Knowledge is your best defense.

Recognize and Combat Social Engeering

CYBERCRIMINALS

Want access to something sensitive

They want your boss's information or the number of an account, or even want to get into the building. Stand firm and ask for proof of identification.

Exert pressure on you

Social engineers want you to act without thinking. If someone is pressuring you to do something without giving you time to consider it, that's a sign of a social engineer.

Send offers too good to be true

You've won the lottery! Or not. If an offer or opportunity seems too good to be true — it probably is.

Pretend to be a client or authority figure

Social engineers will impersonate clients, bosses, friends, family or others who may be able to influence you. Always take extra steps to prove their identity!

Are unwilling to prove identity

A social engineer will often deflect or get angry when asked to prove their identity. They may try to stop you from contacting other people for verification or refuse to give proof.

YOU

Examine all links and attachments

You may receive innocent-looking links or attachments which actually contain malware; examine carefully and don't click unless you're certain it's safe.

Don't use their contact methods

If a message might be from an impostor, contact the real person or organization through a known, safe method, such as a public phone number.

Escalate

If someone's story sounds fishy or they can't prove who they are, pass the issue — and your concerns — up the chain of command.

Don't let yourself be bullied

Social engineers may try to intimidate, emotionally blackmail or threaten you. Don't let it faze you.

Don't share information an attacker could use

If you share personal or sensitive information online, an attacker can harvest it for use in impersonation or attacks.