Social Engineering Awareness

Background

In order to protect Fort McMurray Catholic Schools assets, all employees need to defend the integrity and confidentiality of the organization's resources.

Employees are an important part of the School Division's security. The awareness and integrity of each employee is the best line of defense for protecting the School Division's against Social Engineering Fraud.

Purpose

This administrative procedure has two purposes:

a. To increase the awareness of employees in respect to:

i. the high risk of fraudulent social engineering attacks against the School Division and each individual;

ii. procedures that can use to detect attacks;

iii. techniques used for such attacks;

iv. standard procedures to respond to attacks;

v. who to contact if they suspect or are targeted by such attack;

vi. these circumstances.

vii. Employees recognize they are an important part of the School Division's security. The integrity of an employee is the best line of defense for protecting sensitive information regarding <Company Name>'s resources.

b. To create specific procedures for employees to follow to help them make the best choice when:

i. Someone is contacting the employee - via phone, in person, email, fax or online -

and elusively trying to collect sensitive information; and

ii. The employee is being “socially pressured” or “socially encouraged or tricked” into sharing sensitive data.

Procedure

2. This administrative procedure applies to all employees of the School Division including temporary contractors, casual and part-time staff.

3. Sensitive information of the School Division will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

   a. An “urgent matter”;

   b. A “forgotten password”;

   c. A “computer virus emergency”;

   d. Any form of intimidation from “higher level management”;

   e. Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel;

   f. The requester requires release of information that will reveal passwords, user names or personal information of students or parents;

   g. The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person;

   h. The techniques are used by a person that declares to be "affiliated" with the School Division or any level of Government;

   i. The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company; or

   j. The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or

making inappropriate greetings (coming from a stranger).

4. Action

a. All individuals described in paragraph 2 above must complete the ***Email Safety – Phishing, Social Engineering and Ransomware Awareness Training*** online training module (PublicSchoolWorks) within 30 days from the date of employment and every year thereafter;

b. If one or more circumstances described in paragraph 3 above is detected, the identity of the requester **MUST** be verified before continuing the conversation or replying to email, fax, or online. A verification of a phone call will normally require asking for a name and phone number to call back and dropping the conversation to allow for an offline verification;

c. If the identity of the requester described above **CANNOT** be promptly verified, the person **MUST** immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

d. All suspected cases must be reported to the School Division's Secretary-Treasurer within 24 hours of occurrence.

Compliance

5. The Human Resources Department will ensure that successful completion of the online ***Email Safety – Phishing, Social Engineering and Ransomware Awareness Training*** module from report of individual training profile on PublicSchoolWorks. Staff found non-compliant will be given 10 working days to complete the training. If not completed, the email account and all other access to servers will be suspended;

6. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. The IT Department will provide a monthly report of all suspected Phishing, Malware and Social Engineering attacks to Senior Management. Information will include reports and analytics from Google Security.

Approval Date: September 1, 2019

Reference: Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
ATA Code of Professional Conduct
Freedom of Information and Protection of Privacy Act
FMCSD AP 140, 141, 142, 143, 145, 146, 147, 181, 185