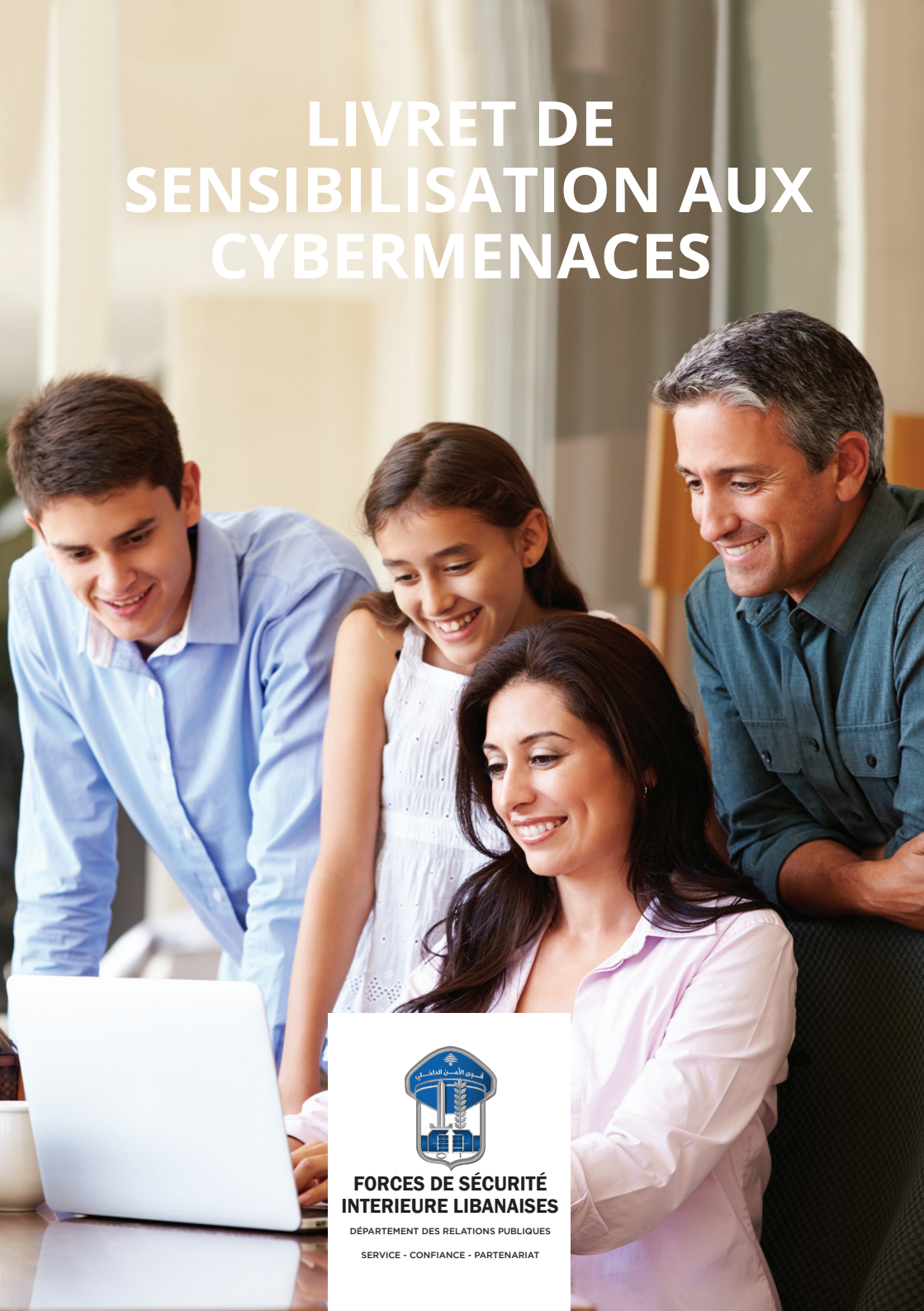
LIVRET DE SENSIBILISATION AUX CYBERMENACES



FORCES DE SÉCURITÉ INTERIEURE LIBANAISES

DÉPARTEMENT DES RELATIONS PUBLIQUES

SERVICE - CONFIANCE - PARTENARIAT

Table des matières

Page

1- Introduction

Le développement technologique, notamment dans le domaine de technologie de l'information et des communications, a transformé le monde en un village planétaire grâce au réseau Internet qui a permis le développement de nombreux logiciels, dont les logiciels de chat, les applications médias sociaux ainsi que d'autres applications réduisant la distance entre les individus et leur permettant de communiquer d'une façon directe et rapide grâce à l'échange des messages, des images et des données, facilitant par ailleurs la fourniture de divers services électroniques qui contribuent à l'exécution des transactions électroniques sous toutes leurs formes.

En revanche, des nouveaux types de crimes fondés sur l'exploitation des technologies de l'information ont apparu dans le but de commettre de nouvelles formes de criminalité ou des crimes déjà connus, mais par des méthodes et des techniques modernes. Les cyber-risques constituent un problème majeur de fait qu'ils entrainent une augmentation de la criminalité liée au piratage et vol des données personnelles des individus et des institutions, ainsi que la menace de l'infrastructure d'information des systèmes et réseaux vitaux au niveau de l'État. D'où, il est à présent impératif d'accroitre la sensibilisation aux risques et menaces liés à l'Internet, y inclus le vol d'identité, des mots de passe, des comptes, le piratage de données, l'extorsion électronique ... en plus de l'adoption des meilleures pratiques en matière de la prévention, la protection et le renforcement des procédures et des mesures de sécurité à prendre en cas d'exposition à des cas pareils.

Face à cette réalité, il incombe aux Forces de Sécurité Intérieure, en outre de ses fonctions et responsabilités nationales, de protéger les citoyens contre tous les risques qui les menacent, notamment les crimes et les cyber-attaques, sachant qu'elle est complètement prête préparée à remplir ce devoir et à assumer cette responsabilité en faisant de son mieux pour assurer la protection requise sur Internet, renforcer la cyber sécurité au Liban, sensibiliser les citoyens, et mener les enquêtes nécessaires pour repérer, interpeller et référer les contrevenants aux autorités judiciaires compétentes tout en veillant à garder la confidentialité de ces enquêtes et respecter la vie privée et les normes des droits de l'homme.

2- Objectif

Ce guide vise à accroitre la sensibilisation des citoyens sur les principaux risques, menaces et cyber crimes auxquels ils peuvent être confrontés, suite à l'utilisation des technologies d'information et de l'accès internet, ainsi que sur les meilleurs moyens possibles pour s'y protéger contre et sauvegarder leur vie privée.

En outre, ce guide présente les mesures préventives et les meilleures pratiques à suivre pour protéger les informations personnelles et les données contre le vol, empêcher l'exposition des dispositifs électroniques au piratage, éviter d'être victime de l'extorsion électronique et protéger les enfants et les autres membres de la famille lors de l'utilisation de l'internet.

3-Les différentes formes de Cyber-criminalité

Avec l'augmentation du recours aux moyens électroniques, notamment les Smartphones et les appareils portables, pour communiquer sur Internet et bénéficier des diverses applications et services électroniques fournis par les entreprises et institutions gouvernementales et privées, ces appareils sont devenus plus vulnérables aux cyber-attaques pour des différents motifs, dont l'extorsion, le vol des informations, la destruction, l'obtention d'un gain financier, ou pour nuire à la crédibilité ou à la réputation. Par conséquent, tous les citoyens sont invités à protéger ces dispositifs contre le piratage et le cyber-attaque. On trouvera ci-après les principales formes les plus répandues de cybercriminalité qui sont apparues récemment :

3.1– Extorsion électronique

C'est l'acte d'intimider et de menacer la victime de publier des photos ou des matériels vidéos, ou de diffuser des informations confidentielles qui la concernent ou concernent l'un des membres de sa famille, afin de l'obliger à payer des sommes d'argent, ou l'exploiter pour des fins

sexuelles, immorales ou illégales au profit des maîtres-chanteurs. Le chantage électronique affecte la condition psychologique et sociale des victimes, ce qui fait qu'un grand nombre de ces victimes hésitent à porter plainte par peur de voir leurs vidéos ou autres matériels diffusés, ou par crainte de la perception de la société ; par conséquent, elles se trouvent forcées à accéder aux requêtes du maître-chanteur et lui envoient l'argent, ou se font du mal, et dans certains cas, tentent de se suicider.

Certains exemples des cas d'extorsion électronique sont exposés ci-dessous:

1- Garder des vidéos, enregistrements, photos personnelles ou pornographiques prises lors des conversations électroniques par caméra et menacer de les publier à moins de payer des sommes d'argent, ou rendre des services sexuels ou autres ...

2- Vol des données et des photos personnelles ou familiales durant les travaux d'entretien et de réparation du téléphone portable afin d'extorquer son propriétaire .

3- Convaincre la victime de connaitre des sites web qu'elle navigue et la menacer de les publier afin de l'extorquer.

3.2– Hameçonnage (Phishing)

C'est une technique utilisée par des fraudeurs afin de voler les renseignements personnels des utilisateurs tels les détails de connexion, le mot de passe, le numéro de téléphone, les cartes de crédit et autres. A cet effet, les cybercriminels créent un faux site Web qui ressemble au site d'origine (un faux site Facebook, tel faceb00k.com au lieu de facebook.com), et envoient par la suite le faux lien du site Web à la victime par.

Courriel ou via les médias sociaux, supposant qu'il est envoyé par une source fiable (comme l'entreprise, la banque ou même le site Web avec lequel la victime a affaire), tout en l'incitant de diverses manières possibles à cliquer sur le lien susmentionné. Dans ce cas, la victime recevra les directives nécessaires afin de fournir des informations personnelles importantes qui seront utilisées ultérieurement par le hacker pour frauder la victime ou accéder d'une façon illégale à ses comptes, ou installer des logiciels malveillants sur les dispositifs de la victime visant à faciliter le vol des informations ou les opérations de sabotage.

3.3– Usurpation d'identité

Il s'agit d'un acte de fraude réalisé en utilisant des informations d'identification personnelle appartenant à une autre personne, comme le nom, le numéro de passeport, la carte d'identité, le permis de conduire, la carte de crédit, les détails ou une copie du compte électronique, sans son autorisation, et ce afin de commettre des actes frauduleux, voler de l'argent et les Cartes de crédit, ou tout simplement nuire ou porter atteinte à la réputation.

Les exemples les plus flagrants de l'usurpation d'identité comprennent :

a. Vol des comptes privés sur les réseaux sociaux, tels LinkedIn, Snapchat, Instagram, Twitter, Facebook afin de prendre délibérément l'identité de la victime et nuire à sa réputation en la diffamant et diffusant des informations compromettantes la concernant, ou en harcelant ses amis en utilisant son compte pour les intimider.

b. Vol des comptes sur les services de courrier électronique et de messagerie instantanée.

c. Vol de comptes sur les sites de jeux électroniques.

d. Ouvrir des comptes bancaires, obtenir des prêts et commettre des actes illégaux en se prenant délibérément l'identité de la victime.

e. Utilisation illégale des comptes de cartes de crédit de la victime pour effectuer des achats ou retirer de l'argent.

3.4– Cyber-harcèlement

Il s'agit d'un acte commis par une personne ou un groupe de personnes pour harcèler, maltraiter ou se moquer d'une autre personne à plusieurs reprises par le biais des courriers électroniques, des sites Web, la diffusion des vidéos et des blogs, ou par tout autre moyen de communication dans le but de porter préjudice à cette personne.

La Cyber-harcèlement comprend :

a. Diffusion des messages calomnieux sur les réseaux sociaux.

b. Propagation des rumeurs sur Internet.

c. Incitation via Internet à exclure une personne d'un certain groupe ou à l'exclure socialement.

3.5– Piratage Informatique

C'est une pratique visant à pirater ou à tenter de pirater les données électroniques des individus, et des institutions gouvernementales ou privées pour les voler ou saboter.

Ces données peuvent contenir des informations confidentielles relatives aux citoyens, agents, fonctionnaires ou autres informations assez importantes comme la propriété intellectuelle.

3.6– Rançongiciel (Ransomware)

Ce type de logiciel contribue au cryptage des données importantes ou de l'ensemble du dispositif (ordinateur ou Smartphone), de sorte que l'utilisateur ne peut plus accéder à ses données. Le hacker demande par la suite, à la victime une « rançon » financière via des crypto monnaies comme le Bitcoin, du fait qu'il est difficile de les traquer, en échange du promet de décryptage des données et le rétablissement de la normalité (Payer la rançon est déconseillé car le décryptage n'est jamais garanti).

3.7– Fraude du courriel d'entreprise compromis:

C'est un type de fraude qui cible les entreprises effectuant des transferts de fonds ou ayant des fournisseurs à l'étranger. Ce type de délit dépend principalement de l'accès aux comptes du courrier électronique des directeurs exécutifs et des responsables des transferts financiers dans l'entreprise en créant des courriers électroniques similaires ou en piratant les courriels originaux par le biais de la technique d'hameçonnage ou l'ingénierie sociale, et puis frauder les employés de l'entreprise en prenant l'identité du Directeur Exécutif ou tout exécutif délégué pour donner l'autorisation d'effectuer les transferts financiers à l'étranger, afin de procéder à des transferts frauduleux entraînant des préjudices financiers considérables.

En d'autres termes, le cybercriminel qui est au courant des procédures suivies, utilise le courriel du directeur compromis pour établir une demande de transfert de fonds. L'employé est tenu de ne pas suivre le processus traditionnel, généralement approuvé, pour certifier la demande de transfert. En fait, l'employé transfère normalement les fonds sur un compte géré par le cybercriminel dans une banque, souvent située en dehors de la juridiction du pays où se trouve l'entreprise ; Dans ce cas, le directeur réel n'est pas normalement au courant du contenu de la demande de transfert des fonds et des réponses envoyées par courriels et reçues par les employés, et ce lors du transfert des fonds effectué par un employé, sur un compte géré par le cybercriminel dans une banque, souvent située en dehors de la juridiction du pays où se trouve l'entreprise.

4- Prévention contre les cyber-risques et la cybercriminalité

Malgré le développement des technologies de protection électronique et de cyber sécurité, allant de pair avec l'augmentation des cyber-attaques, il s'avère nécessaire de prendre certaines mesures essentielles et suivre les meilleures pratiques pour éviter d'être victime de la cybercriminalité et prévenir les risques qui en découlent.

Modifiez le nom d'utilisateur et le mot de passe qui sont spécifiés par défaut par le fabricant

Révisez les permissions données aux applications et supprimer les applications non utilisées

Conservez des copies de sauvegarde de vos données et mettez à jour les systèmes d'exploitation et les logiciels régulièrement

Appliquez des paramètres de sécurité supplémentaires sur les appareils comme les mots de passe solides et l'identification biométrique, etc.

Veillez à télécharger et mettre régulièrement à jour les logiciels antivirus

Veillez à choisir des mots de passe différents pour votre courrier électronique et vos comptes sur les réseaux sociaux

Veillez à appliquer des paramètres de sécurité et de confidentialité supplémentaires sur les réseaux sociaux

4.1– Protection des comptes et applications des comptes inhérents à l'internet

La protection des courriels, des mots de passe, des comptes de réseaux sociaux, des applications du service de messagerie SMS et des équipements électroniques constitue un facteur essentiel de la protection de la société contre les risques inhérents à Internet. Pour atteindre cet objectif, il faut se conformer aux procédures et instructions citées ci-dessous et veiller à leur stricte application.

4.1.1– Choisir un bon mot de passe:

- Utilisez un mot de passe assez solide et compliqué comprenant un mélange de lettres majuscules (A - Z) et minuscules (a - z), ainsi que des nombres, des symboles et des signes spéciaux (#, $, %, @, &, !), mais pas à moins de 12 caractères.

- Utilisez des phrases complètes pour les mots de passe si possible (comme Th1515@5tr0ngP@55) et remplacez certaines lettres par des caractères spéciaux.

- Évitez d'utiliser des informations personnelles dans les mots de passe comme le nom, le numéro de téléphone, l'adresse du domicile, la date de naissance, etc. Les mots de passe ne doivent pas inclure de mots qu'on peut trouver dans le dictionnaire afin qu'ils ne soient pas aisément prévisibles.

- Évitez les lettres en série (abcd12345) et les séquences de clavier comme qwerty et asdzxc.

- Abstenez-vous d'utiliser le même mot de passe pour les différents comptes et applications.

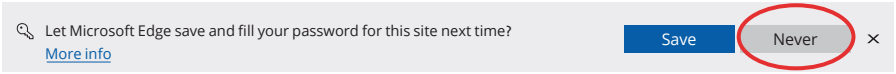
- Utilisez si possible, des applications fiables relatives au gestionnaire des mots de passe pour créer et gérer les mots de passe.

- Ne sauvegardez point les mots de passe avec des informations détaillées sur le compte dans des endroits non sécurisés tels les téléphones portables, les ordinateurs ou les documents écrits.

- Ne partagez pas vos mots de passe et ne les insérez pas devant qui que ce soit.

- Changez immédiatement votre mot de passe en cas de suspicion de piratage de l'un de tes comptes.

- Changez périodiquement le mot de passe de tes comptes et veillez à choisir un nouveau mot de passe différent des précédents.
- Soyez prudent en choisissant les questions de rappel de mot de passe, que certains sites utilisent pour t'aider à se souvenir du mot de passe en cas d'oubli, afin qu'il ne soit pas aisément prévisible (par exemple, le nom du père comme réponse à la question de rappel).
- Évitez d'enregistrer les mots de passe sur l'une des applications qui présentent l'avantage du « sauvegarde de mot de passe ».



4.1.2–Protection des comptes sur les réseaux sociaux (Instagram, Twitter, Facebook, LinkedIn, Snapchat…)

- Respectez les critères de sélection de mot de passe susmentionnés.
- Fournissez les informations minimums requises, essentielles pour l'ouverture d'un nouveau compte sur les réseaux sociaux.
- Révisez les paramètres de sécurité avancées sur les réseaux sociaux et veiller à activez-les afin d'augmenter le niveau de protection lié aux comptes, dont l'activation de la fonction d'authentification à double facteur relative à la validité de l'accès, la limitation de l'accès aux détails du compte, la limitation de l'accès, le renforcement des options de confidentialité et l'activation de l'alerte par des méthodes appropriées, en cas de tentatives douteuses d'accéder au compte.
- Soyez vigilant quant aux informations personnelles détaillées diffusées, vous concernant ou concernant votre famille, sachant qu'il sera difficile de contrôler les informations après leur diffusion.
- Évitez de participer à des activités virtuelles nuisibles ou illégales comme que le chantage, la diffamation, l'outrage ou l'insulte des convictions religieuses ou sectaires, ou lancer des menaces et porter atteinte aux autres.
- Communiquez uniquement avec des personnes dignes de confiance et méfiez-vous des étrangers et des harceleurs qui vous envoient des demandes d'amitié.
- Abstenez-vous de répondre aux conversations provenant des sources inconnues, d'autant plus que certains changent ou cachent, intentionnellement ou non, leur véritable identité (âge, nom, sexe et photo) sur les réseaux sociaux.

- Évitez d'afficher ou de réafficher (... partager, retweeter) des informations incorrectes et peu fiables.

- Abstenez-vous d'envoyer des demandes d'amitié ou d'accepter une demande d'amitié de personnes inconnues, et vérifiez les photos affichées sur leur page et la liste de leurs amis avant d'accepter leur amitié.

- Prenez garde de partager les données de vos comptes sur les réseaux sociaux ou de ne permettre à aucun d'utiliser vos comptes dans toutes circonstances.

- Déconnectez-vous de vos comptes sur les réseaux sociaux après avoir terminé de les utiliser.

- Assurez-vous que les comptes sur les réseaux sociaux sont liés au numéro de téléphone mobile afin de vérifier les données du compte en y accédant, et ce pour faciliter le processus de récupération en cas de perte.

- Prenez garde de cliquer sur les liens non-sécurisés dans les médias sociaux, du fait qu'ils peuvent contenir des virus malveillants.

Comment se protéger sur Internet ?

Evitez de cliquer sur les pièces jointes et les liens contenus dans les e-mails dont l'expéditeur est inconnu

Pensez bien avant de publier des photos et des vidéos illustrant vous et votre famille

Préservez la confidentialité de vos informations personnelles, telles que votre adresse personnelle, lieu de travail, comptes, numéro de téléphone, mots de passe...

Evitez de communiquer avec les étrangers, contactez seulement les personnes que vous connaissez bien et auxquelles vous faites confiance

4.1.3– Protection des comptes du courrier électronique

- Respectez les critères de sélection de mot de passe susmentionnés.

- Veillez à créer personnellement votre nouveau courriel et soyez vigilant au cas où vous autorisez quelqu'un de vous prêter assistance, sachant qu'il sera de ce fait capable de récupérer le mot de passe même si vous le changer.

- Révisez les paramètres de sécurité avancées dans vos propres comptes et activez-les afin d'augmenter le niveau de protection lié aux adresses électroniques, dont l'activation de la fonction d'authentification à double facteur, et la protection contre les courriels indésirables, et l'utilisation du filtre de messagerie etc.

- Partagez les informations liées à votre adresse électronique uniquement avec des personnes dignes de confiance.

- Vérifiez bien les champs des destinataires BCC, CC and TO pour éviter d'ajouter des personnes indésirables.

- Créez une adresse électronique supplémentaire pour restaurer votre adresse électronique principale en cas de piratage ou de vol.

- Abstenez-vous d'utiliser votre adresse électronique pour jouer aux jeux électroniques douteux.

- Méfiez-vous des personnes qui regardent secrètement quand vous devez ouvrir votre courriel dans un lieu public.

- Ignorez les courriers électroniques provenant de sources inconnues ou non-identifiées, requérant vos données personnelles comme que le nom de compte, les mots de passe ou autres.

- Veillez à ne pas ouvrir les liens ou les pièces jointes entrant dans votre boîte postale avant de vérifier la source, et ce pour éviter de télécharger des logiciels nuisibles ou malveillants visant à pirater le compte et le dispositif à des fins d'espionnage ou de sabotage.

- Supprimez immédiatement les courriels indésirables et évitez toute interaction ou réplique; une telle démarche pourrait contribuer à la réception de nouveaux courriels indésirables.

- Méfiez-vous de laisser votre adresse électronique visible sur les réseaux sociaux et autres sites Web, et ne la fournissez qu'aux personnes que vous connaissez.

- Méfiez-vous des courriels dont vous n'êtes pas le destinataire, utilisant des expressions de salutation générales telles que « cher utilisateur » et « cher utilisateur du courriel », sachant qu'il peut s'agir de tentatives d'hameçonnage.

- Veuillez à assurer dans la mesure du possible, la connexion Internet via le protocole sécurisé https, qui est généralement précédé par le symbole de verrou, et ce pour garantir l'intégrité des informations durant les communications avec les fournisseurs de services de messagerie électronique.

- Méfiez-vous des courriels suggérant un état d'urgence qui vous concerne (comme le fait que vous avez dépassé le quota de vos messages, vous avez été victime d'un hameçonnage ou votre courriel est sur le point d'être fermé ...) sachant qu'il peut s'agir de tentatives de violer la confidentialité ou de pirater le compte.

- Abstenez-vous de partager vos informations confidentielles et sensibles (telle votre carte de crédit) ou autres informations importantes par courriel.

- Évitez d'interagir avec les messages tentants qui prétendent que vous avez gagné un prix ou une somme d'argent ; Ces messages visent souvent à mettre en œuvre un hameçonnage frauduleux.

- Conservez d'une façon permanente et périodique des copies de sauvegarde des courriers importants dans la boîte postale.

- Veuillez à vous déconnecter de votre courriel après avoir fini de l'utiliser.

- Ouvrez votre courriel périodiquement pour éviter son expiration ; Le courriel non-utilisé utilisé sera récupéré par la compagnie ce qui le fait disponible à autre personne, et exposé, à travers ce dernier à la piraterie.

4.1.4– Protection des applications de messagerie instantanée (whatsapp, skype, signal, telegram...)

- Respectez les critères de sélection de mot de passe susmentionnés.

- Révisez les paramètres de sécurité avancées dans les applications de messagerie instantanée et activez-les afin d'augmenter le niveau de protection lié à ces applications électroniques, dont l'activation de la fonction d'authentification à double facteur pour la validation d'accès, l'encodage des messages, la sauvegarde des messages importants...

- Méfiez-vous des messages provenant de sources inconnues ou non-identifiées, requérant vos données personnelles et évitez d'ouvrir les liens ou les pièces qui y sont jointes pour ne pas télécharger des logiciels nuisibles ou malveillants visant à voler les informations et données personnelles et à pirater le dispositif.

- Signalez les courriels indésirables dès réception auprès de l'administration de l'application.

- Bloquez les utilisateurs indésirables pour les empêcher de communiquer directement avec vous.

- Soyez prudents quant aux liens attractifs reçus par les applications de chat du fait qu'ils peuvent contenir des virus nuisibles.

- Evitez de vous engager dans les groupes de chat diffusant des informations hostiles ou identifiées comme risquées.

- Evitez de vous engager dans des répliques ou interactions avec des messageries de chat provenant de sources inconnues ou non-identifiées.

- Abstenez-vous de communiquer ou de partager vos photos par le biais des appels vidéo avec quiconque pour ne pas être victime d'extorsion de quelque nature que ce soit.

- Supprimez vos comptes de chat dans les différentes applications et effacez toutes les données qui y sont liées et ce avant de renoncer à votre téléphone mobile pour quelque raison que ce soit.

- Renforcez les paramètres de sécurité en utilisant le code PIN pour ouvrir les applications de chat.

- Veuillez à télécharger toutes les applications par le biais des sites officiels tels Apple Store and Google Play Store.

- Evitez d'envoyer des données confidentielles, des coordonnées bancaires, des mots de passe ou d'autres documents considérés comme sensibles.

4.2– Assurer la sécurité des enfants sur Internet

- Discutez régulièrement avec les membres de la famille le problème des menaces cybernétiques sur les réseaux sociaux et les applications de messagerie instantanée, notamment le cyber-harcèlement et le sextorsion.
- Contrôlez l'accès à internet de vos enfants ; Il est recommandé de garder les différents dispositifs électroniques à portée de vue dans la maison (dans la salle de séjour et non pas dans la chambre à coucher).
- Il est recommandé de passer quelque temps avec vos enfants sur Internet pour leur informer de la navigation privée et s'assurer de leur bon usage de l'internet.
- Parlez ouvertement avec vos enfants sur les informations personnelles qui doivent rester confidentielles, sachant que ces informations peuvent être utilisées pour les reconnaitre, identifier leur adresse, les endroits fréquentés ou les activités auxquelles ils participent afin de leur faire du mal.

- Conseillez vos enfants d'être assez prudents en affichant leurs vidéos et photos sur Internet et réseaux sociaux, vu qu'ils seront facilement accessibles et utilisés à des fins abusives.

- Mettez vos enfants en garde contre l'interaction avec des personnes étrangères ou des personnes inconnues, ou contre le partage des photos, des données, des vidéos ou des informations personnelles (domicile, téléphone, courriel) avec eux. Avertissez vos enfants des conversations vidéo et faites de votre mieux pour les empêcher d'accepter de rencontrer des personnes étrangères ou des personnes inconnues.

- Incitez vos enfants à s'engager dans des conversations avec vous et vous informer de tout problème, menace ou chantage auquel ils pourraient être confrontés sur Internet, quelle que soit son ampleur.

- Explorez avec vos enfants leurs sites préférés et aidez-les à s'y abonner et à s'y inscrire en choisissant un pseudonyme tout en les mettant en garde contre la divulgation des informations sur leur identité personnelle.

- Etablissez un ensemble de règles pour les enfants et assurez-vous qu'ils savent bien la nature des informations apte à être partagées et déterminez les types de sites Web et les jeux appropriés à leur âge et qu'ils peuvent visiter en ligne.

- Limitez le temps que vos enfants passent sur internet sachant qu'ils ont besoin d'un certain équilibre dans les activités pour vivre leur enfance d'une façon saine ; Prenez à cet effet les mesures convenables, comme éteindre le périphérique « routeur » pendant le sommeil ou en d'autres moments.

- Encouragez vos enfants à utiliser les paramètres de sécurité et confidentialité dans les programmes et les applications afin de garantir leur protection.

- Créez un compte électronique familial pour les divertissements aptes à être utilisé pour participer à des compétitions et à d'autres activités.

- Conseillez vos enfants de ne pas diffuser des informations, vidéos ou images injurieux sur Internet, étant donné que cela pourrait les exposer à des poursuites judiciaires.

- Dites à vos enfants de s'abstenir de répondre aux messages préjudiciables ou de communiquer avec celui qui leur envoie des messages offensants sur internet.

- Conseillez à vos enfants de ne pas télécharger de copies illégales des logiciels et applications, ou télécharger des chansons ou des films d'une façon illégale, ou de s'engager dans des jeux qui ne conviennent pas à leur âge.

- Conseillez vos enfants de ne pas appuyer sur les boutons et les annonces publicitaires promouvant des matchs ou de prix sur Internet, sachant que la plupart de ces annonces publicitaires contiennent des logiciels malveillants ou contribuent à la diffusion des contenus nuisibles.

- Il faut s'abstenir d'ouvrir les e-mails anonymes contenant des pièces jointes ou des liens sachant qu'il peut s'agir d'une forme d'hameçonnage ou contenir des virus nuisibles.

- Conseillez vos enfants d'utiliser des moteurs de recherche adaptés à leur âge tel Kiddle.co, kidrex.org et autres.

- Veuillez à contrôler d'une façon régulière les comptes de vos enfants sur les sites des réseaux sociaux et de se poser la question suivante « Est-il possible d'abuser de ces informations ? »

- Veuillez à vérifier l'historique de navigation d'une façon régulière pour voir les pages et adresses électroniques consultés par vos enfants.

- Abstenez-vous de fournir le numéro de carte de crédit aux enfants pour ne pas leur permettre d'exécuter des opérations d'achat et de paiement douteuses, à votre insu.

- Veuillez à utiliser le système de contrôle et filtrage parental pour contrôler et restreindre l'accès aux programmes et sites indésirables tout en permettant aux parents de gérer les activités de leurs enfants sur Internet et de leur empêcher d'accéder aux sites non adaptés pour leur âge.

- Veuillez à sensibiliser les enfants à ne pas supprimer les messages offensants pour les garder comme des preuves de sauvegarde, le cas échéant.

- Veuillez à configurer les paramètres de sécurité dans le navigateur web, comme l'activation du AdBlocking et du Web Filtering.

4.3– Mesures de protection des dispositifs électroniques

Afin d'améliorer les mesures de sécurité et de protection, les utilisateurs peuvent mettre en œuvre certaines mesures visant à protéger les dispositifs électroniques contre le piratage ou la cyber-infiltration :

4.3.1– Mesures de protection des ordinateurs de bureau et des ordinateurs portables

- Respectez les critères de sélection de mot de passe susmentionnés.

- Veuillez à activer le nouvel outil pare-feu (firewall) intégré aux logiciels Windows et Mac pour combler les failles de sécurité des informations qui peuvent être utilisées par les criminels d'internet.

- Activez le système de verrouillage automatique de l'écran/du dispositif peu de temps après avoir arrêté de l'utiliser.

- Veuillez à activer la configuration des mises à jour automatique pour tous les logiciels / applications et ainsi que les systèmes d'exploitation, et ce afin de combler les lacunes constatées au niveau de la sécurité et à travers lesquelles les cybercrimes sont exécutés.
- Désactivez la fonction d'accès à distance à votre ordinateur et activez-la uniquement si nécessaire.
- Veuillez à utiliser un logiciel fiable antivirus et antimalware, et adoptez des copies originales pour les mettre à jour continuellement.

- Ne téléchargez points des logiciels ou des jeux à partir des sites non fiables, et veuillez toujours à les télécharger à partir de leurs sites d'origine.

- N'hésitez point à ignorer les messages et publicités Ads & Popups qui vous invitent à télécharger certains logiciels visant à nettoyer votre ordinateur des virus et des logiciels malveillants.

- Ignorez les demandes de téléchargement / transfert de logiciels ou applications visant à fournir des services spécifiques s'ils sont reçus de sources non fiables.

- Méfiez-vous des offres gratuites de téléchargement de chansons et de jeux, sachant qu'il s'agit de moyens assez communs pour diffuser des logiciels malveillants.

- Vérifiez attentivement les attributions associées aux applications et logiciels et l'étendue de leur besoin avant de les télécharger.

- Désinstallez les applications et les logiciels dont vous n'avez pas besoin.

- Évitez de travailler sur des dispositifs portables, dans des endroits bondés qui ne bénéficient pas de la confidentialité (comme un café, un hôtel, etc.), pour éviter de les regarder secrètement, en particulier lorsque vous travaillez sur des données et des informations privées ou sensibles.

- Veillez à ne pas utiliser la clé USB ou d'autres méthodes de stockage amovible avant de l'inspecter pour vous assurer qu'elle est exempte de logiciels malveillants.

- Effectuez une réinitialisation des paramètres d'usine (Factory Reset/Wipe Data) dans votre smartphone ou votre tablette avant d'en disposer pour quelque raison que ce soit.

4.3.2– Mesures de protection des smartphones et des tablettes

- Activez les paramètres de sécurité avancés (Advanced Security Settings) du smartphone et des tablettes telles que les mots de passe compliqués, la fonction de vérification biométrique (comme la reconnaissance faciale, les empreintes digitales et le scan rétinien), et utilisez des configurations compliquées pour protéger ces appareils.
- Activez la fonction de suivi de l'appareil (Find my phone) et du verrouillage automatique (Autolock) pour sécuriser l'appareil et le retrouver facilement en cas de perte ou de vol.
- Activez le verrouillage automatique de l'appareil après une courte période de non-utilisation.
- Activez la fonction de mise à jour automatique ou périodique (Automatic Update) pour tous les programmes/applications ainsi que les systèmes d'exploitation OS, afin de combler les lacunes de sécurité dans les logiciels qui pourraient être utilisés pour pirater votre appareil.
- Evitez de changer les configurations originales de votre téléphone (par exemple: Rooting ou Jailbreaking).
- Veillez toujours à couvrir la caméra de l'ordinateur portable si non utilisée.
- Déconnectez le dispositif de tous les moyens de communication (Bluetooth, NFC, WiFi) si non pas utilisés.

- Coupez la liaison de l'appareil au réseau de télécommunications (par exemple WIFI, NFC, Bluetooth) si vous ne l'utilisez pas.
- N'accordez pas les permissions qui semblent exagérés ou illogiques aux applications ou logiciels sur le téléphone mobile ou intelligent.
- Téléchargez les applications dont vous avez réellement besoin, uniquement de leurs magasins officiels (comme Google Play Store ou Apple Store) pour éviter les logiciels malveillants.
- Revoyez l'opinion des utilisateurs (notes et avis - Rating & Reviews) concernant la performance, l'efficacité et la fiabilité de l'application que vous avez l'intention d'utiliser avant de la télécharger.
- Téléchargez un programme antivirus fiable (Antivirus & Antimalware) et mettez-le à jour d'une façon régulière.
- Utilisez un réseau fiable pour vous connecter à Internet et évitez les réseaux publiques et gratuits sauf si nécessaire.
- Evitez d'enregistrer les mots de passe ou les informations sensibles sur votre smartphone ou appareil mobile.
- Tenez toujours à garder des copies du contenu de votre appareil et de vos données importantes (ex : contacts, SMS, fichiers, photos et vidéos personnelles, chats etc.) sur disque, CD, DVD, disque dur ou Cloud afin de minimiser les dégâts causés par toute sorte de virus et de programmes malveillants exigeant une rançon ou résultant du vol ou de la perte du téléphone ou de l'appareil mobile.
- Tenez à effacer les réseaux Wi-Fi publiques que vous avez dû utiliser à certains moments.
- Dans les lieux publics, gardez votre appareil en vue et ne le laissez pas hors de portée, même pour une courte durée.
- Veillez à garder pour vous le numéro de série IMEI de votre portable.

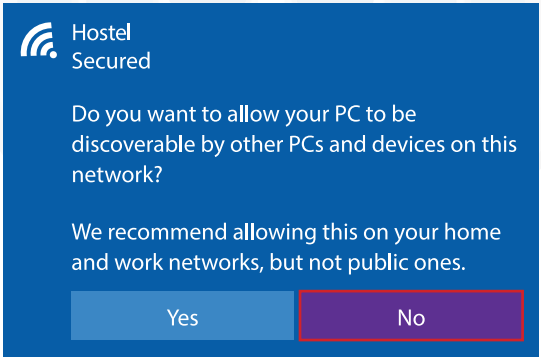
4.4– Mesures de protection du réseau Wi-Fi et des appareils qui y sont liés

4.4.1– WI-FI Public

- Évitez de vous connecter aux réseaux Wi-Fi publics: cafés, restaurants, hôtels, etc. L'accès aux services prépayés d'Internet par téléphone reste plus sécurisé.

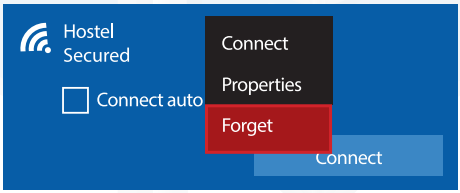
- Toutefois, si vous devez vous connecter à un réseau WI-FI public, veillez à suivre les mesures suivantes:

    - Ne laissez pas d'autres appareils détecter votre ordinateur pendant la connexion.

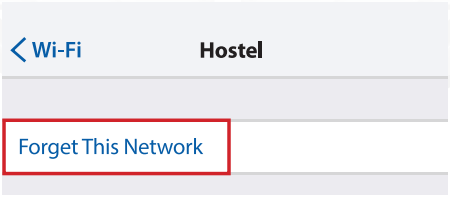


- Evitez la connexion automatique en supprimant (Forget) les réseaux Wi-Fi auxquels vous n'avez pas l'intention de vous connecter de la liste des réseaux fiables à l'avenir.

- Exemple: suppression d'un réseau WI-FI sur Windows:



- Exemple: suppression d'un réseau WI-FI sur IPHONE:



4.4.2– Respecter et appliquer les critères de sélection des mots de passe précités en se connectant à votre réseau Wi-Fi.

- Vérifiez les paramètres de sécurité sur l'appareil Wi-Fi ou le routeur, modifiez le nom d'identification SSID, le nom d'utilisateur et le mot de passe du routeur spécifiés pour le fabricant et appliquez les mises à jour automatiques (Automatic Updates) pour le programme du routeur.

- Activez le cryptage de la communication sur le réseau Wi-Fi privé via les plus nouvelles formes de cryptage (WPA2 / 3 ...) afin de protéger les données entrantes et sortantes de chaque appareil et éviter leurs piratages.

- Adoptez l'authentification à deux facteurs pour les appareils électroniques et les comptes connectés à Internet si possible.

- Déconnectez le routeur wifi en cas de non-utilisation afin d'éviter son piratage.

4.5–Mesures de protection des transactions électroniques et financières

Vous trouvez ci-dessous certaines instructions et mesures qui aident les utilisateurs à préserver l'intégrité des fonds et des cartes de crédit et à protéger leurs transactions financières et électroniques sur Internet.

4.5.1– Mesures de protection des transactions bancaires électroniques

- Réalisez des opérations bancaires électroniques par ordinateurs et portables sécurisés et dotés de logiciels antivirus de pointes pour détecter et corriger les vulnérabilités dans les applications et les systèmes d'exploitation installés.

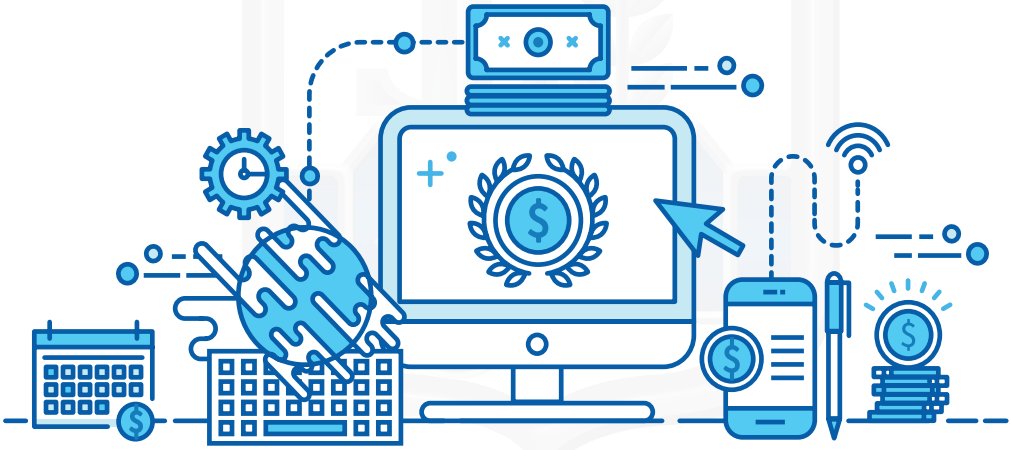
- Évitez d'effectuer des opérations bancaires électroniques si vous êtes connectés à Internet via un réseau Wi-Fi public, ou les sites de communication n'utilisent pas le protocole https

- Ne divulguez pas les détails de vos comptes ou cartes bancaires sauf à des personnes dignes de confiance (par exemple : représentants des banques, des hôtels, etc.) et soyez attentif aux informations que vous révélez.
- Soyez attentif aux informations que vous partagez par téléphone avec tout appelant qui vous demande des détails concernant vos comptes, cartes bancaires ou transactions financières.
- Ne partagez pas les mots de passe (PIN) Et ceux qui sont donnés par la banque pour une seule fois (OTP : One Time Password) avec quiconque, même si cette personne est un employé de la banque. Soyez certain qu'un employé de la banque ne vous demandera jamais les codes de votre compte ou de votre carte de crédit.

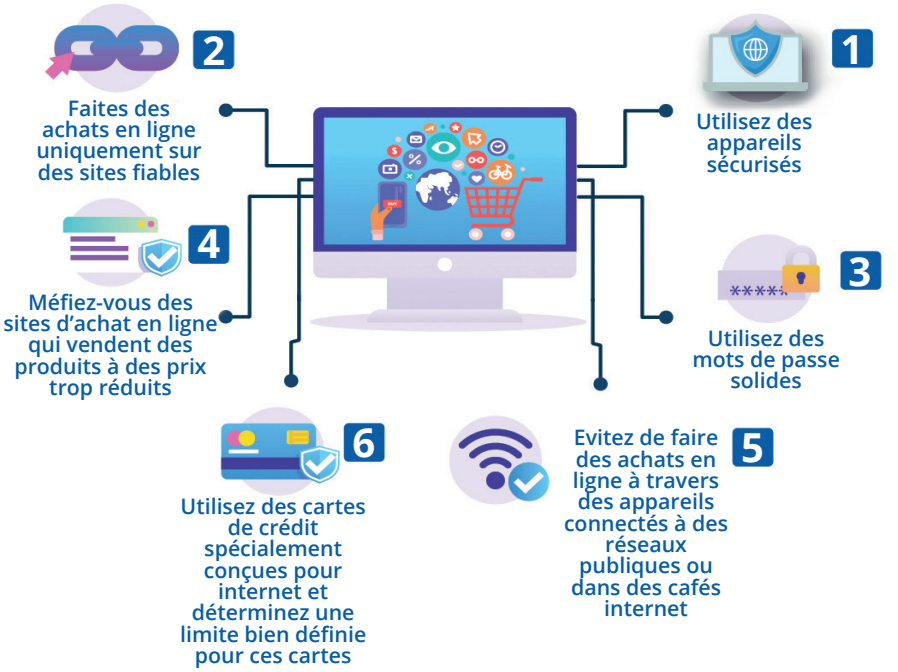
- Assurez-vous que le clavier est hors de vue lorsque vous tapez votre PIN code sur ATM ou lors d'un paiement et évitez de le révéler ou de le donner à quiconque.
- Prenez garde des vols à la tire de votre carte de crédit dans les endroits bondés.
- Détruisez les cartes de crédit périmées en les coupant en petits morceaux et assurez-vous que la bande magnétique et la puce sont détruits.
- Revoyez de temps à autre vos comptes bancaires, en particulier ceux liés à vos cartes de crédit, pour vous assurer de l'exactitude et de la véracité des transactions financières exécutées et informez la banque de toute transaction ou paiement suspects ou même des petites sommes retirées de vos comptes d'une façon régulière.
- La nécessité de procéder à une vérification et à une validation supplémentaire des opérations (exemple : rappel du demandeur) concernant tout paiement dépassant le plafond autorisé.
- Evitez de communiquer des informations relatives à votre compte bancaire après avoir cliqué sur un lien dans un e-mail ou un SMS, car cela pourrait entraîner le vol de vos données et informations personnelles et bancaires.
- Ne répondez jamais à un e-mail prétendant provenir de la « banque » ou de n'importe quelle société demandant votre compte ou des informations confidentielles telles que les mots de passe, les numéros des cartes de crédit, les numéros d'identification personnels ou les numéros d'identification fiscale.
- Déconnectez-vous (logout) dès que vous finissez d'utiliser les services bancaires en ligne.

Mesures de protection des transactions bancaires électroniques

- ✓ Utilisez des appareils sécurisés pour effectuer vos opérations électroniques et bancaires
- ✗ Evitez de partager à travers votre téléphone ou à travers un lien ou un SMS des détails concernant votre compte, votre carte bancaire ou vos opérations financières
- ✓ Utilisez des mots de passe solides
- ✗ Evitez de partager vos mots de passe, vos noms d'utilisateur et vos codes PIN
- ✗ N'effectuez pas de transactions bancaires électroniques lorsque vous êtes connecté à des réseaux Wi-Fi publiques
- ✓ Veillez à utiliser le site officiel de la banque (soyez prudents à l'égard des liens suspects qui prétendent être liés à la banque)
- ✗ Evitez de répondre aux messages ou appels suspects
- ✓ Effectuez des vérifications supplémentaires sur les opérations financières



4.5.2– Mesures pour un achat en ligne sécurisé



- Ne faites pas d'achats en ligne que des sites fiables qui offrent une connexion sécurisée et codée (https ou le symbole du verrou 🔒) .

- Méfiez-vous des moyens de communication suspects pour contacter le service clientèle dans les centres commerciaux en ligne (exemple : le courriel du service clientèle supportcompany@gmail.com au lieu de support@company.com).

- Méfiez-vous des centres commerciaux en ligne qui proposent des produits à des prix très bas et illogiques, suggérant qu'ils sont utilisés pour effectuer des opérations frauduleuses. Parmi les adresses suspectes, on a par exemple « brands-at-awesome-price.com » qui a pour but de mener des opérations d'escroquerie.

- Evitez tout achat en ligne via certains liens reçus par e-mail (par exemple, un e-mail ayant pour but le "phishing" contenant une offre fictive d'un produit souhaité avec un bouton "achetez maintenant".

- Evitez tout achat en ligne via des appareils dans des cybercafés ou via un réseau Wi-Fi public.

- Ne fournissez pas d'informations au-delà de celle nécessaire pour effectuer un achat en ligne.

- Lisez attentivement les opinions des autres consommateurs qui ont eu une expérience positive ou négative avec le même site, vendeur ou produit.

- La nécessité de fixer une limite pour les montants pouvant être retirés des cartes de crédit en une fois. Il est possible d'utiliser des cartes de crédit pour internet (internet credit card) ou prépayées.

- Aucun détail des cartes de crédit ne doit être sauvegardé sur les sites d'achat en ligne.

4.5.3– Mesures de protection contre la fraude financière via l'e-mail professionnel Compromis de messagerie professionnelle (Business Email Compromise)

- La nécessité d'analyser minutieusement les différents messages électroniques, notamment les demandes de virements de fonds et les requêtes inhabituelles des directeurs exécutifs.
- La nécessité de mettre en place des mécanismes et des mesures strictes pour les demandes de virements de fonds reçues par courriel avant d'envoyer des données ou de transférer de l'argent, par exemple:

  ◊ Vérifiez la facture
  ◊ Vérifiez et assurez-vous des détails de paiement du destinataire.
  ◊ Consultez le directeur exécutif, l'avocat ou la compagnie d'assurance ... concernant toute demande liée à des virements de fonds.
- Vérifiez les e-mails comportant des fautes d'orthographe ou des demandes inhabituelles, surtout si le délai de paiement ou de virement est court.
- Vérifiez minutieusement le courriel de l'expéditeur, étant donné que l'e-mail du pirate comprend la plupart du temps une lettre supplémentaire ou différente.
- Vérifiez les demandes de modification de paiement en appelant l'intéressé à un numéro connu auparavant et non à celui indiqué dans l'e-mail contenant la demande.
- Demandez à l'expéditeur d'envoyer les modifications relatives au nouveau mode de paiement par lettre portant le logo de l'entreprise et vérifiez l'authenticité de ce logo.
- Vérifiez tout changement dans les détails de paiement du vendeur au moyen d'une deuxième signature de l'un des employés de l'entreprise.

5. Modalités de traitement des cybers crimes

Comment agir en cas de cyber-risque ou crime:

5.1– Comment agir en cas de perte ou de vol de smartphone ou d'appareil mobile:

En cas de vol ou de perte de votre appareil mobile ou smartphone, vous pouvez prendre une série de mesures, dont certaines sont liées aux procédures de sécurité exposées précédemment dans ce manuel.

Dans ce cas:

- Essayez d'appeler le téléphone mobile à partir d'un autre numéro, pour déterminer s'il sonne.

- Si le dispositif de traçage de l'appareil est précédemment activé (Find my device sur android.com/find pour android et icloud.com/find pour iphone), les étapes suivantes sont à suivre :

a. Vérifiez l'emplacement de l'appareil sur l'application et activez l'alarme si le site est proche.

b. Ne vous rendez pas au lieu où l'appareil fut localisé s'il est loin et informez les Forces de Sécurité Intérieure immédiatement.

c. Utilisez la fonction de verrouillage de l'appareil (Secure Device ou Lock Device) qui permet de verrouiller votre téléphone à distance afin que personne ne puisse accéder à son contenu. À cette fin, vous pouvez afficher un message de votre choix sur l'écran de verrouillage indiquant que l'appareil est perdu.

- Si vous gardez les détails de votre carte de crédit sur le navigateur ou dans une des applications de votre téléphone, contactez immédiatement la banque pour interdire toute transaction et émettre d'autres cartes. Si vous utilisez les services bancaires électroniques à partir du téléphone, vous devez demander le changement immédiat des mots de passe si vous n'êtes pas en mesure de le faire vous-même.

- Tous les mots de passe des différents comptes liés à votre téléphone doivent être modifiés, notamment le mot de passe des magasins d'applications afin que personne ne puisse effectuer des achats.

- Informez les autorités chargées de l'application de la loi de la perte ou du vol de l'appareil et leur donner son numéro de série (IMEI) sur demande.

- Veillez à appeler le service clientèle de la compagnie de téléphone pour mettre le numéro de téléphone hors service et suspendre tous les services.

- Essayez de vous connecter via un autre appareil à tous les services et comptes précédemment utilisés à partir de votre téléphone volé et cliquez sur la fonction de déconnexion de tous les autres appareils (Logout from all other devices) afin de les désactiver sur l'appareil volé.

5.2–Comment agir en cas de chantage électronique

En cas de chantage et si vous ne savez pas quoi faire, suivez les étapes suivantes:

- Restez calme et ne prenez pas de décision sans consulter une personne de confiance, un ami ou un membre de la famille.

- Ne nuisez pas à vous-même ou aux autres, car la police est là pour aider et s'emploie à lutter contre les crimes et à punir les auteurs.

- Photocopiez et enregistrez toutes les preuves et le contenu de la correspondance et des courriels liés au chantage afin de les montrer ultérieurement à la police.

- Ne communiquez pas avec le maître-chanteur, même sous pression.

- Ne cédez pas aux demandes du maître-chanteur, telles que le transfert d'argent, la divulgation du numéro de la carte bancaire ou l'exécution de toute requête formulée, car ceci peut entraîner une augmentation de la pression pour répondre à des demandes supplémentaires.

- Evitez les altercations avec le maître-chanteur et signalez toutes tentatives de chantage ou d'intimidation aux forces de l'ordre sans faire aucune allusion à votre intention.

- Si la Police vous demande cela, restez en contact avec le maître-chanteur afin de le localiser ou de recueillir des preuves supplémentaires si nécessaire.

5.3– Comment agir en cas de Cyber intimidation ou cyberbullying

- Veillez à ne pas se venger et à ne pas répondre.
- Rassemblez toutes les preuves, enregistrez les SMS, les e-mails ou les discussions sur les réseaux sociaux, et informez une personne de confiance, un membre de la famille ou un ami.
- Signalez tout incident d'intimidation et suivez les conseils de la police en ce qui concerne :
    - Bloquez l'intimidateur et modifiez los paramètres de confidentialité afin de limiter la possibilité d'accéder à vos données et vos publications par des étrangers.
    - Signalez tout abus via le service prévu à cet effet dans l'application concernée.

5.4– Comment agir en cas de piratage de compte sur les sites de réseaux sociaux, SMS ou fournisseurs de services

Le cybercriminel apporte parfois des petites modifications suspectes et difficiles à remarquer aux comptes de réseaux sociaux (Facebook, YouTube, Instagram, Twitter, WhatsApp, Gmail, Snapchat...). Par exemple:

- Ne pas pouvoir se connecter avec votre mot de passe.
- Ajouter / supprimer des amitiés, des demandes d'abonnement, des aimes ou des options que vous n'avez pas faites.
- Mettre à jour le statut ou poster des tweets que vous n'avez pas faits.
- Télécharger des photos à votre insu.
- Envoyer des e-mails privés et agaçants à vos amis.
- Modifier la page principale de profil ou les photos de vos comptes à votre insu.
- Recevoir des courriers électroniques ou des notifications inattendues de l'administration des sites de réseaux sociaux, indiquant par exemple que votre adresse e-mail fut modifiée.

Dans pareil cas, vous pouvez prendre les mesures suivantes pour limiter les dégâts que les pirates peuvent causer et tenter de restaurer votre compte volé:

- Essayez de vous connecter d'un autre appareil pour voir si la possibilité de se loguer est définitivement perdu et vérifiez le mot de passe utilisé plusieurs fois.

- Vérifiez si un avertissement fut envoyé par courrier des sites et des services électroniques concernant des activités suspectes survenant dans votre compte (par exemple, une tentative de se connecter à l'un de vos comptes à partir d'un ordinateur inconnu ou d'un endroit inconnu, ou une tentative de changer le nom de l'utilisateur ou le mot de passe).

- Connectez-vous à la page de support via le site official (Snapchat, Gmail, Instagram), ou envoyez une notification rapportant le problème et demandez le blocage du compte (Twitter, Facebook).

- Suivez les instructions fournies par le site ou le service pour récupérer le compte. Dans ce cas, vous aurez peut-être à confirmer votre numéro de téléphone ou votre courriel de sauvegarde ou répondre aux questions personnelles afin de prouver que vous êtes le véritable titulaire du compte.

- Supprimez les applications (WhatsApp, Telegram, Signal, ...) si le compte fut volé et rechargez-le avec authentification par SMS ou par appel. Ainsi, le compte sera désactivé de l'appareil du pirate et réactivé sur votre appareil.

- Après avoir pu vous reconnecter à votre compte, changez immédiatement le mot de passe et assurez-vous de toutes les informations personnelles et autres paramètres afin qu'il n'y ait pas de changement de numéro de téléphone, de courriel de sauvegarde, des questions personnelles ...

- Veillez à ne pas utiliser de mot de passe que vous avez précédemment utilisé.

- Changez les mots de passe des autres comptes si vous utilisez l'ancien mot de passe pour vous connecter à plusieurs comptes, à noter que ce n'est pas du tout recommandé.

- Ensuite, déconnectez-vous de toutes les autres sessions de contact, à l'exception de la session que vous utilisez actuellement (logout from all other Sessions).

- Revoyez et activez les fonctions de sécurité supplémentaires telles que la fonction d'authentification à deux facteurs (mot de passe + code envoyé à votre téléphone portable) ainsi que les autres fonctions de sécurité conçues pour éviter les attaques (par exemple: Facebook vous permet d'ajouter une liste d'amis de confiance qui pourront confirmer votre identité en cas de piratage de votre compte).

- Si vous ne parvenez pas à récupérer votre compte, contactez vos amis et tous vos contacts et informez-les que votre compte fut piraté. De plus, avertissez-les de ne pas accepter aucun message ou de ne suivre aucun lien reçu de ce compte, et de signaler le compte volé à l'administration du site pour bloquer le compte volé.

5.5– Comment agir en cas d'infection par le logiciel malveillant (Malware)

Certains problèmes pourraient survenir, suggérant que les ordinateurs sont infectés par des virus et des logiciels malveillants : lenteur extrême, forte consommation de la batterie de l'appareil, perte de contrôle, suppression de fichiers, modification de l'ordre habituel des fichiers, certains services et fonctions inopérables et fonctionnement de certaines applications d'une façon automatique et inhabituel.

Dans ce cas, les actions suivantes doivent être prises pour résoudre le problème :

- Si vous n'avez pas une copie de vos fichiers, transférez les données et les fichiers importants sur USB ou un disque dur externe en tenant compte du fait que cela pourrait infecter le disque dur ou la mémoire de stockage que vous avez utilisé pour garder les fichiers susceptibles d'être infectés à leur tour.

- Déconnectez l'appareil de l'Internet.

- Changez tous les mots de passe de tes comptes sur internet en utilisant un autre appareil.

- Mettez votre appareil sur mode de sauvegarde (safe mode), vérifiez le disque à l'aide du système d'exploitation (check disk) et nettoyez-le grâce à la propriété Disk Cleanup.

- Faites un examen exhaustif et nettoyez soigneusement votre appareil avec un programme antivirus et suivez les conseils et les instructions fournis.

Si le programme antivirus ne parvient pas à supprimer et à effacer les programmes malveillants, vous devez:

- Formatez l'ordinateur infecté et téléchargez la copie originale du système d'exploitation tel que Windows, Linux ou macOS ; ainsi, vous serez sûr que votre ordinateur est propre de tout virus.

- Installez un programme anti-virus original et fiable.

- Mettez à jour le système d'exploitation et la base de données du programme anti-virus (antivirus update) et assurez-vous que la mise à jour fut effectuée avec succès avant de vérifier les données des copies de sauvegarde la plus récente, le cas échéant, ou celle transférée sur un disque externe ou une mémoire de stockage USB en première étape.

- Transférez à nouveau les données sur votre appareil.

- Examinez votre appareil et vos données régulièrement en utilisant un anti-virus actualisé.

5.6– Comment agir en cas d'infection par un logiciel Ransomware malveillant

Lorsque votre ordinateur ou smartphone est infecté par ce type de logiciel, nous vous conseillons de ne pas exécuter les instructions des hackers et de ne pas payer le montant requis ou la rançon et ceci pour les raisons suivantes:

- Vous n'avez aucune garantie que vous récupérerez vos données car l'unique but des producteurs de ces programmes est de gagner de l'argent.
- Votre appareil restera infecté par le virus malveillant, si vous vous ne le nettoyez pas d'une manière exhaustive.
- Le chantage ne cessera pas et les pirates exigeront plus d'argent ou essaieront de vous attaquer à nouveau afin de vous faire payer d'autres rançons.
- Vous contribuerez d'une manière ou d'une autre au financement de groupes criminels.
- Vous encouragerez ces criminels à développer ces logiciels et à vous prendre comme cible à nouveau.

Dans ce cas, il est recommandé de prendre certaines mesures pour nettoyer l'appareil et le remettre dans son état normal comme suit :

- Essayez de déterminer le type de virus qui pourrait être un virus Locker/Blocker ou un Cryptor qui est un virus de cryptage de fichiers.

- Si vous ne parvenez pas à ignorer la notification qui apparaît sur l'écran et qui avertit de la présence d'un virus, l'appareil est probablement infecté par un Locker qui bloque l'écran, mais si vous parvenez à le dépasser et à accéder à certains ou à tous vos fichiers, vous serez infecté par un Cryptor où le virus de cryptage de fichiers.

- Si vous parvenez à parcourir le système et lire la plupart des fichiers sans aucun problème, vous serez alors confronté à une tentative d'escroquerie ayant pour but de vous obliger à payer une somme d'argent en plaçant une certaine photo sur l'écran (desktop background).

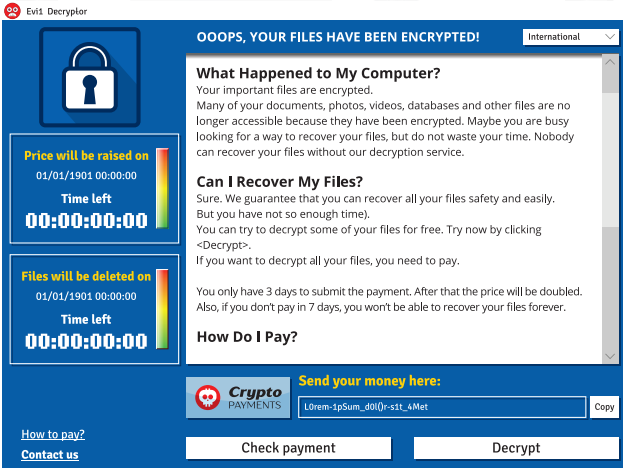
En cas de Cryptor (virus de cryptage de fichier) :

- Déconnectez votre appareil des autres appareils et de tout disque externe.

- Utilisez une caméra pour photographier l'avertissement concernant la présence de virus qui apparaît sur l'écran et signalez-le à la police.

- Essayez de récupérer certains fichiers cryptés à l'aide d'un des programmes de décryptage gratuits qui peuvent être utile avec certains types de ransomwares.

- Utilisez un programme antivirus et effectuez un scan pour essayer de vous débarrasser du ransomware. En adoptant cette solution, vous ne pourrez peut-être pas récupérer vos fichiers cryptés, mais vous serez sûr qu'il n'y a plus de malware.



- Vérifiez si vous pouvez récupérer vos fichiers car certains types de virus cryptés copient vos fichiers et cryptent ces copies avant de supprimer les fichiers originaux. Dans ce cas, il est possible de restaurer les fichiers supprimés en utilisant des applications gratuites telles que ShadowExplorer.

- Utiliserez certaines applications qui aident à déterminer le type et le nom du virus comme Crypto Sheriff, certains outils comme ID Ransomware ou autres....

- Vérifiez s'il y a un outil de décodage en cherchant sur le site « nomoreransom.org ».

- Si vous ne parvenez pas à désactiver et à décoder le ransomware, restaurez votre appareil à la dernière copie prise (Restore Point). Si cette tentative échoue, réinitialisez votre appareil aux paramètres d'usine (Restore Factory Settings) et téléchargez le système d'exploitation à nouveau puis restaurez vos fichiers à partir des copies de sauvegarde créées auparavant.

- Quant au verrouillage d'écran (Screen-locker), le processus de restauration du système sera suffisant pour y accéder à nouveau. Si cela ne fonctionne pas, la solution consiste à utiliser un CD de secours avant d'activer l'appareil et d'effectuer une opération de balayage (scan).

5.7– Comment agir en cas de perte ou de vol de la carte de crédit

Lorsque vous soupçonnez que votre carte de crédit fut volée, perdue, piratée ou utilisée sans votre consentement ou votre connaissance, les procédures suivantes doivent être suivies:

- Contactez directement l'autorité qui a émis la carte de crédit via des canaux de communication fiables: appelez par exemple le service clientèle pour signaler le vol ou la perte de votre carte pour prendre les mesures nécessaires afin de la suspendre et la remplacer.

- Vérifiez le relevé de compte de la carte pour vous assurer qu'aucune opération illégale n'y est incluse et qu'aucun frais ou coûts supplémentaires ne fut imposé sur les transactions informelles.

- Si des frais inhabituels furent constatés, la partie qui a émis la carte doit en être informée afin de prendre les mesures nécessaires pour récupérer la somme prélevée.

- Recueillez la nouvelle carte de crédit de l'entité qui l'a émise et prenez les mesures de sécurité et de protection susmentionnées.

- Mettez à jour votre portefeuille mobile (Mobile Wallet) et tous vos comptes sur les sites d'achat en ligne si vous utilisez votre carte perdue comme mode de paiement.

5.8– Comment agir en cas de fraude bancaire sur Internet

Si vous soupçonnez que vous avez été victime ou vous pourriez être une victime potentielle d'une fraude bancaire ou financière, les mesures suivantes doivent être prises:

- Signalez-le immédiatement à la partie concernée par les opérations frauduleuses auprès de votre banque pour prendre les mesures nécessaires.

- Changez le mot de passe de votre compte bancaire sur le site ou dans l'application mobile.

- Enregistrez la date et l'heure à laquelle vous avez découvert / signalé l'opération frauduleuse ainsi que toutes autres observations pertinentes.

- Surveillez le compte bancaire et enregistrez toute transaction suspecte qui a lieu sur votre compte pour l'utiliser comme preuve.

- Essayez d'enregistrer ce qui s'est passé? Qui est l'auteur de cette action ? L'opération est-elle toujours en cours? Quand est-ce cette opération a eu lieu? Quelle est la valeur des pertes ou des pertes potentielles?

- Identifiez les différentes preuves associées à l'opération ainsi que les factures, contrats, ordres d'achat, chèques, etc.

6- Contacter les Forces de Sécurité Intérieure pour solliciter leur assistance

Les Forces de Sécurité Intérieure tiennent à préserver la confidentialité totale des investigations menées dans les cybers crimes et ne ménageront pas leurs efforts afin de résoudre votre problème.

Signalez aux Forces de Sécurité Intérieure toute cyber-menace, risque ou crime par l'un des moyens suivants:

- Bureau de la lutte contre la cybercriminalité et de Protection de la Propriété Intellectuelle: **+961 1 293293**
- Service "**بلغ**" Sur le site des Forces de Sécurité Intérieure :

www.isf.gov.lb

Service de rapport

* Texte du rapport

* Type de rapport

Cyberintimidation

* Email

* Téléphone (chiffres uniquement)

* voulez-vous qu'on vous contacte ?

Oui

Note: S'il y a des pièces jointes, veuillez les envoyer via l'email mentionné ci-dessus à l'adresse: ballegh@isf.gov.lb

- ○ Non, je n'enverrai pas de pièces jointes.
- ○ Oui, j'enverrai les pièces jointes par e-mail.

Envoyer

FORCES DE SÉCURITÉ INTERIEURE LIBANAISES

DÉPARTEMENT DES RELATIONS PUBLIQUES

SERVICE - CONFIANCE - PARTENARIAT

Preparé par:
Comité de la Cybersécurité
Novembre 2020

Funded by the European Union