Understanding SOCIAL ENGINEERING ATTACKS

And the complex nature of how hackers attempt to gain unauthorized access to sensitive information.





A **social engineering attack** occurs when a cybercriminal tricks someone into giving them information that can then be used to gain unauthorized access to data, systems, or financial assets.

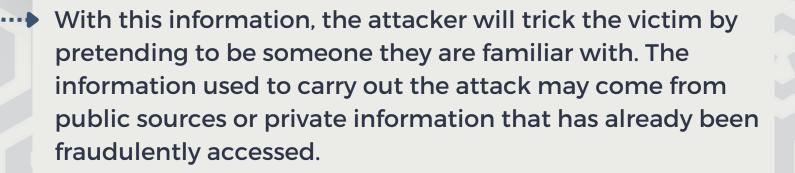
This does not necessarily mean the attacker's goal is to directly obtain password or account information from the victim however.

Instead, a successful social engineering attack generally relies on the victim's **willingness to give information or access** to the attacker.





The attacker may first **establish a level of trust** with the victim. Often this is accomplished by first gaining information about them or their company.



From here, the attacker exploits the victim after gaining their trust.





An example of this type of attack may be a hacker that impersonates a company's CEO. The attacker might then send an email to someone in the business's accounts payable department authorizing a fraudulent charge or requesting sensitive information.



Continue to learn more



Another example of a social engineering attack might involve a hacker pretending to be a company's IT support. Information the hacker used to impersonate the IT company might have come from public or private information.





It is important to be aware of social engineering attacks and the research cybercriminals might undertake to carry them out, as well as how to **recognize**, **prevent**, **and respond** to them if they occur.



To learn more about how we help our clients, please visit:

https://www.leacif.com/cybersecurity-advisory



Innovate your expectations | Live your values | Define your control