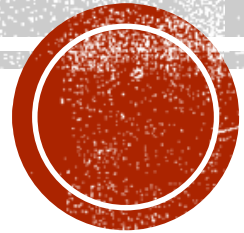
ÉVEIL À LA SÉCURITÉ

Par Marc Gaudreau, CISSP



OBJECTIFS DE LA PRÉSENTATION

- Comprendre les risques et les menaces
- Reconnaître une menace (dans le doute, abstenez-vous)
- Mesures de prévention de base
- Comportements à risque

RISQUES DE CYBER SÉCURITÉ

- Qu'il s'agisse de procéder à des opérations bancaires, entrer en contact avec des amis, ou examiner le marché de l'immobilier dans sa région, l'utilisation d'Internet fait maintenant partie du quotidien.
- Ce que peu de gens savent de cette ressource incroyable c’est qu'elle constitue également un lieu de prédilection pour ceux qui s'adonnent à des activités criminelles. L'information de chacun peut être suivie et devient ainsi compromise.
- Si l'on prend le temps de se renseigner à propos des menaces et des risques communs, la sécurité et la protection en ligne sont relativement simples.

GROUPE HELIOS

MENACES COURANTES À CONNAÎTRE

- Cheval de Troie
- Détournement de domaine
- Écoute électronique par réseau Wi-Fi
- Hameçonnage
- Logiciels espions
- Mystification
- Piratage
- Pourriels
- Programmes malveillants
- Rançongiciels
- Réseau de Zombie
- Vers informatiques
- Virus

GROUPE HELIOS

CHEVAL DE TROIE

- Un cheval de Troie n'est peut pas être un terme avec lequel vous êtes familier, mais il y a de fortes chances que vous ou quelqu'un que vous connaissez en ait déjà été touché.
- **De quoi s'agit-il?**
- Un programme malveillant qui a l'apparence d'un logiciel légitime ou qui y est intégré. Il s'agit d'un fichier exécutable qui s'installera et sera lancé automatiquement une fois téléchargé.
- **Quelles sont les conséquences?**
- Les chevaux de Troie suppriment les fichiers.
- Ils utilisent votre ordinateur pour en pirater d'autres.
- Ils vous observent par l'intermédiaire de votre caméra Web.
- Ils enregistrent vos frappes de claviers (comme les numéros de carte de crédit entrés pour faire des achats en ligne);
- Ils enregistrent les noms d'utilisateurs, les mots de passe et d'autres informations personnelles.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

DÉTOURNEMENT DE DOMAINE

- Le détournement de domaine est un type de fraude en ligne.
- **De quoi s'agit-il?**
- Un moyen de vous diriger vers un site malveillant et illégitime en redirigeant l'adresse URL légitime. Même si l'adresse URL est entrée correctement, il peut encore être redirigé vers un faux site.
- **Quelles sont les conséquences?**
- Le détournement de domaine a comme objectif de vous convaincre que le site est réel et légitime par mystification ou en ayant exactement la même apparence que le site actuel et ce, dans les moindres détails. Par conséquent, vous pourriez entrer vos informations personnelles et, sans le savoir, les donner à quelqu'un de malintentionné.
- Apprenez-en davantage sur les façons de protéger votre identité.

GROUPE HELIOS

ÉCOUTE ÉLECTRONIQUE PAR RÉSEAU WI-FI

- L'écoute électronique par réseau Wi-Fi est une autre méthode employée par les cybercriminels pour obtenir de l'information personnelle.
- **De quoi s'agit-il?**
- Écoute virtuelle de l'information qui est partagée sur un réseau Wi-Fi non sécurisé (non chiffré).
- **Quelles sont les conséquences?**
- Grâce à l'écoute électronique par réseau Wi-Fi, il est possible d'accéder à votre ordinateur grâce à l'équipement adéquat.
- Les cybercriminels volent vos informations personnelles, y compris vos renseignements, pour procéder à une ouverture de session et les mots de passe.
- Apprenez-en davantage à propos des réseaux Wi-Fi.

GROUPE HELIOS

HAMEÇONNAGE

- La technique d'hameçonnage est utilisée le plus souvent par des cybercriminels, car elle est facile à exécuter et peut produire les résultats recherchés sans avoir à fournir trop d'effort.
- **De quoi s'agit-il?**
- De faux courriels, messages texte et sites Web conçus pour avoir exactement la même apparence que ceux des entreprises réelles ou qui semblent être envoyé par de vraies entreprises. Les criminels les envoient pour vous voler votre information personnelle et financière. Ceci est également connu sous le nom de « mystification ».
- **Quelles sont les conséquences?**
- Les différentes techniques d'hameçonnage ont comme objectifs de vous inciter à fournir aux cybercriminels vos informations. Ces derniers vous demandent de mettre à jour, de valider ou de confirmer votre compte. Les méthodes sont souvent présentées de façons officielles et intimidantes pour vous encourager à prendre les mesures nécessaires.
- L'hameçonnage permet de fournir aux cybercriminels votre nom d'utilisateur et vos mots de passe afin qu'ils puissent accéder à vos comptes (compte bancaire en ligne, les comptes commerciaux, etc.) et voler vos numéros de carte de crédit.
- Apprenez-en davantage sur les façons de protéger votre identité.

GROUPE HELIOS

LOGICIELS ESPIONS

- Les logiciels espions et publicitaires sont souvent utilisés par des tiers pour s'infiltrer dans un ordinateur.
- **De quoi s'agit-il?**
- Un logiciel qui recueille vos renseignements personnels à votre insu. Il se présente souvent sous la forme d'un téléchargement « gratuit » et est automatiquement installé avec ou sans votre autorisation. Il est difficile de le supprimer complètement et il infectera possiblement votre ordinateur avec de nouveaux virus.
- **Quelles sont les conséquences?**
- Les logiciels espions et publicitaires recueillent vos informations sans que vous le sachiez et les font ensuite parvenir à des tiers.
- Ils envoient vos noms d'utilisateur, vos mots de passe, vos habitudes de navigation, votre liste de contacts, vos applications téléchargées, vos paramètres et même la version de votre système d'exploitation à des tiers.
- Ils modifient le fonctionnement de votre ordinateur à votre insu.
- Ils vous dirigent vers des sites indésirables ou vous inondent d'annonces incontrôlables intruses.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

MYSTIFICATION

- Cette technique est souvent utilisée conjointement avec l'hameçonnage dans le but de vous voler vos informations.

- **De quoi s'agit-il?**
- La création d'un faux site web ou d'une fausse adresse courriel pour qu'il ou qu'elle semble provenir d'une source légitime. Une adresse courriel peut même comprendre votre propre nom ou celui d'une de vos connaissances. Il est ainsi difficile de savoir si l'expéditeur est bien réel.
- **Quelles sont les conséquences?**
- La mystification permet d'envoyer des pourriels en utilisant votre adresse courriel ou une variation de votre adresse courriel, à votre liste de contacts.
- Elle permet de recréer les sites Web qui ressemblent aux sites authentiques. Il pourrait s'agir de sites d'institutions financières ou d'autres sites qui exigent de se connecter ou de fournir d'autres informations personnelles.
- Apprenez-en davantage sur les façons de protéger votre identité.

GROUPE HELIOS

PIRATAGE

- Le piratage est un terme utilisé pour décrire les mesures prises par quelqu'un qui accède à un ordinateur sans l'autorisation du propriétaire. Grâce à la disponibilité d'informations en ligne sur les outils, les techniques et les programmes malveillants, il est assez facile, même pour des gens qui ne sont pas spécialistes, d'entreprendre ce genre d'activité malveillante.
- **De quoi s'agit-il?**
- Le processus par lequel les cybercriminels réussissent à avoir accès à votre ordinateur.
- **Quelles sont les conséquences?**
- Les pirates informatiques trouvent les failles (ou des bogues déjà existants) des paramètres de sécurité et les exploitent afin d'avoir accès à de l'information.
- Le piratage permet d'installer des chevaux de Troie offrant ainsi une porte dérobée aux pirates afin qu'ils pénètrent dans l'ordinateur et cherchent l'information.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

POURRIELS

- Le pourriel est l'une des méthodes les plus courantes tant pour envoyer des informations aux personnes non méfiantes que pour en obtenir. Le Canada s'est doté d'une loi, la Loi canadienne anti-pourriel, et vous pouvez en apprendre davantage à son sujet en consultant le site Web http://combattrelepourriel.gc.ca.
- **De quoi s'agit-il?**
- La distribution de masse de messages non sollicités, de publicités ou de pornographie à des adresses qui peuvent être facilement trouvés sur Internet à travers les sites de réseaux sociaux, entre autres, les sites Web d'entreprises et les blogues personnels.
- La Loi canadienne anti-pourriel s'applique à tous les messages électroniques commerciaux. Un message électronique commercial est un message électronique qui encourage la participation à une activité commerciale, indépendamment de la présence d'une attente raisonnable de profit.
- **Quelles sont les conséquences?**
- Les pourriels vous importunent avec des courriels indésirables.
- Ils imposent un fardeau aux fournisseurs de services de communication et aux entreprises, car ils doivent filtrer les messages électroniques.
- Ils tentent de vous hameçonner afin d'obtenir vos informations en vous incitant à suivre des liens ou en vous offrant des promotions et des offres qui sont trop belles pour être vraies.
- Ils permettent aux programmes malveillants, aux escroqueries, à la fraude et aux menaces d'atteindre votre ordinateur et ainsi créer un risque pour votre vie privée.
- Apprenez-en davantage à propos des pourriels.

GROUPE HELIOS

PROGRAMMES MALVEILLANTS

- Les programmes malveillants sont l'une des façons les plus courantes d'infiltrer un ordinateur ou de l'endommager.
- **De quoi s'agit-il?**
- Un programme malveillant qui infecte votre ordinateur comme les virus informatiques, les chevaux de Troie, les logiciels espions et publicitaires.
- **Quelles sont les conséquences?**
- Les programmes malveillants vous intimident avec des logiciels de sécurité non autorisés aussi appelés épouvanticiels. Il s'agit habituellement d'un message d'avertissement qui s'affiche précisément pour vous avertir que votre ordinateur rencontre un problème de sécurité ou pour vous donner d'autres renseignements erronés.
- Ils reformatent le disque dur de l'ordinateur touché entraînant ainsi la perte de toutes informations qui s'y trouvaient.
- Ils modifient ou suppriment les fichiers.
- Ils volent de l'information de nature délicate.
- Ils envoient des courriels en votre nom.
- Ils prennent le contrôle de votre ordinateur et de tous les logiciels qui sont en marche.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

RANÇONGICIEL

- **De quoi s'agit-il?**
- Un rançongiciel est un type de maliciel qui restreint l'accès à votre ordinateur ou à vos fichiers et qui affiche un message où l'on exige un paiement afin de retirer la restriction. Les deux principaux vecteurs d'infection semblent être les courriels d'hameçonnage contenant des pièces jointes malveillantes et les écrans flash publicitaires sur les sites Web.
- **Ce que cela peut faire**
- Il existe deux types communs de rançongiciel :
- le rançongiciel avec verrouillage de l'écran : il affiche une image qui vous empêche d'accéder à votre ordinateur;
- le rançongiciel avec chiffrement : il chiffre les fichiers sur le lecteur de disque dur de votre système, et parfois ceux qui sont stockés dans les lecteurs réseau partagés, les dispositifs de stockage USB, les disques durs externes et même certains systèmes de stockage en nuage, vous empêchant de les ouvrir.
- Le rançongiciel affichera un avis indiquant que vos données ou votre ordinateur ont été verrouillés et exigeant que vous effectuiez un paiement afin de récupérer l'accès. Parfois, l'avis indique que les autorités ont détecté une activité illégale sur votre ordinateur et que le paiement constitue une amende destinée à éviter des poursuites.

GROUPE HELIOS

RANÇONGICIEL

- **Ce que vous pouvez faire**
- Ne payez pas la rançon. Ces menaces sont destinées à vous effrayer et à vous intimider et ne proviennent pas d'un organisme d'application de la loi. Même si vous envoyez un paiement, rien ne garantit que vous récupériez l'accès à votre système.
- Si votre ordinateur a été infecté (c.-à-d. que vous êtes dans l'impossibilité d'y accéder ou que vos fichiers ont été chiffrés), communiquez avec un technicien ou spécialiste en informatique de bonne réputation afin de savoir si votre ordinateur peut être réparé et si vos données peuvent être récupérées.
- Afin de réduire les impacts d'une infection par rançongiciel, assurez-vous de faire une copie de sécurité de vos données sur un lecteur amovible externe de stockage. Il est possible que vos données demeurent inaccessibles, alors une copie de sécurité pourrait s'avérer être d'une très grande valeur.
- Pour signaler l'incident, veuillez communiquer avec votre service de police local et avec le Centre antifraude du Canada, au 1-888-495-8501 ou à http://www.antifraudcentre-centreantifraude.ca/.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

RÉSEAUX DE ZOMBIES

- Si vous n'avez jamais entendu parler de réseaux de zombies, c'est probablement, parce qu'ils passent souvent inaperçus.
- **De quoi s'agit-il?**
- Un ensemble de robots Web ou de robots qui créent une armée d'ordinateurs infectés (appelés « zombies ») et qui sont contrôlés à distance par l'initiateur. Votre ordinateur en fait peut-être partie sans que vous ne le sachiez.
- **Quelles sont les conséquences?**
- Les réseaux de zombies envoient des pourriels contenant des virus.
- Ils répandent toutes sortes de programmes malveillants.
- Ils utilisent votre ordinateur dans le cadre d'attaques par déni de service contre d'autres systèmes.

GROUPE HELIOS

VERS INFORMATIQUES

- Les vers informatiques sont une menace courante pour les ordinateurs et pour l'utilisation d'Internet dans son ensemble.
- **De quoi s'agit-il?**
- Un ver informatique, contrairement à un virus, travaille seul sans avoir à se joindre à des fichiers ou des programmes. Il vit dans la mémoire de votre ordinateur, n'endommage pas ou ne modifie pas le disque dur et se propage en s'envoyant lui-même à d'autres ordinateurs en réseau, que ce soit au sein d'une entreprise ou d'Internet.
- **Quelles sont les conséquences?**
- Ils se propagent à chaque personne dans votre liste de contacts.
- Ils provoquent d'énormes dégâts en éteignant certaines composantes d'Internet, en faisant des ravages sur un réseau interne et en causant aux entreprises touchées des pertes énormes de revenus.
- Apprenez-en davantage sur les façons de protéger votre ordinateur.

GROUPE HELIOS

VIRUS

- La plupart des gens ont déjà entendu parler de virus informatiques, mais peu savent exactement ce qu'ils sont ou ce qu'ils font.
- **De quoi s'agit-il?**
- Il s'agit de programmes informatiques malveillants qui sont souvent envoyés en pièce jointe par courriel ou par l'intermédiaire d'un téléchargement. Les virus tentent d'infecter votre ordinateur, ainsi que les ordinateurs de chacune des personnes apparaissant dans votre liste de contacts. Le simple fait de visiter un site peut lancer le téléchargement automatique d'un virus.
- **Quelles sont les conséquences?**
- Les virus envoient des pourriels.
- Ils fournissent aux criminels l'accès à votre ordinateur et à votre liste de contacts.
- Ils trouvent et scrutent vos informations personnelles sur votre ordinateur, par exemple, mots de passe.
- Ils piratent votre navigateur Internet.
- Ils désactivent vos paramètres de sécurité.
- Ils affichent des publicités indésirables.
- Lorsqu'un programme est exécuté, le virus qui y est attaché peut s'infiltrer dans le disque dur, mais aussi dans les clés USB et les disques durs externes. Toute pièce jointe créée en utilisant ce programme et envoyée pourrait infecter les personnes à qui elle a été envoyée.

GROUPE HELIOS

VIRUS

- **Comment saurez-vous si votre ordinateur a été infecté?**
- Quels sont les points à vérifier?
  L'ordinateur prend plus de temps à démarrer, il redémarre par lui-même ou ne démarre simplement pas.
- L'ordinateur prend beaucoup de temps à lancer un programme.
- Les fichiers et les données ont disparu.
- Le système et les programmes tombent constamment en panne.
- La page d'accueil installée n'est plus la même (à noter que cela pourrait être causé par un logiciel publicitaire qui a été installé sur l'ordinateur).
- Les pages Web prennent du temps à se charger.
- L'écran de l'ordinateur semble déformé.
- Les programmes sont exécutés sans votre contrôle.
- Si vous soupçonnez un problème, assurez-vous que votre logiciel de sécurité soit à jour et lancez-le pour vérifier si un virus a infecté votre système. Si rien n'a été trouvé, ou si vous n'êtes pas certain de ce qu'il faut faire, demandez de l'aide technique

GROUPE HELIOS

LA VIE EN LIGNE

- Courriels, réseaux sociaux ou achats en ligne - Internet est le lien qui dirige vers à peu près tout. Voilà pourquoi la sécurité en ligne ne devrait jamais quitter notre esprit.
- Courriel
  Les risques associés aux comptes courriel.
- Banques et finances
  Les différentes façons de voir son information bancaire compromise.
- Réseautage social
  Protéger l'information personnelle partagée et éviter les escroqueries.
- Mobilité
  Les attaques contre les appareils mobiles : en quoi consistent-elles?
- Achats en ligne
  Connaître les risques associés aux achats et aux enchères en ligne.
- Jeux en ligne et divertissement
  Les risques associés au divertissement, aux jeux et aux concours en ligne.
- Téléchargement et partage de fichiers
  Comment télécharger en toute sécurité.
- Voix sur IP
  Les menaces associées aux appels téléphoniques en ligne

GROUPE HELIOS

QUESTIONS ?

http://support.groupehelios.com/