

# How to Protect Your Data from Social Engineering Attacks

A social engineering attack needs only one thing to be successful: the trust of the targeted party. All it takes is a single email, phone call, or text message that appears to come from a trusted source for a cyber criminal to gain access to sensitive information. Here's how to avoid these types of cyber threats:



1

**CAREFULLY INSPECT ALL INCOMING MESSAGES**

Cyber criminals who use social engineering tactics are banking on their victims acting first and thinking later. Examine all aspects of your incoming messages for suspicious elements, such as a spoofed email address or website URL.

2

**BE WARY OF AN URGENT TONE**

Social engineering campaigns typically lean on language that conveys a strong sense of urgency. Examples include high-pressure sales tactics and intimidating ultimatums, such as the threat of legal action.

3

**BEWARE OF UNEXPECTED MESSAGES FROM YOUR CONTACTS**

Cyber criminals routinely take over people's email accounts to try and trick that person's contacts with a scam. If you aren't expecting an email from a contact, especially one with a link or attachment that is out of character, verify its legitimacy before opening.

4

**DELETE ANY REQUEST FOR FINANCIAL DATA OR PASSWORDS**

If you're asked to reply to an email, phone call, or text message with your financial or password information, it's likely a scam. Even if the message promises a reward in return, never divulge sensitive information in a response.

5

**DON'T CLICK ON SUSPICIOUS LINKS OR ATTACHMENTS**

Don't click on unexpected links, even if they come from familiar email senders or organizations. You can be redirected to a website or start a download that can infect your device. The same guidelines apply for email attachments.

6

**UTILIZE YOUR EMAIL CLIENT'S SPAM FILTER**

Every email program comes with a spam filter. In your account settings, adjust the filter options to your liking and periodically check your spam inbox for any legitimate mail that got sent there by accident.