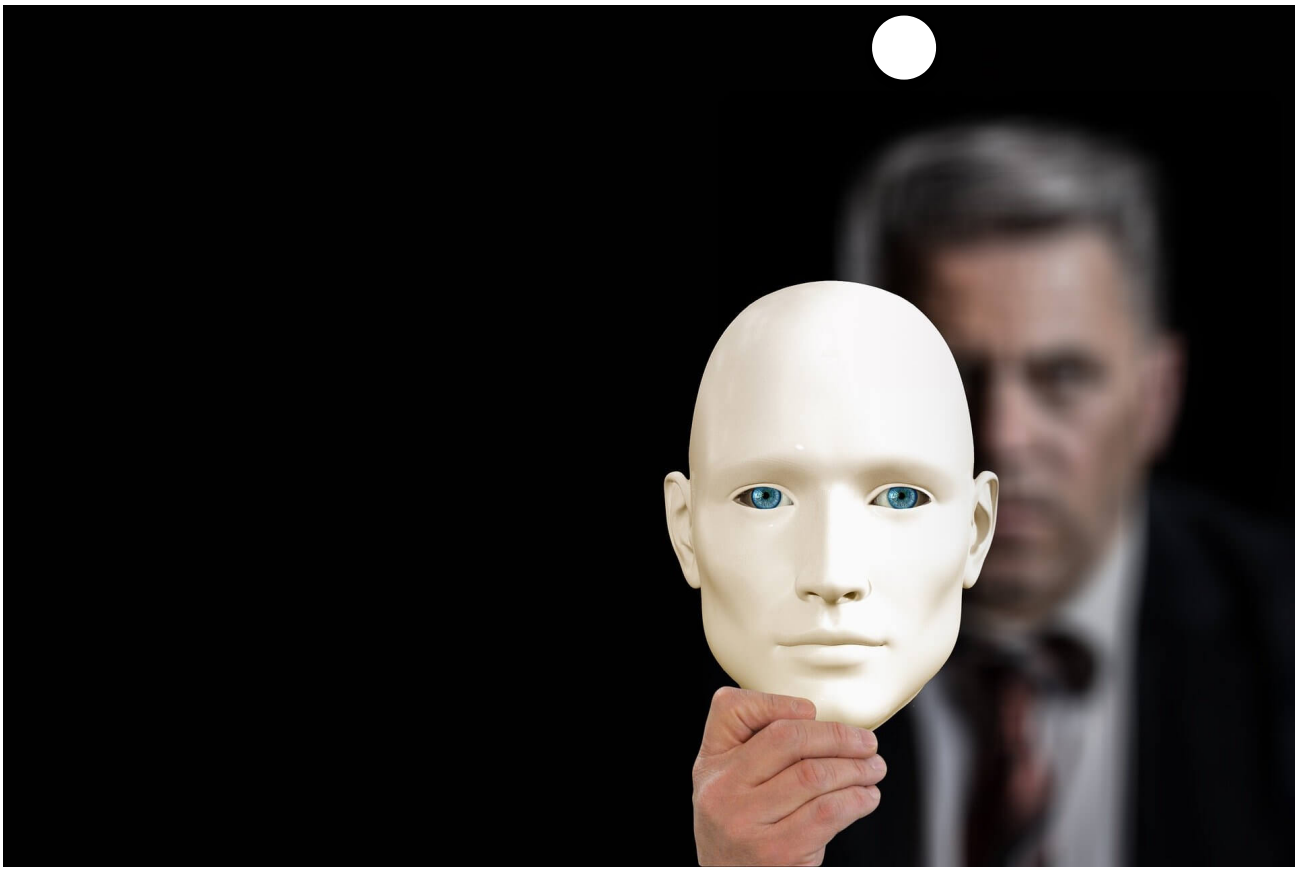
Ways to avoid social engineering attacks



What is social engineering?

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's 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.

For instance, an intruder could pose as IT helpdesk staff and ask users to give information such as their usernames and passwords. And it is surprising how many people don't think twice about volunteering that information, especially if it looks like it’s being requested by a legitimate representative.

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

Types of social engineering attacks

There are various 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.

Baiting

Baiting involves creating a trap, such as a USB stick loaded with malware. Someone curious to see what's on the stick puts it in their USB drive, resulting in the system being compromised. In fact, there's a USB stick that can destroy computers by charging itself with energy from the USB drive and then releasing it in a ferocious power surge — damaging the device where it's been inputted. (the USB stick only costs $54).

Pretexting

This attack uses a pretext to gain attention and hook the victim into providing information. For instance, an internet survey might start out looking quite innocent but then ask for bank account details. Or someone with a clipboard might turn up and say they're doing an audit of internal systems; however, they might not be who they say they are, and they could be out to steal valuable information from you.

Phishing

Phishing attacks involve an email or text message pretending to be from a trusted source — asking for information. A well-known type is the email purportedly from a bank wanting its customers to 'confirm' their security information and directing them to a fake site where their login credentials will be recorded. 'Spear phishing' targets a single person within a company, sending an email that purports to come from a higher-level executive

Vishing and Smishing

These types of social engineering attack are variants of phishing - 'voice fishing' which means simply phoning up and asking for data. The criminal may pose as a co-worker; for instance, pretending to be from the IT helpdesk and asking for login information. Smishing uses SMS messages instead to try and obtain this information.

Quid pro quo

They say "fair exchange is no robbery" but in this case, it is. Many social engineering attacks make victims believe they are getting something in return for the data or access that they provide. 'Scareware' works in this way, promising computer users an update to deal with an urgent security problem when in fact, it's the scareware itself that is the malicious security threat.

Contact spamming and email hacking

This type of attack involves hacking into an individual's email or social media accounts to gain access to contacts. Contacts may be told the individual has been mugged and lost all their credit cards and then ask to wire money to a money transfer account. Or the 'friend' may forward a 'must see video' which links to malware or to a keylogging Trojan.

Farming vs hunting

farming" and is riskier for the attacker: there's more chance they will be found out. But, if their infiltration is successful, it can deliver far more information.

How to avoid 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. There are a number of tips that can help detect social engineering attacks...

Check the source

Take a moment to think about where the communication is coming from; don't trust it blindly. A USB stick turns up on your desk, and you don't know what it is? A phone call from out of the blue 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.

What do they know?

Does the source not have information you'd expect them to have, such as your full name, etc.? Remember, if a bank is phoning you, they should have all of that data in front of them and they will always ask security questions before allowing you to make changes to your account. If they don't, then the chances of it being a fake email/call/message are significantly higher, and you should be wary.

Break the loop

Social engineering often depends on a sense of urgency. Attackers hope their targets will not think too hard about what's going on. So just taking a moment to think can deter these attacks or show them for what they are — fakes.

Ask for ID

One of the easiest social engineering attacks is bypassing security to get into a building by carrying a large box or an armful of files. After all, some helpful person will hold the door open. Don't fall for this. Always ask for ID.

The same applies to other approaches. Checking the name and number of whoever is calling or asking, "Who do you report to?" should be a basic response to requests for information. Then simply check the organization's chart or phone directory before giving out any private information or personal data. If you don't know the individual requesting the information and still don't feel comfortable parting with the information, tell them you need to double check with someone else, and you will come back to them.

determine which emails are likely to be spam. They might detect suspicious files or links, they may have a blacklist of suspicious IP addresses or sender IDs, or they may analyze the content of messages to determine which are likely to be fake.

Is this realistic?

Some social engineering attacks work by trying to trick you into not being analytical and taking the time to assess whether the situation is realistic can help detect many attacks. For example:

- If your friend was really stuck in China with no way out, would they send you an email or would they ring you/ text you as well?
- Is it likely that a Nigerian prince left you a million dollars in his will?
- Would the bank ring up asking for your account details? In fact, many banks note when they send emails to their customers or talk to them on the phone. So double check if you're not sure.

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 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 won't push their luck if they realize they've lost the advantage of surprise.

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

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 straight 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.

Related links

Social Engineering - Definition

How Malware Penetrates Computers and IT Systems

Tech Support Scams

How to get rid of a calendar virus on different devices

I've Been the Victim of Phishing Attacks! What Now?

Don't be a phishing victim: Is your online event invite safe to open?

How safe are eWallets? How to Protect Your eWallet

Stay in Touch

Home Solutions

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

All Solutions

Medium Business Products
(101-999 EMPLOYEES)

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
(1000+ EMPLOYEES)

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Products

Global