Administrative Procedure 647

Procedure for Handling Potential Social Engineering Calls

1. Objective and Importance of Caution

Social engineering attacks are designed to manipulate individuals into providing information that should remain confidential. Attackers may pose as trusted entities – such as law enforcement, media, government agencies, or businesses – to gain access to personal, student, staff or organizational information.

It is critical to remember:

- **The attacker's goal is to collect information.**
- **No personal, financial, or internal information should be shared without proper verification.**
- **Even small details (such as confirming someone works for the division) can be useful to attackers.**

In following this procedure, staff can help protect the school division from fraud, identity theft, and/or security threats.

2. Initial Call Handling

When receiving a call from someone claiming to be from any organization (law enforcement, media, government agency, business, etc.):

A. Gather Basic Information

1. **Ask for the caller's full name, title, and organization.**
2. **Ask for the callback number and official email address.**
3. **Ask for the purpose of the call and what specific information they need.**
4. **DO NOT provide any sensitive or internal information immediately.**
    - Example: "For security purposes, I need to verify your credentials before

proceeding. Can you provide me with your organization's official contact details?"

B. Verification Process

If the Caller Claims to Be from a Known Organization (RCMP, Media, Government, Vendor, etc.):

1. **Look up the organization's official contact details** online (do not use the number they provide).
2. **Call the organization directly using their publicly listed phone number** and ask to be connected to the person who contacted you.
3. **Check if the caller's email is legitimate** (e.g. official domain vs. free services like Gmail, Yahoo).

If the Caller Claims to Be from a Business or Vendor:

1. **Check your division's records** to confirm whether you have an existing relationship with them.
2. **Look up their official website and contact information** to verify their identity.

3. Handling Suspicious Calls

- If the caller becomes **aggressive, evasive, or refuses to verify their identity,** end the call.
- If they claim to be in an emergency but refuse to provide verifiable details, be cautious.
- Do not disclose **personal, student, staff, or financial information** without verification.

4. Reporting Suspicious Calls

1. **Document the call details** in the **Social Engineering Call Log** (see section 6):
   - Caller's claimed name, title, and organization
   - Phone number displayed on Caller ID (if available)
   - Nature of the request
   - Any notable behavior (urgency, threats, refusal to verify)
   - Caller's claimed name, title, and organization
   - Phone number displayed on caller ID (if available)
   - Nature of the request
   - Any notable behavior (urgency, threats, refusal to verify)
2. **Report the call to division leadership.**
3. If the caller claimed to be from law enforcement, **notify the local RCMP detachment** to verify.

5. Staff Training on Social Engineering Prevention

A. Training Objectives

All front desk and administrative staff will be trained to:

- Recognize social engineering tactics (urgency, authority, manipulation).
- Follow verification steps before providing information.
- Document and report suspicious calls.
- Protect sensitive school division information.

B. Training Delivery

- **Annual Security Awareness Training** on social engineering (conducted by division leadership).
- **Scenario-Based Role-Playing Exercises** to practice handling fake calls.
- **Quick Reference Guide** at front desks summarizing the procedure.

6. Social Engineering Call Log (Alert System for Repeat Attempts)

A. Purpose of the Call Log

- Track patterns of suspicious calls.
- Identify repeat attempts from the same caller or organization.
- Escalate concerns to leadership if necessary.

B. Information to Record in the Call Log

Date	Time	Caller Name	Claimed Organization	Phone Number	Reason for Call	Verification Attempted	Notes (Suspicious Behaviour)
YYYY-MM-DD	HH:MM AM/PM	John Doe	RCMP)	555-785-1234	Request for staff info	Yes/No	Aggressive, refused verification

- **Division leadership will review the log weekly** and issue alerts if there are repeated social engineering attempts.
- **If a pattern emerges** (e.g., same caller ID, same script), leadership will issue a **security advisory to all staff.**

Reference:	Date Approved: March, 2025 Reviewed or Revised: