

Bonnes pratiques
NUMÉRIQUES

Bonnes pratiques NUMÉRIQUES en 11 leçons

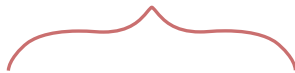
- ✓ Choisir avec soin ses mots de passe 7
- ✓ Être prudent lors de l'utilisation de sa messagerie 9
- ✓ Séparer les usages personnels des usages professionnels 11
- ✓ Prendre soin de ses informations 13
- ✓ Effectuer des sauvegardes régulières 15
- ✓ Mettre à jour régulièrement vos logiciels 17
- ✓ Être prudent avec son smartphone et sa tablette 19
- ✓ Être vigilant lors d'un paiement sur Internet 21
- ✓ Utiliser un antivirus et un pare-feu 23
- ✓ Se méfier des clés usb et protéger ses données 25
- ✓ Télécharger ses programmes sur les sites officiels des éditeurs 27



- Glossaire* 29
- En cas d'incident* 31
- Pour aller plus loin* 31



Pourquoi sécuriser son
INFORMATIQUE?



Alors que le numérique fait désormais partie de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. En effet, les nouvelles technologies sont omniprésentes et porteuses de nouveaux risques. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours, découvertes scientifiques) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un smartphone, d'une tablette, d'un ordinateur portable. La sécurité informatique est donc une priorité pour le bon fonctionnement de l'université: une attaque informatique sur le système peut causer la perte de contrôle, l'arrêt ou la dégradation des informations et des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'établissement.

Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre à l'université. À cet effet, la sensibilisation des collaborateurs aux règles d'hygiène informatique est fondamentale et surtout très efficace pour limiter une grande partie des risques.

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.

Leçon n°1

Jeter son dévolu sur un **MOT DE PASSE**

Choisir avec soin
ses mots de passe



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 types différents (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire.

La robustesse d'un mot de passe dépend :

- ☑ de sa longueur ;
- ☑ de la difficulté de le deviner facilement (présence dans un dictionnaire) ;
- ☑ de la combinaison de différents types de caractères utilisés ;
- ☑ du nombre de caractères utilisables.

Les attaques sur les mots de passe :


- ☒ Force brute : toutes les combinaisons sont essayées (en direct ou sur l'empreinte) ;
- ☒ Ingénierie sociale : obtention du mot de passe par ruse (phishing, usurpation d'identité) ;
- ☒ Vol : il existe des organisations qui louent de puissantes machines ou des réseaux de machines pour tenter de casser les mots de passe des utilisateurs qui détiennent des informations monnayables.



Leçon n°2

Rester prudent face à **L'INCONNU**

Être prudent lors de
l'utilisation de sa messagerie



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

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- △ Avant de cliquer, passez la souris sur le lien pour vérifier l'adresse URL ;
- △ Ne répondez jamais à une demande d'informations personnelles ou confidentielles (phishing) ;
- △ Ne cliquez **JAMAIS** sur les liens contenus dans des messages d'origine douteuse ;
- △ N'ayez jamais une confiance aveugle dans le nom de l'expéditeur ;
- △ N'ouvrez pas de pièces jointes d'expéditeurs non reconnus et dans tous les cas soyez très vigilants avec les pièces jointes ;
- △ 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 ;
- △ N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales...

Leçon n°3

Ne pas mélanger vie **INTIME et PRO.**

Séparer les usages
perso. des usages pro.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone...) personnels et professionnels.

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, smartphone, tablette...) 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, intrusion, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

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...) 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...) 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.

Leçon n°4

Choyer ses précieuses INFORMATIONS

Prendre soin de ses
informations



Les données que vous laissez sur Internet vous échappent instantanément. Des personnes malveillantes pratiquent l'ingénierie sociale: elles 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.

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 :
 - 📍 Vérifiez l'exactitude de l'adresse des URL des portails d'authentification que vous utilisez régulièrement, <https://cas.univ-tours.fr> pour celui de l'université,
 - 📍 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 ;
- ⊕ 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...).

Leçon n°5

Conserver les doux SOUVENIRS

Effectuer des sauvegardes
régulières

Choisir une solution adaptée

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

Pour sauvegarder vos données professionnelles, vous devez utiliser les services de sauvegarde proposés par le service informatique de l'Université (solution de sauvegarde des données sur les serveurs de fichiers, solution de sauvegarde des postes sensibles).

Pour sauvegarder vos données personnelles, vous pouvez 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.

Prendre les dispositions nécessaires

Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques : confidentialité des données ; incertitude sur la localisation des données ; disponibilité et intégrité des données ; irréversibilité des contrats.

Soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services.

Veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées, en les chiffrant à l'aide d'un logiciel de chiffrement avant de les copier dans le « cloud ».

Plus d'informations dans le guide sur l'externalisation et la sécurité des systèmes d'information réalisé par l'ANSSI*.

Leçon n°6

Rester
TENDANCE

Mettre à jour régulièrement
vos logiciels



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.

Le service informatique est chargé de la mise à jour du système d'exploitation et des logiciels sur les appareils appartenant à l'Université.

Sur vos appareils personnels, il vous appartient de faire cette démarche.

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

Leçon n°7

Garder au chaud ses PÉRIPHÉRIQUES

Être prudent avec son
smartphone et sa tablette

Bien que proposant des services innovants, les 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, ou autres). 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 pré-enregistrez pas vos mots de passe.



Leçon n°8

Ne pas se laisser

PLUMER

Être vigilant lors d'un
paiement sur Internet

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre smartphone, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur ou dans les fichiers clients du site marchand. 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://* apparaît 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 de votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

Leçon n°9

Sortir
COUVERT

Utiliser un antivirus et
un pare-feu



Vous devez vous assurer qu'un logiciel antivirus est installé sur votre ordinateur et qu'il est activé et actualisé. Si un virus est détecté, demandez l'aide du service informatique.

À la maison, utilisez un logiciel antivirus comprenant une fonction de mise à jour automatique des définitions de virus. Configurez votre logiciel afin qu'il analyse automatiquement, à intervalles réguliers, tous les fichiers enregistrés sur votre ordinateur.

Il est indispensable de protéger le poste de travail par un pare-feu qui filtrera les tentatives d'accès illicites depuis Internet.



Leçon n°10

Partir à L'AVENTURE

Se méfier des clés usb et
autres matériels amovibles



Les supports amovibles (disques, clé USB, etc.) sont des médias à utiliser avec prudence.

Ils ne doivent être utilisés que pour transférer les données et non pas comme un moyen de stockage permanent, car le risque de perdre les données est important.

Ces médias sont sujets plus que les autres à :

- ⊕ Des risques de perte, de vol, etc. ;
- ⊕ Une détérioration plus rapide que des matériels professionnels ;

Il ne faut pas les utiliser pour stocker des informations sensibles :

- ⊖ Sujets ou notes d'examens, données privées, dossiers de carrière ;
- ⊖ Mots de passe, codes bancaires, etc.

Si la clé USB est utilisée pour transporter des données sensibles, il est indispensable de chiffrer son contenu.

Désactivez l'exécution automatique des clés USB sur votre ordinateur.

L'emploi d'ordinateurs portables, de 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.



Leçon n°11


Revenir dans les jupons
DU SITE-MÈRE

Télécharger ses programmes sur
les sites officiels des éditeurs



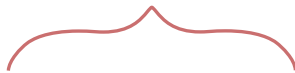

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour qui, le plus souvent, contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes 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...


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 réfléchissez 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.



Glossaire

- 
- i Antivirus** : logiciel informatique destiné à identifier, à neutraliser et à effacer des logiciels malveillants.
 - i Cheval de Troie** : programme qui s'installe de façon frauduleuse pour remplir une tâche hostile, à l'insu de l'utilisateur (espionnage, envoi massif de spams...).
 - i Chiffrement** : procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.
 - i Logiciel espion** : logiciel malveillant qui s'installe dans un ordinateur afin de collecter et de transférer des données et des informations, souvent à l'insu de l'utilisateur.
 - i Mise à jour** : action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel.
 - i Pare-feu (firewall)** : logiciel et/ou matériel permettant de protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet, protection d'un réseau d'entreprise, etc.) en filtrant les entrées et en contrôlant les sorties selon les règles définies par son utilisateur.
 - i Phishing (hameçonnage)** : méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
 - i Système d'exploitation** : logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels.
- 



En cas d'incident

Ne cédez pas à la panique, et ayez les bons réflexes:

- ✓ En cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation...);
- ✓ Déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez-la sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque;
- ✓ Prévenez votre informaticien de proximité, par téléphone ou de vive voix, car l'intrus peut-être capable de lire les courriels. Ils prendront en compte l'incident et remonteront l'alerte au niveau des Responsables Sécurité des Systèmes d'Information (RSSI) de l'université.

Pour aller plus loin

- ⊕ ANSSI : www.ssi.gouv.fr
- ⊕ CNIL : www.cnil.fr
- ⊕ Délégation à l'intelligence économique (D2IE) : www.intelligence-economique.gouv.fr
- ⊕ Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Police nationale) : www.internet-signalement.fr



université
de TOURS

© Université de Tours - 51D'com - G. Parnot - nov. 2017 / Illustrations : Fotolia et unsplash

Sécurité des
systèmes d'information

 ssi.univ-tours.fr
 rssi@univ-tours.fr