Courriels frauduleux – hameçonnage (phishing)

Fiche étudiant(e)

NIVEAU : Avancé

OBJECTIFS :

- linguistiques :

- consolider son vocabulaire informatique
- pratiquer le vocabulaire en lien avec les courriels frauduleux et l'hameçonnage
- l'impératif

- communicatifs :

- améliorer sa compétence de communication orale
- donner des conseils / des instructions

RESSOURCES COMPLÉMENTAIRES :

- Le vocabulaire informatique de l'OQLF : https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/index.html
- http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-fra.htm

DÉROULEMENT :

1. Voici la situation de communication et votre tâche finale :

Mise en situation :

Vous êtes informaticien et travaillez pour une société qui donne des cours d'informatique à des individus ou à des compagnies privées. Vous devez former des individus ou des employés et les sensibiliser aux bonnes pratiques en matière de sécurité.

Tâche :

Animez un atelier intitulé *Attention aux courriels frauduleux ! Comment se protéger contre l'hameçonnage ?*

Voici ce que vous devez expliquer aux participant(e)s de votre atelier :

- ce qu'est un courriel frauduleux
- les caractéristiques d'un courriel frauduleux
- les phrases types qui peuvent être utilisées dans un courriel frauduleux
- les renseignements que ces courriels souhaitent obtenir (renseignements visés)
- À quoi peuvent servir ces renseignements ?
- Que faire si vous recevez ce genre de courriel ?
- Que faire si vous avez donné des informations personnelles ?

2. Préparez votre atelier en suivant les étapes suivantes.

<u>Étapes à suivre pour préparer votre atelier</u> :

- Faites une recherche sur les courriels frauduleux (hameçonnage) (voir Annexe 1) et

> L'hameçonnage est un terme général utilisé pour décrire l'envoi, par des criminels, de courriels, de messages textes et de sites Web qui sont conçus pour avoir l'air de provenir d'entreprises, d'institutions financières et d'organismes gouvernementaux légitimes bien connus et qui visent à tromper le destinataire afin de lui soutirer des renseignements personnels, financiers ou de nature délicate. On appelle également ce crime « usurpation de marque ».

dégagez une définition à donner à vos participant(e)s. Exemple :

Voici une liste de vocabulaire à maîtriser pour expliquer ce qu'est un courriel frauduleux :

Noms masculins	**Noms féminins**	**Verbes**
envoi	victime	tromper
courriel	entreprise	obtenir
criminel	institution financière	déclencher
message texte	organisme gouvernemental	valider
site web	réaction impulsive	mettre à jour
compte	nouvelle excitante	confirmer
renseignement financier	réponse immédiate	usurper
renseignement personnel	information	vérifier
appel téléphonique	usurpation	avoir accès à
site frauduleux	cible	accéder
numéro	barre d'adresse	ouvrir
mot de passe	assurance sociale	demander
permis de conduire	date de naissance	acheter
compte bancaire	adresse complète	
	carte de crédit	

- Préparez-vous à expliquer aux participant(e)s les caractéristiques d'un courriel frauduleux

- Préparez des phrases types qui peuvent être utilisées dans un courriel frauduleux
- Préparez-vous à expliquer à vos participant(e)s quels sont les renseignements que les courriels frauduleux souhaitent obtenir (renseignements visés)
- Préparez-vous à expliquer à vos participant(e)s à quoi peuvent servir les renseignements qu'ils / elles pourraient fournir en répondant à un courriel frauduleux
- Préparez-vous à donner des conseils à vos participant(e)s pour savoir que faire s'ils / elles reçoivent un courriel frauduleux.
- Préparez-vous à donner des conseils à vos participant(e)s pour savoir que faire s'ils / elles ont donné des informations personnelles en répondant à un courriel frauduleux.
- Au besoin, consultez la fiche *Donner un conseil* (Annexe 2).

3. Animez votre atelier.

ANNEXES

1. COURRIELS FRAUDULEUX ET HAMEÇONNAGE (PHISHING)

Identifiez-le

En quoi consistent l'hameçonnage ou les courriels frauduleux?

L'hameçonnage est un terme général utilisé pour décrire l'envoi, par des criminels, de courriels, de messages textes et de sites Web qui sont conçus pour avoir l'air de provenir d'entreprises, d'institutions financières et d'organismes gouvernementaux légitimes bien connus et qui visent à tromper le destinataire afin de lui soutirer des renseignements personnels, financiers ou de nature délicate. On appelle également ce crime « usurpation de marque ».

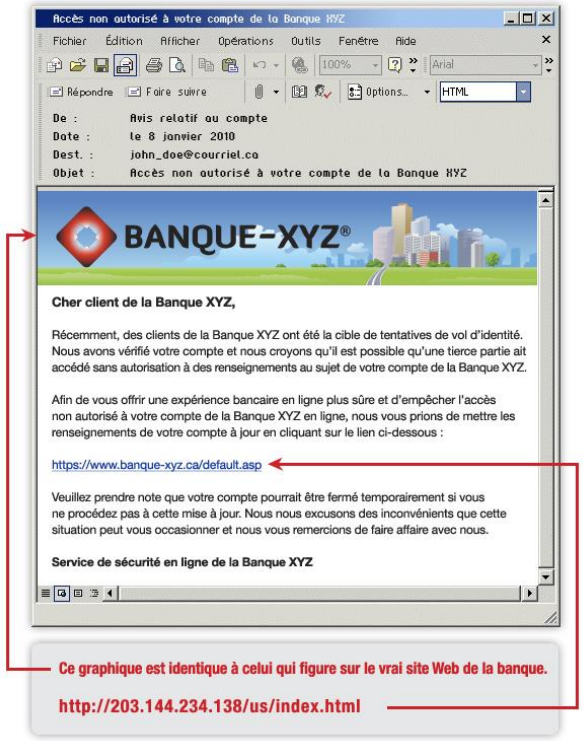
Caractéristiques

- Le contenu d'un courriel ou d'un message texte hameçon vise à déclencher une réaction impulsive de votre part. Ces courriels vous annoncent une nouvelle bouleversante ou excitante et vous demandent une réponse immédiate sous un faux prétexte. Les courriels hameçons ne sont habituellement pas personnalisés.
- En règle générale, les messages hameçons vous demanderont de mettre à jour, de valider ou de confirmer les renseignements de votre compte, à défaut de quoi, les conséquences pourraient être fâcheuses. On pourrait également vous demander de faire un appel téléphonique.
- Bien souvent, le message ou le site Web comporte des logos qui semblent authentiques de même que d'autres renseignements d'identification tirés de sites Web légitimes. Les organismes gouvernementaux, les institutions financières et les services de paiement électronique constituent des cibles courantes pour l'usurpation de marque.

Phrases clés

- *Alerte – virement d'argent par courriel : Nous vous prions de vérifier les renseignements de la transaction ci-dessous …*
- *Dans le cadre des efforts continus que nous déployons pour protéger votre compte et réduire les cas de fraude, nous avons remarqué que votre profil bancaire en ligne a besoin d'être mis à jour…*
- *Cher titulaire de compte en ligne,*
  Votre compte n'est pas accessible à l'heure actuelle …
- *Important message d'intérêt public de la part de…, Vous avez 1 message relatif à la sécurité à lire!*
- *Nous avons le regret de vous informer que nous avons dû bloquer l'accès à votre compte bancaire. Pour réactiver votre compte, composez le (numéro de téléphone).*

Exemple d'un courriel hameçon



** Dans certains cas, le site frauduleux peut modifier la barre d'adresse de votre navigateur pour lui donner une apparence légitime, en affichant notamment l'adresse Web d'un vrai site et un préfixe sécuritaire « https:// ». Prenez l'habitude de vérifier la barre d'adresse du site Web afin de voir si l'adresse est différente de celle inscrite dans le courriel.

Renseignements visés : Votre numéro d'assurance sociale, votre nom complet, votre date de naissance, votre adresse complète, le nom de jeune fille de votre mère, vos noms

d'utilisateur et mots de passe de services en ligne, votre numéro de permis de conduire, vos numéros d'identification personnels (NIP), des renseignements sur vos cartes de crédit (numéros, dates d'expiration et les trois derniers chiffres inscrits à l'endos de votre carte) et vos numéros de comptes bancaires.

Ce à quoi vos renseignements pourraient servir : Grâce à vos renseignements, les fraudeurs peuvent accéder à vos comptes bancaires, ouvrir de nouveaux comptes, virer le solde de vos comptes, demander des prêts, des cartes de crédit et d'autres biens ou services, effectuer des achats, accéder à votre compte de courriel personnel, dissimuler des activités criminelles, recevoir des prestations du gouvernement ou obtenir un passeport.

Si vous recevez l'un de ces courriels suspects :

Signalez-le au Centre antifraude du Canada ou en communiquant avec l'institution financière de laquelle il semble provenir.

Si vous avez reçu l'un de ces courriels suspects et que vous avez fournis sans le savoir des renseignements personnels ou financiers, faites ce qui suit :

- **Étape 1.** Communiquez avec votre banque ou votre institution bancaire ou la compagnie émettrice de votre carte de crédit.
- **Étape 2.** Communiquez avec les agences d'évaluation du crédit et demandez à ce que des alertes à la fraude soient inscrites à vos rapports de solvabilité.
  - Equifax Canada
    Numéro sans frais : 1-800-465-7166
  - TransUnion Canada
    Numéro sans frais : 1-877-525-3823
- **Étape 3.** Communiquez avec votre service de police local.
- **Étape 4.** Signalez toujours l'hameçonnage. Si vous avez répondu à un courriel suspect, signalez-le au Centre antifraude du Canada

Mesures de prévention

- Méfiez-vous des courriels ou des messages texte dans lesquels on vous demande de fournir sur-le-champ des renseignements personnels ou financiers (les institutions financières et les compagnies émettrices de carte de crédit ne demandent pas habituellement à leurs clients de confirmer leurs renseignements par courriel).
- Communiquez avec l'institution ou la compagnie à l'aide d'un numéro de téléphone figurant dans une source sûre, comme un annuaire téléphonique ou un relevé.
- N'envoyez jamais de renseignements personnels ou financiers par courriel.
- Évitez de cliquer sur des liens qui sont incorporés à des courriels et qui prétendent vous diriger vers un site sûr.
- Prenez l'habitude de vérifier la barre d'adresse du site Web afin de voir si l'adresse est différente de celle inscrite dans le courriel.

- Mettez régulièrement à jour les antivirus, les logiciels anti espion, les filtres-courrier et les pare-feu afin de protéger votre ordinateur.
- Plusieurs compagnies et institutions financières légitimes ayant été la cible des hameçonneurs ont publié des coordonnées dont les clients peuvent se servir pour signaler les cas potentiels d'hameçonnage. De plus, elles ont expliqué dans des communiqués en ligne les façons de reconnaître l'hameçonnage et les mesures à prendre pour se protéger contre ce type de fraude.
- Vérifiez régulièrement vos relevés de transactions bancaires, de cartes de crédit et de cartes de débit pour vous assurer que toutes les transactions qui y figurent sont légitimes.

Liens

- Centre antifraude du Canada
- Sécurité publique Canada - Pensez cybersécurité
- Association des banquiers canadiens
- Visa
- Mastercard (anglais seulement)
- American Express
- CIBC

Source: http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-fra.htm

2. DONNER UN CONSEIL

EMPLOI DE L'IMPÉRATIF PRÉSENT

TU (informel)	VOUS (formel)
Allume ton ordinateur !	Allumez votre ordinateur !
Sois prêt à éteindre l'ordinateur !	Soyez prêt à éteindre l'ordinateur !
N'éteins pas l'ordinateur !	N'éteignez pas l'ordinateur !
N'ouvre pas de pièce jointe !	N'ouvrez pas de pièce jointe !
Garde bien cette notice !	Gardez bien cette notice !
Adresse-toi à ton supérieur pour tout conseil !	Adressez-vous à votre supérieur pour tout conseil !
N'oublie pas d'appeler ce client !	N'oubliez pas d'appeler ce client !

EMPLOI DE L'EXPRESSION « IL FAUT ... »

« il faut + nom »

Pour travailler dans un service à la clientèle, il faut de l'entregent.
Pour protéger son ordinateur, il faut un antivirus.

« il faut + infinitif »

Pour protéger son ordinateur, il faut acheter un antivirus.
Pour travailler dans un service à la clientèle, il ne faut pas être stressé.

Remarque :

Pour exprimer un conseil, on conjugue également l'expression « il faut » au conditionnel présent (« il faudrait ...»).
Il faudrait trouver une solution.
Il faudrait acheter un nouvel antivirus.
Il ne faudrait pas couper la parole au client.

EMPLOI DU VERBE *DEVOIR* SUIVI DE L'INFINITIF

TU (informel)	VOUS (formel)
Pour créer un fichier client, tu dois utiliser Excel.	Pour créer un fichier client, vous devez utiliser Excel.
Pour installer ton ordinateur, tu dois appeler un technicien.	Pour installer votre ordinateur, vous devez appeler un technicien.
Tu dois t'adresser à ton supérieur pour des questions techniques.	Vous devez vous adresser à votre supérieur pour des questions techniques.

Remarque:

Pour exprimer un conseil, on conjugue également le verbe *devoir* au conditionnel présent (tu devrais, vous devriez, ...).

TU (informel)	VOUS (formel)
Pour créer un fichier client, tu devrais utiliser Excel.	Pour créer un fichier client, vous devriez utiliser Excel.
Pour installer ton ordinateur, tu devrais appeler un technicien.	Pour installer votre ordinateur, vous devriez appeler un technicien.

Avec la contribution financière de :

Office québécois de la langue française
Québec