west protect

SAFE Tip Sheet
Social Engineering

Callers will pretend to be legitimate

In social engineering, criminals play on human emotion to steal company information.

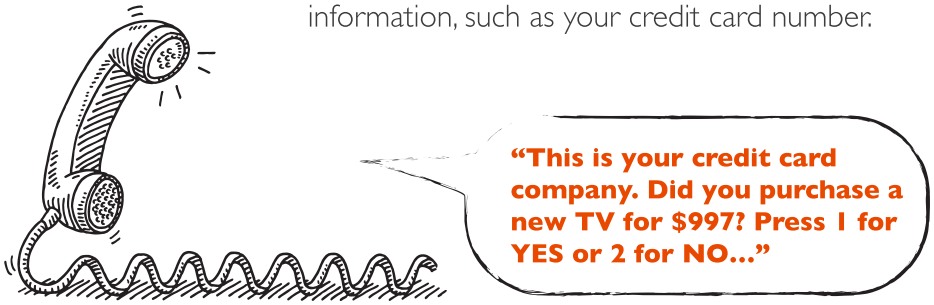
It can happen:

- in person
- over the phone
- on social media
- in text
- in email

The caller might drop names or claim they are from one of your vendors or business partners. Or they might say they are a new employee, or calling from the Service Desk. The biggest warning sign is if the call comes out of the blue and seems odd. Trust your instincts!

The call might be automated

You may receive a phone call with alarming news, asking you to press a button and provide information, such as your credit card number.



It can start simply

Social engineers collect bits of information over time, then piece it all together to impersonate a person or execute a scam.

If a stranger asks you for information you think is harmless (such as the name and title of a co-worker), be on guard! It could be the beginning of a social engineering scam.

Be especially aware on mobile devices.

The screen is smaller, and people are often multi-tasking. This means you're distracted and it can be easier to fall for a scam.

Emails can be personalized

With all the data breaches recently, criminals are gathering more data than ever. This means they can create "spear phishing" emails that are personalized and seem very real. Keep your guard up!

WHEN IN DOUBT, DON'T GIVE INFORMATION OUT!