SOCIAL ENGINEERING

Social Engineering is a type of fraud that takes advantage of our tendency to give others the benefit of the doubt. Knowing how it occurs can help you identify a potential threat.

What should you be looking out for in social engineering emails?

Check The Details

- Inaccurate time / dates
- URL / link routing to incorrect websites
- Messaging including claims you know to be false
- Errors in the to / from address
- Spelling / grammar issues throughout

Ask Yourself

- Is the email relevant to my job / role?
- Is the from / to field listing someone I don't know or don't work with?
- Does the email subject match the body content?
- Is there an attachment that is irrelevant to the email?

Consider The Sender

- Is this person acting "out of character" when communicating?
- Is the message threatening in nature?
- Are they implying bad consequences for inaction?
- Are they suggesting a promise you don't remember?

Think About Timing

- Is the email telling me to do something immediately?
- Is it written to make the sender look rushed so I act faster?
- Does it offer a time limit for response?
- Have they forgotten to explain exactly why the user action is so rushed?

How Mara Can Help Keep You Safe

Creating training programs that support and reinforce security policies

Creating security programs and policies that help reduce social engineering risks

Conducting risk assessments to identify security risks and ways to mitigate them

MARA CONSULTING

Learn more about our team, our practice and how we can help at maraconsulting.ca