



Social Engineering

Social Engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks or taking an action (e.g., clicking a link, opening a document).

QUICK TIPS TO AVOID INFECTION



Be suspicious of emails from unknown senders, emails that request sensitive information such as PHI or PII, or emails that include a call to action that stresses urgency or importance.



Never open email attachments from unknown senders.



Implement incident response plans to manage successful phishing attacks.



Implement multi-factor authentication (MFA).

KNOW THE RISK

Healthcare had the highest cost per data breach in 2022.



\$4.91M

the average cost of a single data breach

PROTECT YOUR ORGANIZATION

Prevention is the best medicine.

Check out the [Prescription Series Posters](#) to learn how you can prevent Social Engineering attacks.

Presented in [Technical Volumes 1 and 2 of HICP](#), the ten Cybersecurity Practices range from personnel training and awareness to the development and implementation of new processes, the acquisition and customization of new technology, and, ultimately, to fostering a consistent, robust, and continually updated approach to cybersecurity.

