Guide d'utilisateurs – Vigipirate dans le domaine numérique

Table of Contents

1. Préambule

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. Le présent guide d'utilisateur couvre les règles et consignes de sécurité régissant l'activité quotidienne. Il est primordial de les respecter afin de renforcer les mesures de sécurité.

Ce guide est un extrait des documents : Guide d'hygiène informatique ANSSI, Bonnes pratiques à l'usage des professionnels en déplacement et Guide des bonnes pratiques de l'informatique

2. Choisir avec soin vos mots de passe

Enjeu: Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à vos données. La fuite de mot de passe permet un hacker d'introduire dans le parc informatique et ensuite causer des dégâts considérables que ce soit financièrement ou fonctionnellement.

Recommandations:

- 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. Vous pouvez calculer la "force" de votre mot de passe via: https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/
- Utilisation d'un logiciel de gestion de mots de passe est fortement conseillé : https://apc.u-paris.fr/APC_CS/fr/intranet/macpass-keepass-client-mac

3. Mettre à jour régulièrement vos logiciels

Enjeu: 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.

Recommandations:

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles
- Utilisez exclusivement les sites Internet officiels des éditeurs.

4. Effectuer des sauvegardes régulières

Enjeu: 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.

Recommandations:

- Pour sauvegarder vos données, vous pouvez faire une demande auprès de l'équipe ASR via https://supportapc.in2p3.fr/. Le Quota est 40 Go par personne. Pour plus de détail: https://apc.u-paris.fr/APC_CS/fr/intranet/sauvegarde-des-portables
- Vous pouvez également utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, que vous rangerez ensuite dans un lieu éloigné de votre ordinateur.

5. Sécuriser l'accès Wi-Fi

Enjeu: L'utilisation du Wi-Fi est une pratique attractive. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes malintentionnées.

Recommandations:

- Activer le client VPN du laboratoire quand vous avez une connexion Wi-Fi.
- Pour avoir l'accès au service VPN du laboratoire : https://www.apc.univ-paris7.fr/APC_CS/fr/intranet/acces-vpn

6. Être aussi prudent avec votre ordiphone (smartphone) ou votre tablette qu'avec votre ordinateur

Enjeu: 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.

Recommandations:

- 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 ;
- Ne préenregistrez pas vos mots de passe

7. Protéger vos données lors de vos déplacements

Enjeu: L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol

ou la perte auraient des conséquences importantes sur les activités de l'organisation. Il convient de se référer au passeport de conseils aux voyageurs édité par l'ANSSI : https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

Recommandations:

- Avant: Evitez le transport de données non nécessaires; Privilégiez l'utilisation de box.in2p3.fr pour stocker vos données nécessaire durant votre mission. Informez-vous sur la législation du pays de destination; Sauvegardez les données que vous emportez.
- Pendant: Faites preuve de discrétion; Évitez de laisser vos documents et équipements sans surveillance; Activez systématiquement le client VPN sur votre ordinateur portable; Utilisez une clé de protection pour la recharge USB qui empêche tout échange de données lorsque vous vous connectez à une prise USB. Cela évite le vol de données, les tentatives d'infections ou de piratage pendant la recharge ; Déclarer en cas de perte, de vol ou tous types d'incidents: https://apc.u-paris.fr/APC_CS/fr/intranet/declarer-un-lincident
- Après: Renouvelez les mots de passe utilisés lors de votre déplacement .
- Au laboratoire, nous disposons des portables de prêt pour votre déplacement. Pour le réserver, merci d'ouvrir un ticket via https://supportapc.in2p3.fr/

8. Être prudent lors de l'utilisation de sa messagerie

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

Recommandations:

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 l'équipe ASR via https://supportapc.in2p3.fr/ ;
- 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.

9. Télécharger vos programmes sur les sites officiels des éditeurs

Enjeu: 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.
Pour rappel, l'installation de logiciel « cracké » (piraté pour ne pas à avoir à payer la licence), est totalement contraire à la charte du CNRS (http://www.dgdr.cnrs.fr/BO/2007/03-07/415-bo0307-dec070007dAj.htm) qui précise que «Les logiciels doivent être utilisés dans les conditions des licences souscrites. ». Évidemment cela engage la responsabilité de l'utilisateur en question.

Recommandations: 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.

10. Être vigilant lors d'un paiement sur Internet

Enjeu: Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand.
Recommandations: Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- Assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;

- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

Si possible, lors d'un achat en ligne :

- Privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire ;
- N'hésitez pas à vous rapprocher votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

11. Séparer les usages personnels des usages professionnels

Enjeu: Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels.
Le AVEC (Apportez Votre Équipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des problèmes en matière de sécurité des données (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).
Recommandation: Dans ce contexte, 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 du laboratoire. **Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de vos travaux de recherche après avoir réussi à prendre le contrôle de votre machine personnelle.**
- Pensez à ouvrir un ticket sur la Plateforme UserSupport afin de demander un portable de prêt pour votre stagiaire en précisant le système souhaité (Linux, Mac Os, ou Windows) car **l'utilisation de portable personnel au réseau du laboratoire n'est pas autorisé.**

12. Prendre soin de vos informations personnelles, professionnelles et de votre identité numérique

Enjeu: 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.

Recommandations: Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- Soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :
- Ne transmettez que les informations strictement nécessaires ;
- Pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;
- Ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;
- Pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité (Guide de la CNIL sur la sécurité des données personnelles: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf) ;
- Enfin, utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...).