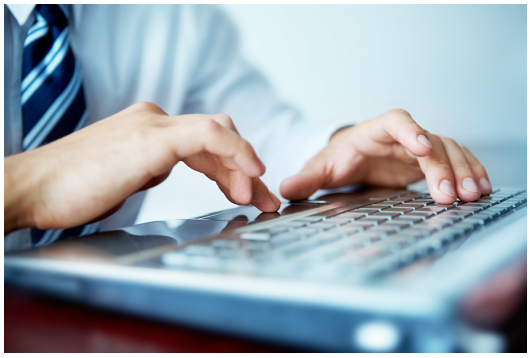
Information Security Awareness Program

SOCIAL ENGINEERING

Social Engineers typically misrepresent themselves as someone you know or a company that you're familiar with in order to manipulate you into giving away personal or confidential information. They will try many methods to access your information – phone, email and even in person.

The many faces of Social Engineering:

Impersonation



This could be over phone, email, or in person. Social Engineers pretend to be someone that you know and trust, such as a senior official or someone from Human Resources or the Technology Service Centre. Typically they use intimidation or a false sense of urgency to get you to cooperate.

Baiting

This is when someone asks you a series of seemingly harmless questions, trying to steer the conversation in order to "catch" the right answers**.** They'll frequently inject facts to attempt to sound legitimate.

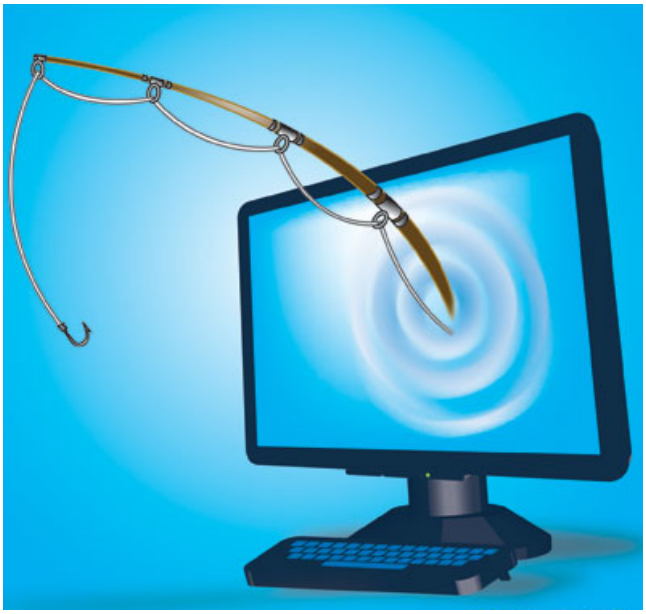
Piggybacking/Tailgating

This is when someone you don't know tries to follow you into a secure building or area. Do you hold the door for that person behind you? They could be looking for unauthorized access to valuable assets and government information. Make sure they are a known employee and are wearing their I.D. card.

Shoulder Surfing

This is often too easy to do – shoulder surfing is simply someone looking over your shoulder to see what you're typing or what's on your computer screen. However, they can even look from a window or doorway, or simply listen to your conversation.

Be considerate that some employees have requirements to protect information (personal information, health information, business information) even from colleagues.



Dumpster Diving

This is self-explanatory; it's simply someone searching through the trash or recycling for confidential or sensitive documents that were not properly disposed of. You should always use the GNWT's document disposal services to dispose of information.

Talk to your Records Coordinator about appropriate ways to dispose of substantive recorded information.

Phishing/Spear Phishing

Phishing and Spear Phishing are when a cybercriminal claims to be a person or company they aren't, to try to trick you into going to virus infected sites, downloading infected documents, or providing confidential information that would allow them access to your organization or personal information. They're usually identifiable by typos and grammar mistakes, as well as strange hyperlinks or phone numbers.

How to avoid Social Engineering:

- Follow appropriate procedures before giving out information. Determine if you have the authority to give it out, and if the person has the authority to receive it. Question the purpose of information requests, even if the request appears to come from another Government of the Northwest Territories office. Treat all information with care.
- If you see someone you don't know on government premises, ask them "Can I help you?" "Are you looking for someone?" Make sure they have a business reason to be visiting.
- Be aware of your surroundings, and use computer privacy tools such as locking your screen (Windows key + 'L')**.**
- Don't tell **anyone** your password!
- Before you throw information in your desk trash bin, ask yourself if it would be okay for unauthorized people to see.
- If you receive an email you weren't expecting, don't click on anything! Call the person or company directly to determine if it's legitimate. If you are unsure or it seems suspicious, report it to the Technology Service Centre.
- Notify anything suspicious on your computer or any accidental release of information to your supervisor and the Technology Service Centre. This is called **Information Incident Reporting.** This process is to ensure that the Government of the Northwest Territories is equipped to deal with threats to its information assets.

For more information on Information Security, or questions about potential or confirmed Social Engineering incidents, contact the OCIO. You can reach us at the e-mail address below.