R.S.S.I.
Laurent Péquin
Université de La Réunion

Bonnes pratiques informatiques

Bonnes pratiques informatiques

Avant-propos

Réalisé par le biais d'un partenariat entre l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et la CGPME, ce guide a pour objectif de vous informer sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples pour sécuriser votre usage de l'informatique. Chaque règle ou « bonne pratique » est accompagnée d'un exemple inspiré de faits réels auxquels l'ANSSI a été confrontée.

Choisir avec soin ses mots de passe

Dans le cadre de ses fonctions de comptable, Julien va régulièrement consulter l'état des comptes de son entreprise sur le site Internet mis à disposition par l'établissement bancaire. Par simplicité, il a choisi un mot de passe faible : 123456. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : l'entreprise s'est fait voler 10 000 euros.

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire.

Trois méthodes simples peuvent vous aider à définir vos mots de passe :

- La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : votre mot de passe devient : ght5CDs%E7am
- La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : votre mot de passe devient : aE2IP,lJ2Géa!
- La méthode de la phrase avec 4 mots finissant par un point d'exclamation : « Ma voiture roule rapidement ! » (le mot de passe est tel quel, avec les espaces et la majuscule au départ, ce qui vous fait 29 caractères)

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle...) ne doivent **jamais** être réutilisés pour d'autres services. Il est préférable de ne pas recourir aux outils de stockage de mots de passe (cf. la politique de gestion des mots de passe sur notre site web), cependant, il existe un outil recommandé par l'ANSSI : Keepass2.

Mettre à jour régulièrement vos logiciels

Carole, administrateur du système d'information d'une PME, ne met pas toujours à jour ses logiciels. Elle a ouvert par mégarde une pièce jointe piégée. Suite à cette erreur, des attaquants ont pu utiliser une vulnérabilité logicielle et ont pénétré son ordinateur pour espionner les activités de l'entreprise.

Dans chaque système d'exploitation (Android, iOS, MacOS, Linux, Windows,...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction. Si vous avez le moindre doute, parlez-en avec votre informaticien de proximité.

Bien connaître ses utilisateurs et ses prestataires

Noémie naviguait sur Internet depuis un compte administrateur de son entreprise. Elle a cliqué par inadvertance sur un lien conçu spécifiquement pour l'attirer vers une page web infectée. Un programme malveillant s'est alors installé automatiquement sur sa machine. L'attaquant a pu désactiver l'antivirus de l'ordinateur et avoir accès à l'ensemble des données de son service, y compris à la base de données de sa clientèle.

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » et les droits dits « d'administrateur ».

Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu,...), prenez un compte utilisateur. Il répondra parfaitement à vos besoins.

Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels,...). Il est réservé aux informaticiens de proximité.

En règle générale, les systèmes d'exploitation récents vous permettent d'intervenir facilement sur le fonctionnement global de votre machine sans changer de compte : si vous utilisez un compte utilisateur, le mot de passe administrateur est demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur. Appliquez cette règle chez vous, sur votre ordinateur personnel afin d'éviter de nombreux risques.

Effectuer des sauvegardes régulières

Patrick, commerçant, a perdu la totalité de son fichier client suite à une panne d'ordinateur. Il n'avait pas effectué de copie de sauvegarde.

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports ainsi que le lieu de stockage (chaleur, possibilité de vol donc accès aux informations de l'université facilement, …)

Attention : copier vos fichiers locaux sur un disque réseau monté en permanence ne constitue pas une sauvegarde fiable (rançongiciels ou ransomware notamment).

Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Arthur possède un ordiphone qu'il utilise à titre personnel comme professionnel. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, l'éditeur de l'application peut accéder à tous les SMS présents sur son téléphone.

- Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique :

- n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;

- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;

- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;
- Utilisez un outil reconnu par l'ANSSI pour stocker vos mots de passe

Protéger ses données lors de ses déplacements

Dans un aéroport, Charles sympathise avec un voyageur prétendant avoir des connaissances en commun. Lorsque celui-ci lui demande s'il peut utiliser son ordinateur pour recharger son ordiphone, Charles ne se méfie pas. L'inconnu en a profité pour exfiltrer les données concernant la mission professionnelle très confidentielle de Charles.

Avant de partir en mission

- n'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;
- sauvegardez ces données, pour les retrouver en cas de perte ;
- vérifiez que vos mots de passe ne sont pas préenregistrés.

Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
- désactivez les fonctions Wi-Fi et Bluetooth de vos appareils ;
- retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d'effacement sécurisé
- refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (ordiphone, clé USB, baladeur...)

Après la mission

- effacez l'historique des appels et de navigation ;
- changez les mots de passe que vous avez utilisés pendant le voyage ;

- faites analyser vos équipements après la mission par un informaticien.

- n'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, voyages...) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Jean-Louis a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Jean-Louis le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

l'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail;

n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts;

si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence;

ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing » ;

n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;

désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

Télécharger ses programmes sur les sites officiels des éditeurs

Emma, voulant se protéger des logiciels espions (spyware), a téléchargé un logiciel spécialisé proposé par son moteur de recherche. Sans le savoir, elle a installé un cheval de Troie.

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Dans ce contexte, afin de veiller à la sécurité de votre machine et de vos données :

- téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance
- pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires
- restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens
- désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

Séparer les usages personnels des usages professionnels

Paul rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

- il est recommandé de séparer vos usages personnels de vos usages professionnels :
- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
- n'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
- de la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Alain reçoit un courriel lui proposant de participer à un concours pour gagner un ordinateur portable. Pour ce faire, il doit transmettre son adresse électronique. Finalement, Alain n'a pas gagné mais reçoit désormais de nombreux courriels non désirés.

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.