ROCKY CREDIT UNION

English	French
PRIVACY AND SECURITY: STAYING SAFE ON THE INTERNET	SÉCURITÉ SUR INTERNET
We are committed to protecting your privacy and safeguarding your personal and financial information. Online banking makes managing your finances easy and convenient. However, there are some simple measures you should take whenever you go online to access your accounts. Because your online security is our priority, we have compiled information and suggestions to keep your personal and financial information safe and secure.	Nous nous sommes engagés à protéger votre vie privée et à sauvegarder vos renseignements personnels et financiers. Les services bancaires en ligne vous permettent de gérer vos finances facilement et aisément. Toutefois, il y a des mesures à prendre et de bonnes pratiques d'usage à suivre lors des connexions pour accéder à vos comptes. Comme votre sécurité est notre priorité, nous avons compilé des suggestions et des conseils afin de contrer les menaces reliées à l'Internet.
Section 1: SECURITY GUARANTEE	**Section 1: GARANTIE DE SÉCURITÉ**
Our online banking system is safeguarded with the best security available in a commercial environment, ensuring that your information is protected while data is transmitted between your computer and our banking server.	Notre système de services bancaires en ligne est protégé grâce aux meilleurs systèmes de sécurité disponibles dans les environnements commerciaux, assurant ainsi que vos données soient protégées lorsqu'elles circulent entre votre ordinateur et notre serveur bancaire.
Encryption	**Chiffrement**
Internet encryption protects your information while it is in transit between your computer and our systems. Encryption ensures that data cannot be read or altered because the information is scrambled. Our online banking website uses a 128 bit SSL, encrypting both request and response transactions, through a secure connection. To establish a secure connection, make sure that the prefix of our website address in your browser reads 'https' (and not simply 'http'). All the browsers we support meet this requirement. If yours doesn't, please download the appropriate encryption support from your browser's supplier.	Le chiffrement protège vos données pendant qu'elles circulent entre votre ordinateur et nos systèmes. Comme les données sont brouillées, le chiffrement assure que les données ne peuvent être ni lues ni modifiées. Notre site Web est adapté au protocole de chiffrement à 128 bits SSL, chiffrant autant la demande que la réponse des opérations, par une connexion sécurisée. Afin d'établir une connexion sécurisée, vérifiez que le préfixe de notre adresse Web indique « https » (et non simplement « http »). Tous les navigateurs que nous prenons en charge adhèrent à cette exigence. Si le vôtre ne le fait pas, veuillez télécharger le chiffrement approprié de votre fournisseur de services.
Section 2: SAFE BROWSING	**Section 2: NAVIGATION SÉCURISÉE**
When visiting a branch, you can feel confident that your money is safe and secure. We are keeping you just as safe when you bank online but once your information reaches your computer, you have a responsibility to protect it.	Lors d'une visite en succursale, vous êtes confiant que votre argent est en sécurité. Nous désirons vous faire ressentir la même confiance quand vous effectuer vos opérations bancaires en ligne mais, une fois que vos données atteignent votre ordinateur, vous avez la responsabilité de les protéger.
Personal Access Codes (PAC): Keep Them Safe	**Code d'Accès Personnel (CAP): Assurer leur sécurité**
Online credentials can be numerous as they are needed for email accounts, social networking sites, online newspapers and shopping websites.	Puisqu'elles sont requises pour s'identifier aux comptes courriels, aux sites de réseautage personnel, aux journaux en ligne et aux sites Web de magasinage en ligne, les données de

That's a lot of usernames and passwords – and it can be tempting to use the same combination for everything. But this makes it far too easy for hackers because once they have one password, they can access all your sites. Login credentials are the keys to your accounts so don't leave those keys around for anyone to find. For online banking, the key is your Personal Access Code (PAC). We recommend you: • Choose a PAC that is easy for you to remember but difficult for others to guess. Avoid using current phone numbers, dates of birth, or social insurance numbers. • Be smart and don't save a list of your credentials on your PC. If you have to write them down, keep these details locked away somewhere only you can access or consider using password-management software, which secures and encrypts usernames and passwords and allows you to use a single master password. • Do not share your PAC with anyone, especially online. Employees of our financial institution will never call, email, write or ask you to provide your online banking credentials. Ever. • Don't authorize browsers to memorize your credentials. Saving these on your computer allows anyone using your PC to gain access to your login-protected sites. • Consider changing your PAC every 90 days for optimum security.	connexion sont multiples. Il est tentant d'utiliser la même combinaison pour tout. Cependant ceci facilite la tâche aux pirates informatiques, puisqu'une fois décelée, tous vos sites peuvent être atteints. Vos données de connexion sont les clefs de vos comptes; il faut les protéger. Pour accès aux services bancaires en ligne, votre Code d'Accès Personnel (CAP) est votre clef. Nous suggérons : • De choisir un CAP simple à mémoriser mais difficile à deviner. Éviter de choisir des numéros de téléphones courants, des dates de naissance ou des numéros d'assurance sociale. • D'être vigilant et de ne pas sauvegarder vos données personnelles sur votre ordinateur personnel ou domestique. Si vous devez les noter, assurez-vous de placer ces détails en lieu sûr connu de vous seul(e) ou considérez d'utiliser un logiciel d'enregistrement des mots de passe, qui sécurise et chiffre les ID utilisateurs et mots de passe et vous permet d'utiliser un seul mot de passe illimité. • De ne pas partager votre **CAP** avec qui que ce soit, spécialement en ligne. Les employés de notre institution financière ne téléphoneront jamais, ni n'enverront de courriels ou de lettres vous exigeant de fournir vos données de connexion reliées aux services bancaires en ligne. Jamais! • Ne pas autoriser vos navigateurs à mémoriser vos données personnelles. Le fait de les enregistrer sur votre ordinateur permet à quiconque utilise votre ordinateur d'accéder à vos sites sécurisés. • De considérer modifier votre CAP tous les 90 jours pour assurer une sécurité optimale.
MONITORING YOUR ACCOUNTS	**CONTRÔLER VOS COMPTES**
Make sure you review your account statements (whether online or on paper) on a regular basis. Frequently reviewing your paper and/or electronic account statements ensures that you spot any incorrect or	Assurez-vous de réviser régulièrement vos relevés de compte (en ligne ou papier). En révisant fréquemment vos relevés papier et/ou électroniques, vous vous assurez de pouvoir saisir toutes

fraudulent transactions as soon as they occur. If your card has been skimmed (when the card's magnetic stripe and PIN are fraudulently copied by embedded devices at ATMs or point-of-sale devices) or unauthorized transactions have been made, you will want to catch this as soon as possible.	opérations incorrectes ou frauduleuses aussitôt qu'elles paraissent. Si vous êtes victime d'un subterfuge de carte (quand la bande magnétique et le NIP ont été frauduleusement copiés par des appareils intégrés aux guichets automatiques ou terminaux de point de vente) ou d'opérations effectuées sans votre autorisation, vous voulez le savoir le plus tôt possible.
Personal Details	**Données personnelles**
When you move, it is important to notify us of your change of address. If your mailing information isn't up-to-date, statements or letters that contain personal information will continue to be sent to your former address.	Quand vous déménagez, il est important de nous aviser de tout changement d'adresse. Si vos coordonnées postales ne sont pas à jour, vos relevés ou toute correspondance contenant des renseignements personnels continueront à être envoyés à votre ancienne adresse.
Logging In and Out	**Connexion et Déconnexion**
When you are finished with your banking session, always log out by clicking the "Log Out" button, as opposed to simply closing the browser window. To help protect your information, your online banking session will end automatically if there has been no activity for a period of time. If your session has timed out, no further transactions can be made until you log in again. This time-out feature helps protect your accounts from unauthorized access.	Quand vous avez terminé votre session bancaire, toujours mettre fin à la session en cliquant le bouton « Déconnexion » au lieu de simplement fermer la fenêtre du navigateur. Suite à une période d'inactivité et afin de protéger vos renseignements personnels, votre session de services bancaires en ligne prendra fin automatiquement. Si votre session est expirée, aucune opération ne sera exécutée jusqu'à ce qu'une nouvelle connexion soit effectuée. Cette fonction aide à protéger votre compte d'un accès non autorisé.
Clearing Cookies and Cache	**Effacer vos témoins et vider votre mémoire-cache**
When you spend time on the Internet, your browser stores information, such as the websites you visit, the images and files you view, and your personal information, including passwords and login details. This data is held on your computer's hard drive and is known as 'cache.' Even though you may have logged out and closed your browser, this information may remain accessible. You can protect your data by clearing your browsing history regularly. Learn how to clear the history in every browser you use.	En naviguant sur Internet, votre navigateur mémorise de l'information, tel que les sites Web visités, les images et les fichiers visualisés ainsi que vos données personnelles, incluant vos mots de passe et vos informations de connexion. Ces données sont conservées sur le disque dur de votre ordinateur et est connu sous le nom de mémoire-cache. Malgré que vous ayez mis fin à votre session et fermé votre navigateur, cette information est toujours accessible. Vous pouvez protéger vos données en effaçant régulièrement l'historique de navigation. Voici quelques conseils pour démontrer comment effacer l'historique de chaque navigateur utilisé.
Private Browsing	**Navigation privée**
Some web browsers have a feature that allows you to browse the Internet without the browser storing information, such as the sites you visit, the images you see and videos you watch. This feature is sometimes used by people who share the same computer.	Certains navigateurs ont une fonction qui vous permet de naviguer sur Internet sans laisser de traces des sites visités, des images visualisées et des vidéos regardés. Cette fonction est souvent utilisée par des personnes qui partagent un ordinateur.

Private browsing is a temporary option and must be selected in order for it to be activated. Private browsing, however, does not give you immunity to spyware or make you anonymous. It is still possible for your Internet service provider, employer or the websites you visit to track your online activity.	Ce mode est temporaire et doit être sélectionné pour être activé. Cette fonctionnalité ne vous offre toutefois pas une immunité contre les logiciels espions et ne vous rendent pas anonymes. Il est encore possible, malgré tout, que votre fournisseur de services Internet, votre employeur ou les sites Web visités continuent de repérer votre activité en ligne.
Section 3: INTERNET SCAMS	**Section 3: ESCROQUERIES DE L'INTERNET**
While pickpockets can only target a few people each day, Internet fraudsters cast their nets much wider, using the anonymity and reach of mass emails and fake websites. You can protect yourself from these situations by knowing how to identify and avoid these scams.	Bien que les voleurs ciblent quelques personnes par jour, les fraudeurs de l'Internet peuvent atteindre des multiples victimes sous le couvert de l'anonymat en déployant des courriels de masse et de faux sites Web. Vous pouvez vous protéger en sachant identifier et éviter ces escroqueries.
Phishing	**Hameçonnage**
A common way for Internet scammers to obtain your personal information is through a method called phishing. Usernames, passwords, banking information and credit card details are phished through email or instant messaging. Phishing works by sending communications, which appear to be from your financial institution, but they are not. You are asked, supposedly by your financial institution, to log in to your online banking to verify account information. Often some type of security concern is cited as the issue. The fake email instructs you to click on a link that takes you to a non-legitimate version of your online banking site – one that is largely indistinguishable from the legitimate site – and you'll be asked to enter your credentials. Phishing emails may include: • Warnings about account closures • Requests to update your information • Offers to register for a new service • Offers for pre-approved credit cards • Free virus-protection programs Once you click on the link, which directs you to a phishing website, you'll be prompted to enter personal or banking information. Phishing scams seek personal details, such as your address, social security number or mother's maiden name. The details obtained will then be used for identity theft. Never provide personal details or any account details in an email. Electronic messaging is not a secure form of	Un des moyens utilisé par les fraudeurs de l'Internet pour obtenir vos données personnelles s'appelle l'hameçonnage. Les noms d'utilisateurs, mots de passe, données bancaires et détails des cartes de crédit sont « hameçonnés » par courriel ou par messagerie instantanée. L'hameçonnage fonctionne en envoyant des communications qui semblent être de la part de votre institution financière, mais ne le sont pas. On vous demande, supposément de la part de votre institution financière, de vous connecter à vos services bancaires en ligne afin de vérifier des détails de votre compte. Souvent, on mentionne un trouble de sécurité comme problème. Le faux courriel vous invite à cliquer sur un lien qui vous amènera vers une version illégitime de votre site en ligne bancaire – visuellement impossible à distinguer de l'original - et on vous demandera d'inscrire vos renseignements personnels. L'hameçonnage peut inclure : • Des avertissements concernant la fermeture d'un compte • Des demandes de mise à jour de vos données • Des offres de nouveaux services • Des offres pour des cartes de crédit pré-approuvées • Des logiciels d'antivirus gratuits Une fois lié au site d'hameçonnage, on vous invitera à entrer des renseignements personnels et des données bancaires. Les escrocs d'hameçonnage recherchent les renseignements personnels, tels votre adresse, numéro d'assurance sociale ou le nom de jeune fille de votre mère. Les détails obtenus seront utilisés à des fins de vol d'identité. Ne fournissez jamais de renseignements personnels ou aucun détail de vos comptes dans un courriel. La

communication. If you receive a message that you are unsure about, please contact us.	messagerie électronique n'est pas un moyen fiable de communication. Si vous recevez un message douteux, veuillez entrer immédiatement en communication avec nous.
Pharming	**Détournement de renseignements – «Pharming»**
Another way for hackers to get their hands on your personals details is by pharming them. Pharming occurs when hackers use a malicious code on your PC, which compromises your computer's host file and redirects you to fake websites. The malware hides the fraudulent URL, cloaking it in the legitimate one that appears in your browser. With pharming, the dishonest redirection of URLs happens even when you type correct URLs directly into your browser, making you think that you're on the correct website when you are not. Once there, you are asked to enter your online banking credentials or account information, which hackers take and use for criminal activity.	Une autre méthode pour les fraudeurs de mettre la main sur vos renseignements personnels est en les détournant – «pharming». Ceci se produit quand un pirate utilise un code malveillant sur votre ordinateur, ce qui compromet le programme hôte et vous redirige vers de faux sites Web. Le logiciel malveillant cache l'URL frauduleux, le masque dans l'adresse URL légitime qui apparaît sur votre navigateur. De cette façon, la redirection malhonnête d'adresses URL se produisant quand vous tapez l'adresse URL correcte directement sur votre navigateur,vous fait croire que vous êtes sur le bon site Web quand vous ne l'êtes pas. Une fois redirigé, vous êtes invité à entrer vos données bancaires personnelles ou les détails de vos comptes, qui sont plus tard utilisés par les pirates pour activités criminelles.
How to Avoid Phishing and Pharming Scams	**Comment éviter l'hameçonnage et le détournement**
We will never send you emails or communications asking you to verify or provide your online banking details. The best way to protect yourself is to never use a link provided in an email to access your online banking (because we don't send those; scammers do). Do not open emails or email attachments from unknown sources. Scan email through your anti-virus software. Always type your financial institution's website address directly into your browser and remember to look for confirmation that you are browsing securely. The letter "s" in 'https' indicates you are navigating in a secure site, in comparison to the open and unprotected 'http' URLs. Look for the 'https' when online shopping, too. Don't believe emails warning that your account has been compromised or that you'll miss out on a great deal if you fail to act immediately. If you are concerned, call or visit one of our customer service representatives.	Nous ne vous demanderons jamais de vérifier ou de fournir, soit par courriel ou par toute autre communication, quelconque détail de vos activités bancaires. La meilleure manière de vous protéger est de ne jamais utiliser un lien fourni dans un courriel pour accéder à vos services bancaires (parce que nous ne le feront jamais; les pirates le font.) N'ouvrez jamais des courriels ou des fichiers-joints de sources inconnues. Balayez les courriels en utilisant votre logiciel antivirus. (Hyphen fichier-joints) Il est important de toujours inscrire l'adresse Web de votre institution financière manuellement directement sur votre navigateur et de ne pas oublier de rechercher la confirmation que vous naviguez en sécurité. La lettre « s » dans « https » indique que vous êtes sur un site sécurisé, par comparaison aux adresses URL « http » non sécurisées. Lorsque vous magasinez en ligne, recherchez aussi « https ». Ne croyez pas les courriels qui indiquent que vos comptes sont compromis et que vous allez rater une aubaine si vous n'agissez pas immédiatement. Si vous êtes inquiet, n'hésitez pas à communiquer avec un de nos représentants des services à la clientèle.
Anti-Virus Software	**Logiciel antivirus**
Install anti-virus software on your computer to protect your information, money and privacy. Such software detects viruses and cleans your computer so that harmful viruses	Il vaut mieux installer un logiciel antivirus sur votre ordinateur afin de protéger vos données, votre argent et votre vie privée. Ces logiciels décèlent les virus et assurent que les virus

do not spread. Set up your anti-virus to run frequent scans and update the software as soon as it is required. Ensure you have real-time scanning of every email and every file you download.	nuisibles ne se propagent pas. Votre logiciel antivirus doit pouvoir balayer fréquemment et de façon continue et vous devez le tenir à jour. Assurez-vous que chaque courriel et chaque fichier que vous téléchargez soient balayés en temps réel.
Malware	**Programme malveillant**
Malicious software (malware), spyware, worms and Trojans are the same class of destructive viruses; just with different names. Nobody wants a computer virus. They can steal your personal information, take over your PC and use your computer to attack other people's computers. Your PC can become infected through email attachments, downloading infected content or visiting harmful websites.	Les logiciels malveillants, les logiciels espions, les vers et cheval de Troie, sont de la même classe de virus destructeurs, seuls leurs noms diffèrent. Personne ne veut contracter un virus. Ils peuvent voler votre identité, s'emparer de votre ordinateur et l'utiliser pour attaquer d'autres ordinateurs. Votre ordinateur peut être infecté par des fichiers-joints, en téléchargeant des fichiers contaminés ou en visitant des sites Web nuisibles. Hyphen fichier-joints
Spyware	**Logiciels espions**
Spyware is exactly what it sounds like – tracking software that is downloaded to your computer (without your knowledge) when you visit certain Internet sites. Secretly, it gathers information about you and your browsing habits. This information can be trivial or it can include passwords and personal data that you wouldn't want criminals to get their hands on. It can also interfere with user controls and disable legitimate anti-virus programs. The best way to protect your computer against spyware is smart browsing. Stay away from sites that look unsafe and avoid streaming or downloading content from untrustworthy sources. Many anti-virus products offer targeted spyware solutions that inspect your operating system, installed programs, downloads and files.	Un logiciel espion porte bien son nom – un logiciel de suivi qui est téléchargé sur votre ordinateur (à votre insu) quand vous visitez certains sites Internet. Secrètement, ils recueillent des renseignements vous concernant ainsi que vos habitudes de navigation. Ces renseignements peuvent être sans importance ou peuvent contenir des mots de passe et des données personnelles que vous ne voudriez pas retrouver entre les mains de criminels. Un logiciel espion peut aussi gêner les contrôles utilisateurs et désactiver des logiciels antivirus légitimes. La meilleure façon de protéger votre ordinateur contre les logiciels espions est de naviguer judicieusement. Méfiez-vous des sites qui semblent douteux et évitez de transmettre en continu ou de télécharger du contenu provenant de sources peu fiables. Plusieurs produits antivirus offrent des solutions ciblant les logiciels espions qui inspectent votre système d'exploitation, vos logiciels installés, vos téléchargements et vos fichiers.
Scareware One of the most common viruses to watch out for is known as scareware. These scams pop-up on your screen and display alarmist warnings, telling you a virus has invaded your computer. Scareware prompts you to download (and often pay for) fake anti-virus software to remove the non-existent viruses. Scareware is a scam that tries to trick you into paying money in exchange for nothing. You can protect against scareware by keeping your anti-virus software up-to-date and by being judicious about what you choose to download to your computer. You should also familiarize yourself with the interface of your	**« Scareware »** Un des plus communs virus à surveiller est un « scareware ». Ces messages d'avertissement s'affichent spécifiquement sur votre écran pour vous alarmer, vous informant qu'un virus a envahi votre ordinateur. Il vous incite à télécharger (et souvent à payer) un faux logiciel antivirus qui doit supprimer des virus non existants. C'est une escroquerie qui tente de vous soutirer de l'argent sans rien vous donner en échange. Vous pouvez vous protéger contre les virus «scareware» en tenant votre logiciel antivirus à jour et en étant judicieux dans vos choix de téléchargements. Vous devriez aussi vous familiariser avec l'interface de votre logiciel antivirus légitime

legitimate anti-virus program, so you won't be fooled if one of these pop-ups appears.	pour le reconnaître si un de ces messages apparaît sur votre écran.
Section 4: COMPUTERS & SMARTPHONES	**Section 4: ORDINATEURS ET TÉLÉPHONES INTELLIGENTS**
We have created secure channel to communicate with our customers but you need to do your part by making sure your computer is virus-free and the operating system is kept updated.	Nous avons créé une voie de communication sécurisée afin de communiquer avec nos clients, mais vous devez faire votre part en vous assurant que votre ordinateur soit tenu à jour et sans virus.
Operating Systems	**Systèmes d'exploitation**
Your computer's operating system needs to be up-to-date in order to defend itself from viruses and malicious software (malware). If one part of your operating system develops a virus, it leaves holes in your PC's security defences and compromises the safety of the information contained in your computer. Keeping your software up-to-date is one of the most important ways of staying safe online because it is much harder for viruses to infect an updated operating system and software. Hackers are targeting operating systems with new viruses all the time and software companies combat these efforts with security patches. You should always download the latest security patch as soon as it becomes available. Your operating system lets you know when updates are available by notifying you there are new security features to download. You can also upgrade your operating system to the latest version available from the manufacturer; however, you should ensure your computer has sufficient hardware capacity to support an upgrade. Remember to back up your data. To fully eliminate a virus that has infected your machine, the re-installation of your operating system may be required. Protect yourself against the permanent loss of important data by frequently backing up your files on an external hard drive so you'll have the data should you ever have a problem with your operating system.	Le système d'exploitation de votre ordinateur doit être mis à jour afin de pouvoir se protéger des virus et des programmes malveillants. Si une partie de votre système d'exploitation est infectée par un virus, le système de défense et la sécurité de votre information contenus dans votre ordinateur seront compromis. Comme il est plus difficile d'infecter un système d'exploitation et ses logiciels qui sont à date, la mise à jour de vos logiciels est essentielle pour assurer votre sécurité en ligne. Les pirates ciblent constammant les sytèmes d'exploitation avec de nouveaux virus et les fabricants de logiciels combattent ces efforts en développant des rustines. Vous devriez télécharger les plus récentes rustines dès qu'elles sont disponibles. Votre système d'exploitation vous avise des nouvelles mises à jour en vous invitant à télécharger les nouveaux éléments de sécurité. Vous pouvez aussi mettre votre système d'exploitation à niveau en installant, directement du manufacturier, la plus récente version. Vérifiez toutefois que votre ordinateur ait la capacité matérielle suffisante pour assurer la mise à niveau. Veuillez vous souvenir de sauvegarder vos données. Afin de totalement éliminer un virus qui aurait infecté votre ordinateur, il faudra possiblement réinstaller le système d'exploitation. Protégez-vous d'une perte permanente de vos données importantes en sauvegardant vos fichiers sur un disque dur externe qui permettra de récupérer les données s'il se produisait un problème.
Browsers	**Navigateurs**
Web browsers are the gateways to the Internet. Similar to having an up-to-date operating system, upgraded browsers provide more features, stability and security. The latest versions of web browsers have security features	Les navigateurs de Web sont le portail de l'Internet. Autant la mise à jour du système d'exploitation est importante, autant avoir un navigateur mis à niveau assurera des fonctions, une stabilité et une sécurité accrues. Les versions récentes des navigateurs ont développé des mesures de sécurité qui identifient et bloquent des sites Web

that can identify and block harmful and fake websites and pop-ups, and warn you if a site is flagged as unsafe. Some browsers also have a 'Private Browsing' feature, which conceals your browsing history from others. Whether you use Internet Explorer, Firefox, Safari, Chrome or something else, stay safe online by using the latest version available.	et des fenêtres surgissantes « pop-ups » faux et nuisibles et elles vous préviennent si un site semble douteux. Certains navigateurs offrent une « navigation privée » qui cache votre historique de navigation des autres utilisateurs. Que vous utilisiez Internet Explorer, Firefox, Safari, Chrome ou un autre navigateur, exercez des mesures de sécurité en utilisant les toutes dernières versions disponibles.
Firewalls	**Pare-feu**
A firewall protects your computer and home network from harmful websites and hackers. It sits between your computer and the Internet, scanning information that is being transmitted. It allows for safe browsing, while blocking unauthorized intrusions. Firewalls also stop your computer from being used by hackers to send malicious software to other computers. Most computers now come with a firewall as part of the standard operating system. However, you can get the maximum protection for your computer by installing additional firewalls and ensuring they are kept up-to-date.	Un pare-feu protège votre ordinateur et votre réseau domestique des sites Web nuisibles et des pirates. Il se place entre votre ordinateur et l'Internet, balayant l'information qui est transmise. Il favorise la sécurité de la navigation tout en bloquant les intrusions non autorisées. Les pare-feu empêchent **aussi** que votre ordinateur ne soit l'instrument de transmission de logiciels malveillants vers d'autres ordinateurs. Habituellement, le pare-feu fait partie intégrante d'un sytème d'exploitation standard. Cependant, pour une protection maximale, vous pouvez installer des pare-feu additionnels tout en assurant leur mise à jour.
PROTECTING YOUR SMARTPHONE	**PROTÉGER VOTRE TÉLÉPHONE INTELLIGENT**
Browsing the web has never been easier – it's all at your fingertips. Smartphones let you surf, shop or bank wherever you are. Make sure your information stays secure while you're on the move by following these smartphone-safe browsing tips: • Activate your phone's password feature, which locks the screen and prevents anyone but you from accessing your phone. Set up the password feature on your phone with a code that only you know. • Don't connect to unknown networks through Wi-Fi hotspots to make financial transactions. • Beware of smishing – that's phishing on phones through text messages. Never download media or images, or click on text-message links that come from unrecognizable people or phone numbers. Never provide personal details or any account details using any form of electronic	Naviguer sur le Web n'a jamais été si facile – tout est au bout des doigts! Les téléphones intelligents vous permettent de surfer, de magasiner ou d'effectuer des opérations bancaires où que vous soyez. Voici quelques conseils de navigation lorsque vous utilisez votre téléphone intelligent afin d'assurer la sécurité de vos données : • Activer la fonction mot de passe; celle-ci verrouille l'écran et empêche toute autre personne d'accéder à votre téléphone. Établir la fonction mot de passe en utilisant un code que vous seul(e) connaissez. • Ne pas se connecter à des réseaux inconnus par des points d'accès sans-fil pour effectuer vos opérations bancaires. • Se méfier du « SMiShing » – harmeçonnage par messagerie texte (SMS). Ne jamais télécharger de média ou des images, ni cliquer sur des liens de messages texte provenant de personnes ou de numéros de téléphone inconnus. Ne jamais fournir de renseignements personnels ou de détails de compte

messaging because this is not a secure form of communication. If you are unsure, please contact us. • Download apps exclusively from the official source for your smartphone's platform, such as the Android, Apple or BlackBerry stores. • Install anti-virus software for your smartphone when available and update it frequently. • Install location finding applications, which work with your phone's built-in GPS. These applications allow you to locate and/or remotely erase (or "wipe") data in your phone if it is lost or stolen. • Update your smartphone's operating system as soon as newer versions are available.	par toute méthode électronique. Cette forme de communication n'est pas sécurisée. Dans l'incertitude, veuillez communiquer avec nous. • Toujours télécharger les apps exclusivement à partir de la source officielle de la plate-forme de votre téléphone intelligent, tel que des magasins Android, Apple ou BlackBerry. • Installer un logiciel antivirus pour votre téléphone intelligent s'il est disponible et effectuer une mise à jour régulière. • Installer un programme de repérage de position, agissant en relation avec le système de GPS intégré de votre téléphone. Ces programmes vous permettent de localiser et/ou d'effacer à distance (ou « d'épurer ») les données enregistrées dans votre téléphone, si ce dernier est perdu ou volé. • Effectuer une mise à jour du système d'exploitation de votre téléphone intelligent aussitôt qu'une nouvelle version est disponible.
Section 5: WI-FI & E-SHOPPING	**Section 5: WI-FI & MAGASINAGE EN LIGNE**
These days, everyone is on the go and it's not uncommon to access Wi-Fi at coffee shops, hotels, restaurants or airports. Using wireless networks to access information is convenient, but not risk-free. Be smart when you surf. Protect yourself from threats by: • Using only a trusted computer to access your online banking. Don't use shared library or café computers. • Managing your online banking only from secure networks. We recommend that you don't use unsecured public networks for anything sensitive. • Connecting only to password-protected networks. If there are several networks available, ask employees of the organization which network they operate. • Never leaving your computer unattended, especially if you are logged into your online banking.	Ces jours-ci, tout le monde est à la course et il n'est pas rare d'accéder aux réseaux Wi-Fi dans les cafés, les hôtels, les restaurants ou dans les aéroports. C'est très pratique d'utiliser ces réseaux sans fil pour atteindre de l'information, mais ce n'est pas sans risque. Il faut être vigilant. Voici quelques conseils pour vous protéger contre les menaces : • Utiliser seulement un ordinateur fiable pour accéder à vos services bancaires en ligne. Ne pas utiliser d'ordinateur à accès partagé dans les bibliothèques ou dans les cafés. • Gérer des opérations bancaires strictement à partir de réseaux sécurisés. Nous suggérons de ne jamais utiliser de réseaux publics non sécurisés pour tout ce qui est confidentiel. • Se connecter seulement à des réseaux protégés par mot de passe. Si plusieurs réseaux sont disponibles, vérifiez auprès des employés de l'organisation de quel réseau ils se servent. • Ne jamais laisser votre ordinateur sans surveillance, spécialement si vous êtes connecté à vos services bancaires.

• Using different PACs and security questions as login credentials. If someone obtains your credentials for one site, such as a social networking site, you don't want them to be able to access your other ones. • Ensuring you log out before you close your browsers.	• Utiliser divers CAP et diverses questions de sécurité comme données de connexion. Si quelqu'un obtient vos données personnelles d'un site, soit d'un site de réseautage social, par exemple, vous ne voudriez pas qu'il ait accès aux autres données. • Assurer votre déconnexion avant de fermer vos navigateurs.
SHOPPING ONLINE	**MAGASINAGE EN LIGNE**
Online shopping is the epitome of convenience. There are no lines and no crowds, but it can also be a haven for fraudsters. Consider the following tips when using your credit cards online to ensure your information stays secure: • Make sure that you are shopping at a trusted retailer when you enter your credit card details online. • Provide retailers with only the necessary details to complete the transaction. These include your credit card number, expiry date, the security code on the back of the credit card and the card's billing address. Never provide your social insurance number, account details or your mother's maiden name. For shopping sites that require you to register with a username and password, don't use your online banking PAC. • Use your credit cards only on e-commerce websites that use secure browsing technology on the screens where you enter your card information. Ensure the web address begins with 'https' (as opposed to 'http') and has a closed padlock icon on the screen. • Ensure that smaller retailers requesting credit card details have reputable contact details, a physical address and you feel comfortable with providing them your card information. • Never give your account or credit card details to	Magasiner en ligne est le summum du pratique. Personne en ligne, pas de foule, mais un paradis pour les fraudeurs. Afin d'assurer la sécurité de vos données personnelles, considérez les conseils suivants quand vous utilisez vos cartes de crédits en ligne : • S'assurer de magasiner au site d'un détaillant digne de confiance. • Fournir seulement les renseignements nécessaires pour compléter la transaction : le numéro de la carte de crédit, la date d'expiration, le code de sécurité à l'arrière de la carte et l'adresse de facturation. Ne jamais fournir votre numéro d'assurance sociale, des détails de votre compte ou le nom de jeune fille de votre mère. Si un site requiert un enregistrement avec un ID utilisateur et un mot de passe, nous vous suggérons de ne pas utiliser votre CAP des services bancaires en ligne. • N'utiliser vos cartes de crédit que sur des sites Web de vente en ligne qui utilisent une technologie de navigation sécurisée visible à l'écran où vous entrez l'information de votre carte. S'assurer que l'adresse Web commence par «https » (et non simplement «http ») et que la page affiche un symbole de cadenas fermé. • S'assurer de la validité des coordonnées et de l'adresse physique des plus petits détaillants qui demandent l'information concernant vos cartes de crédit. Ils doivent vous inspirer une confiance suffisante pour que vous partagiez les renseignements de vos cartes de crédit. • Sur eBay ou Craigslist, ne jamais partager les détails de

anyone on eBay or Craigslist.	vos comptes ou cartes de crédit avec quiconque.
OUR PRIVACY AND SECURITY POLICY	**NOTRE CODE DE CONFIDENTIALITÉ ET DE SÉCURITÉ**
For more information on the specific policies and practices that we use to safeguard your personal and financial information, please click here to view our Privacy Statement.	Pour obtenir de plus amples renseignements au sujet des politiques et pratiques spécifiques que nous utilisons afin de protéger vos renseignements personnels et financiers, veuillez cliquer ici pour visualiser notre Code de la protection de la vie privée.