RANÇONGICIELS
Fiche étudiant(e)

NIVEAU : Intermédiaire

OBJECTIFS **:**

Linguistiques :

- pratiquer le vocabulaire en lien avec les rançongiciels
- pratiquer le vocabulaire en lien avec les réseaux sans fil
- l'impératif

Communicatifs :

- donner des conseils

RESSOURCES COMPLÉMENTAIRES :

- Le vocabulaire informatique de l'OQLF : https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/index.html
- Le texte intégral portant sur les rançongiciels qui a servi de source d'inspiration dans la réalisation de cet atelier, disponible à l'adresse : https://www.pensezcybersecurite.gc.ca/cnt/prtct-dvcs/hm-ntwrks-fr.aspx
- http://www.rcmp-grc.gc.ca/scams-fraudes/ransomware-rancongiciels-fra.htm

DÉROULEMENT :

Mise en situation :

Vous êtes informaticien et travaillez pour une société qui donne des ateliers informatiques 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 deux ateliers à l'intention d'un public général, consommateur de produits informatiques (pas spécialisé en informatique). Le premier a pour objet les rançongiciels, alors que le deuxième porte sur la protection des réseaux sans fil à domicile. Imaginez que les participant(e)s à vos ateliers sont vos camarades de classe.

1. Préparez votre premier atelier.

Atelier 1 – ATTENTION AUX RANÇONGICIELS

Vous utilisez un ordinateur personnel à la maison ou dans votre compagnie ?

Comment se protéger?

Étapes à suivre pour préparer votre premier atelier :

- Faites une recherche sur les rançongiciels (voir Annexe 1) et dégagez une définition à donner à vos participant(e)s. Exemple :

Qu'est-ce qu'un rançongiciel?

Il s'agit d'un logiciel malveillant, aussi appelé maliciel, qui infecte un ordinateur et qui bloque l'accès au système ou aux données. Il exige ensuite que la victime paie une rançon afin de ravoir accès à ses renseignements. Actuellement, les rançongiciels les plus courants sont ceux qui cryptent toutes les données. Une alerte s'affiche à l'écran de la victime indiquant que ses fichiers ont été cryptés (ou un message similaire, selon le type de rançongiciel).

- Voici une liste de vocabulaire à maîtriser pour expliquer ce qu'est un rançongiciel :

Noms masculins	**Noms féminins**	**Verbes**
maliciel	victime	paniquer
professionnel de la TI	menace	utiliser
fichiers	une personne (digne de confiance)	appeler
incident	données	isoler
service de police		récupérer
Centre antifraude du Canada (CAFC)		signaler

- Pour illustrer vos explications, donnez comme référence le site ci-dessous où vos participants pourront trouver des exemples réels :

http://www.rcmp-grc.gc.ca/scams-fraudes/ransomware-rancongiciels-fra.htm

- Préparez une visite guidée de ce site à l'intention de vos participant(e)s en insistant sur les informations les à retenir.

- Préparez la question suivante à poser à vos participant(e)s : « Comment se protéger contre les rançongiciels ? Quelles sont les précautions à prendre ? »

- Préparez la liste de vocabulaire suivante à distribuer à vos participant(e)s. Vous leur demanderez d'utiliser au moins 10 mots dans leur réponse.

Noms masculins	**Noms féminins**	**Verbes**
maliciel	victime	bloquer
accès à	alerte	infecter
fichiers	écran	payer
lien	données	crypter
message	pièce jointe	cliquer
destinateur	source	s'afficher
courriels	sauvegarde	sauvegarder
renseignement	information	ouvrir
système	copie	avoir accès à
logiciel de sécurité		déconnecter
antivirus		restreindre
appareil		
privilège administratif		

- Au besoin, consultez la fiche *Donner un conseil* (Annexe 3).

2. Une fois la préparation terminée, animez votre premier atelier.

3. Préparez votre deuxième atelier.

Atelier 2 – PROTECTION DES RÉSEAUX SANS FIL À DOMICILE

Vous êtes informaticien et travaillez pour une société qui donne des ateliers informatiques à des individus.

Vous devez former des individus et les sensibiliser aux réseaux sans fil

Vous devrez expliquer :

- Ce qu'est un réseau sans fil,
- ses avantages,
- les risques,
- les précautions,
- comment se protéger,
- contre quoi

Étapes à suivre pour préparer votre deuxième atelier :

- Effectuez une recherche sur les réseaux sans fil à domicile (voir Annexe 2) et dégagez quelques informations de base à donner à vos participant(e)s. Exemple :
- Préparez une liste de conseils à donner pour protéger son réseau sans fil. (Annexe 2)

Les réseaux sans fil permettent le raccordement d'appareils ensemble au moyen de signaux radio au lieu de câbles ou de fils. Ils procurent flexibilité et commodité et, comme vous l'avez peut-être deviné, comportent un risque accru. Les téléphones intelligents et les appareils mobiles qui sont automatiquement sans fil présentent leur propre ensemble de risques et nécessitent leurs propres précautions, au sujet desquels vous pouvez en apprendre davantage ici.

Voici une liste de vocabulaire qui pourra vous aider :

Noms masculins	**Noms féminins**	**Verbes**
Signaux radio	flexibilité	utiliser
appareil	commodité	Infecter
Câble /fil	Protection	protéger
raccordement		raccorder
Téléphone intelligent	Précaution	
Appareil mobile	Mauvaises intentions	
Mot de passe	Connexion personnelle	
intrus	information	
téléchargement		télécharger
accès		accéder
appareil		voler
Privilège administratif	Bande passante	Limiter

4. Une fois la préparation terminée, animez votre deuxième atelier.

ANNEXES

POUR ALLER PLUS LOIN

1. RANÇONGICIELS

Reconnaissez-les, rejetez-les et signalez-les!
Le nombre d'incidents liés aux rançongiciels au Canada augmente à un rythme alarmant. En 2015, les Canadiens ont été touchés par 1600 attaques de rançongiciels par jour et, en septembre 2016, le nombre d'incidents avait presque doublé. Et il s'agit seulement des cas connus. Malheureusement, de nombreux incidents ne sont pas signalés.

Reconnaissez-les!

Qu'est-ce qu'un rançongiciel?
Il s'agit d'un logiciel malveillant, aussi appelé maliciel, qui infecte un ordinateur et qui bloque l'accès au système ou aux données. Il exige ensuite que la victime paie une rançon afin de ravoir accès à ses renseignements. Actuellement, les rançongiciels les plus courants sont ceux qui cryptent toutes les données. Une alerte s'affiche à l'écran de la victime indiquant que ses fichiers ont été cryptés (ou un message similaire, selon le type de rançongiciel). Voici un exemple réel :

Rejetez-les!

Utilisateur d'un ordinateur personnel - Comment puis-je me protéger?

- Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe d'un courriel dont vous ne connaissez pas le destinateur.
- Ne fournissez aucun renseignement personnel au téléphone ou en ligne si vous ne connaissez pas la source.
- Installez uniquement des logiciels de confiance.
- Effectuez régulièrement une sauvegarde de votre système et de vos données et conservez des copies sur un disque dur distinct et amovible. N'oubliez pas de vous déconnecter dès que vous avez terminé! Si possible, vérifiez les copies de votre sauvegarde sur un ordinateur distinct ayant un autre système d'exploitation.
- Installez un logiciel de sécurité réputé sur tous vos appareils, y compris les ordinateurs personnels, les téléphones cellulaires et les tablettes.
- Sécurisez votre routeur sans fil.
- Désactivez le partage de fichiers et les postes à distance.

- Veillez à ce que tous vos logiciels, y compris les logiciels antivirus, soient à jour sur tous vos appareils, y compris les ordinateurs personnels, les téléphones cellulaires et les tablettes.

Utilisateur d'un ordinateur professionnel - Comment puis-je protéger mon entreprise?

- Formez les employés et sensibilisez-les aux bonnes pratiques en matière de sécurité.
- Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe d'un courriel dont vous ne connaissez pas le destinateur.
- Utilisez un logiciel de sécurité réputé.
- Restreignez les privilèges administratifs.
- Effectuez régulièrement une sauvegarde de votre système et de vos données sur un nuage ou sur un média amovible, comme un disque dur externe qui n'est pas constamment connecté au serveur. Si possible, vérifiez les copies de votre sauvegarde sur un ordinateur distinct ayant un autre système d'exploitation.
- Créez une liste des applications autorisées (liste blanche) pour empêcher l'exécution de logiciels malveillants ou non autorisés.
- Veiller à ce que tous les logiciels, y compris les logiciels antivirus, soient à jour sur tous les ordinateurs, serveurs et appareils, notamment les téléphones cellulaires et les tablettes.
- Élaborez un plan de continuité des activités et un plan d'intervention en cas d'incident.

Signalez-les!

Utilisateur d'un ordinateur personnel - Comment dois-je réagir?

Si vous devenez une victime, ne paniquez pas. Cessez immédiatement d'utiliser votre ordinateur. Appelez un professionnel de la TI digne de confiance qui pourra essayer d'isoler la menace.

Signalez l'incident à votre service de police local. N'oubliez pas qu'il est important de signaler tous les incidents; ils constituent un outil précieux pour les enquêteurs.

Communiquez également avec le Centre antifraude du Canada (CAFC) en signalant l'incident en ligne en tout temps. Cliquez sur l'onglet « Signaler un incident », puis sur le lien menant au « Système de signalement des fraudes » ou appelez le CAFC en composant le 1-888-495-8501, de 8 h 30 à 17 h (HNE), du lundi au vendredi.

Vous pouvez obtenir de **l'aide supplémentaire** sur le site Web No More Ransom. Ce site est un outil visant à aider les victimes à récupérer leurs données. Il a été créé par des autorités policières et des entreprises spécialisées en sécurité de l'information à l'échelle mondiale.

Lignes directrices supplémentaires :

- Protégez-vous

Utilisateur d'un ordinateur professionnel - Comment mon entreprise doit-elle réagir?

Cessez immédiatement d'utiliser votre ordinateur. Si vous y avez accès, consultez votre service de TI ou un spécialiste de la TI.

Les infrastructures essentielles, les entreprises et les gouvernements provinciaux, territoriaux et municipaux doivent immédiatement signaler l'incident auprès du Centre canadien de réponse aux incidents cybernétiques (CCRIC) par courriel : ps.cyberincident.sp@canada.ca.
Le CCRIC contribue aux mesures d'atténuation et de prévention.
Nous vous encourageons à entamer une enquête criminelle en signalant l'incident au service de police local. Informez-en ensuite le CCRIC. N'oubliez pas qu'il est important de signaler tous les incidents; ils constituent un outil précieux pour les enquêteurs.
Vous pouvez également communiquer avec le Centre antifraude du Canada (CAFC) en signalant l'incident en ligne en tout temps. Cliquez sur l'onglet « Signaler un incident », puis sur le lien menant au « Système de signalement des fraudes » ou appelez le CAFC en composant le 1-888-495-8501, de 8 h 30 à 17 h (HNE), du lundi au vendredi.

Lignes directrices supplémentaires :

- Guide Pensez cybersécurité pour les petites et moyennes entreprises

Nous vous encourageons fortement à ne pas payer la rançon **pour les raisons suivantes :**

- Rien ne garantit que vos données soient récupérées.
- Vous risquez d'être à nouveau victime d'extorsion après le paiement de la rançon initiale.
- Vous pouvez faire de vous une cible future.
- L'extorsion par l'entremise d'un rançongiciel est une infraction criminelle. L'argent que vous enverrez à la personne responsable servira à financer des criminels ou des organisations criminelles et les motivera à faire d'autres victimes.

Nous savons qu'il peut y avoir des raisons légitimes de payer la rançon, comme le risque éventuel de ne plus avoir accès à vos données, car vous n'avez pas de sauvegarde. Nous vous encourageons à signaler tous les incidents, même si vous avez payé la rançon exigée par les extorqueurs.

Source : https://www.pensezcybersecurite.gc.ca/cnt/prtct-dvcs/hm-ntwrks-fr.aspx

2. LA PROTECTION DE VOTRE RÉSEAU SANS FIL À DOMICILE

Les réseaux sans fil permettent le raccordement d'appareils ensemble au moyen de signaux radio au lieu de câbles ou de fils. Ils procurent flexibilité et commodité et, comme vous l'avez peut-être deviné, comportent un risque accru.
Les téléphones intelligents et les appareils mobiles qui sont automatiquement sans fil présentent leur propre ensemble de risques et nécessitent leurs propres précautions, au sujet desquels vous pouvez en apprendre davantage ici.

La protection de votre réseau sans fil à domicile

Lorsque vous utilisez un réseau Wi-Fi, la mesure de protection minimale que vous devez absolument prendre est d'assurer la protection par mot de passe et chiffrement sans fil (WPA2 dans les endroits où elle est disponible, autrement WPA) de tous vos appareils, y compris votre routeur sans fil. Voici pourquoi vous devriez protéger votre réseau Wi-Fi à domicile des étrangers et des intrus :

- Un réseau non sécurisé permet à quiconque qui est muni d'un appareil Wi-Fi dans votre rayon d'utilisation d'accéder à votre connexion Internet personnelle et à vos appareils et ordinateurs.
- Vous pourriez fournir un service Wi-Fi « gratuit » à tous vos voisins. De nombreux utilisateurs malhonnêtes se promènent par ailleurs à la recherche de réseaux Wi-Fi non sécurisés à exploiter.
- Les intrus peuvent voler votre bande passante et votre capacité d'utilisation pour télécharger des fichiers volumineux comme des films ou des jeux, vous laissant une grosse facture ou limitant votre utilisation et vos vitesses de téléchargement.
- Vous pourriez être tenu responsable de gestes criminels menés au moyen de votre réseau non sécurisé – même si vous n'étiez au courant de rien à ce sujet!
- Votre historique de navigation, vos mots de passe et vos données de connexion ainsi que le contenu de votre messagerie électronique non sécurisés seront tous facilement accessibles.
- On pourra accéder à vos fichiers communs non sécurisés, les copier ou les supprimer.
- Vos périphériques Wi-Fi non sécurisés, comme vos imprimantes ou vos systèmes de jeu vidéo, seront tous facilement accessibles.
- Les réseaux non sécurisés figurent immédiatement comme réseaux non verrouillés et vulnérables sur les appareils de balayage des réseaux sans fil. Ils constituent une proie facile.
- Même un réseau sécurisé WPA2 peut-être compromis par une attaque par réinstallation de clé, ce qui peut laisser vulnérables les informations sensibles.

Maintenant que vous savez pourquoi il est tellement important de sécuriser votre réseau Wi-Fi voici quelques autres points à vous rappeler :

- Lorsque vous établissez le mot de passe de votre réseau Wi-Fi à domicile, suivez toujours les directives d'établissement des mots de passe forts.
- Essayez de limiter votre rayon d'utilisation à votre maison en plaçant votre routeur le plus près possible du milieu de vos locaux d'habitation dans la mesure du possible, au lieu de le placer près des fenêtres.
- Assurez-vous de mettre à date les logiciels et les systèmes d'exploitation de chaque appareil relié à votre réseau, dont votre routeur, vos ordinateurs, des téléphones intelligents, et des appareils intelligents, afin de protéger l'ensemble de votre réseau.
- Pourquoi ne pas utiliser le chiffrement sans fil? Vous pouvez poser deux gestes à cet égard : premièrement, prenez soin d'activer le chiffrement SSL dans les paramètres des sites que vous visitez (comme votre courriel). Deuxièmement, visitez la version

HTTPS sécurisée des sites plutôt que le site http normal non sécurisé en ajoutant simplement un « S » à l'adresse URL du site Web.

- Une configuration optimale de votre routeur vous permettra de maximiser la protection possible de votre installation particulière. Vous devez peut-être consulter le manuel de votre routeur ou communiquer avec votre fournisseur.

Source : https://www.pensezcybersecurite.gc.ca/cnt/prtct-dvcs/hm-ntwrks-fr.aspx

3. 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 toute information !
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 clients, tu dois utiliser Excel.	Pour créer un fichier clients, 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 clients, tu devrais utiliser Excel.	Pour créer un fichier clients, 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