Socializing Risks

We're wired to connect, but not all connections are beneficial. Here's how to spot red flags that indicate a connection might be risky.

Unsolicited Contact: Receiving unexpected emails, messages, or phone calls from unknown individuals or organizations.

Requests for Personal Information: Attempts to gather sensitive information such as passwords, Social Security numbers, or financial details.

Phishing Emails: Emails that appear legitimate but contain suspicious links or attachments, urging immediate action or offering something too good to be true.

Urgency and Fear Tactics: Messages that create a sense of urgency or fear, pressuring you to act quickly without thinking.

Spoofed Communication: Emails, messages, or calls that appear to come from trusted sources but have subtle inconsistencies, such as incorrect email addresses or phone numbers.

Unusual Social Media Activity: Strange friend requests, messages, or posts from accounts that seem fake or compromised.

Pretexting: Individuals pretending to be someone they're not, using a fabricated story to gain your trust and extract information.

Quid Pro Quo: Offering services or benefits in exchange for information, often disguising the true intent behind the request.

Tailgating and Physical Intrusion: Unauthorized individuals attempting to follow employees into secure areas or manipulating physical access controls.

Spear Phishing: Highly targeted phishing attacks based on personal or professional details, often involving extensive research on your background.

Baiting: Offering enticing items such as free downloads, discounts, or gifts that require you to provide personal information or download malicious software.

Elicitation: Casual conversations where the individual subtly extracts information from you, often without you realizing it.

Barracuda®
Your journey, secured.