Social Engineering

Social Engineering is a way that people use normal social interactions to manipulate people to breach security. It isn't limited to any technology or system, it can be conversation, texting, body language, or email.

The goals of Social Engineering are typically sensitive or personal information, but it can be used to access secure systems. Social Engineering is used for fraud, identitiy theft, or can be the prelude to a more serious hack.

Usually Social Engineering plays on a person's expectations, and emotions. Sometimes it means a person is pretending to be a delivery person, or they could pretend to be frazzled and running late. They play on our gut reactions in order to bypass our reasoning.

There is no single techology or strategy that can defend against social engineering. Each person is the front line against this kind of intrustion. The critical element to protect yourself and your organisation is critical thinking.

How to Avoid Being a Victim?

Keep your eyes open and ask yourself questions:

- If someone wants to enter your house, ask yourself if this is really a secure situation? Are you expecting maintenance or a delivery? Is this person from the company that you'd expect?
- Why is someone asking about details about your work? Is this information that could be used maliciously?
- How is this person making me feel? Am I feeling sorry for this person who forgot their keycard? Am I feeling intimitated by this bigshot who demands access and information? Am I feeling like I owe this friendly stranger in the café?
- Does this person really have authority? Have I actually seen any of their credentials?
- Does it make sense for me to be using my financial information in this situation? Am I dealing with a verified and trusted entity?
- Am I communicating in a secure way? Is this connection secure? Can I be overheard?

These questions might give you a sense that something is off about a situation. Be dilligent and double-check information. Verfiy information with a trusted third party. Don't take everything at face value.

What to do if you think you are a victim?

- If you believe your financial accounts have been compromised, contact your financial institution or credit card company immediately. Watch for any unexplainable charges to your account.
- Document the situation, report the attack to the police and file a report.
- Check your credit report with:
  Equifax Canada – www.consumer.equifax.ca/home/en_ca
  Trans Union Canada – www.transunion.ca
- If you believe you might have revealed confidential or sensitive information about your organization, report it to the appropriate Security or Privacy people within your organization.

What additional steps can you take to protect your privacy?

- Do business with credible companies – Before supplying any information online, verify the credibiliy, security and integrity of the company.
- Do not always use your primary email address online Consider creating an additional email account.
- Avoid using debit cards for online purchases – Credit cards usually offer some protection against identity theft and may limit the monetary amount.

Resources

Canadian Anti–Fraud Call Centre
www.antifraudcentre.ca

Equifax Canada
https://www.consumer.equifax.ca/personal/

TransUnion Canada
www.transunion.ca

Scams, Fraud and Economic Crime
http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

Social–Engineering.Org
http://www.social-engineer.org/