



eFence

eFence Security

www.efencesecurity.com

info@efencesecurity.com

1-(800)-817-0203

Awareness and education are your best defenses. Stay informed about the latest scams and regularly update your knowledge on common social engineering tactics. Remember, reputable institutions will never ask for sensitive information unsolicited. By cultivating a skeptical mindset and staying informed, you create a robust shield against social engineering scams.

Cyber Hygiene

Protecting Yourself from Social Engineering Scams

Social engineering scams have become increasingly sophisticated, posing a significant threat to our online security. These schemes manipulate human psychology, tricking individuals into divulging sensitive information or performing actions that compromise their privacy. It's crucial to recognize the signs and adopt preventive measures to safeguard yourself against these scams.



Your 'friend' sends you a strange message.



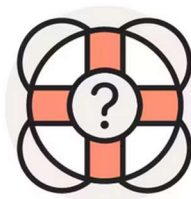
Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



The sender can't prove their identity.

One common tactic is phishing, where attackers impersonate trusted entities, often via email or text, to trick recipients into revealing passwords or financial details. Be cautious of unexpected emails or messages requesting sensitive information. Verify the sender's authenticity before clicking on any links or sharing personal data.

Another prevalent form of social engineering is pretexting, where scammers create a fabricated scenario to extract information. They might pose as colleagues, authorities, or service providers seeking confidential data. Always validate the identity of the person contacting you, especially if they're requesting sensitive information. Legitimate organizations will not mind you taking your time to confirm their authenticity.