Watch out!
5 Social engineering tricks.

Scamsters rely on old con-man tricks to learn everything from your password to your bank account number.

While many of these tricks have a tech twist, they all follow the age-old pattern of counting on greed or emotion to persuade you to act against your better judgment. Watch for the following:

1. E-signature needed.

Most people have grown accustomed to using DocuSign or similar services to execute documents. But criminals send emails disguised as requests to sign, hoping you'll click the button in the message—which actually takes you to an ID theft site.

2. Act now or else.

This may be the oldest trick used by social engineers. They imply that if you don't click now and perform an action, your account will be suspended ... or you may even be arrested. Any email or phone call that seeks to rush you into a decision is almost certainly a scam.

3. Helpful Henry.

Most of us are courteous and helpful by nature, and social engineers are adept at leveraging this. The lure may be a stranger who has "forgotten" their card key, or an email supposedly from a new sales rep who just needs some product info.

4. Tick you off.

Another scammer strategy is the email that appears to be poor customer service, such as a flight cancellation or notification of an undelivered package. The criminals are hoping your frustration will lead to a quick email back, after which they try to direct you to a fraud site.

5. Good old greed.

You can't cheat an honest man. If you find a USB stick in the company parking lot and plug it in, hoping for something juicy or intriguing, you have no one else to blame.

220010.12 IAS (5/22)