SOCIAL ENGINEERING *What to know*

Social Engineering is the act of manipulating individuals through actual human interaction in order to acquire information about an individual or organization

3 BASIC TYPES OF TACTICS

PHISHING

The practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information.

VISHING

The practice of eliciting information or attempting to influence action via the telephone, such as “phone spoofing.”

IMPERSONATION

The practice of pretexting as another person with the goal of obtaining information or access to a person, company or computer system.

Spotting a SOCIAL ENGINEERING ATTACK

Social engineering attacks often rely on one or more tactics that make it easier to tell you’re being targeted. Look out for these common signs:

1 THEY REQUEST SOMETHING OF VALUE FROM YOU.
For example; money, bank account numbers, personal information, in-person or remote access to your PC or mobile devices.

2 THEY WANT YOU TO KEEP THE MATTER “SECRET” OR “PRIVATE”.
Because any attempt to verify the authenticity of the request on your part would easily expose the true nature of the attack.

3 THEY NEED YOU TO TAKE URGENT ACTION.
By rushing you along, they hope to keep you off-balance, limiting your natural ability to detect when something isn’t quite right.

4 THEY APPROACH YOU FROM A POSITION OF AUTHORITY.
We are all brought up not to question authority, so attackers will use that to their advantage, assuming roles such as:
- A senior administrator
- Law Enforcement
- Software Manufacturers

Annapolis Valley
Regional Centre for Education
Information Technology Division

902.538.4674
techsupport@avrce.ca
http://it.avrce.ca/