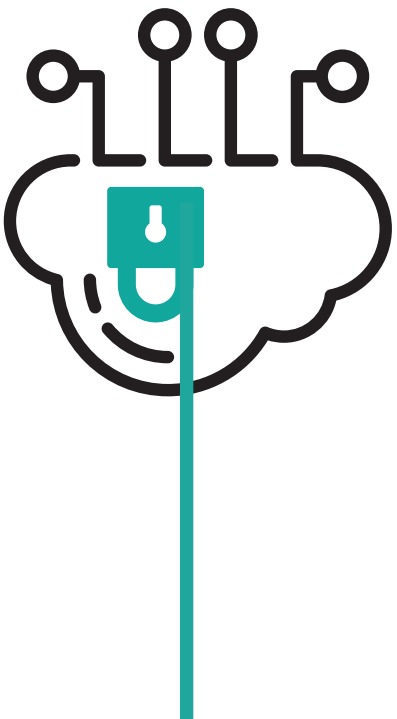
LES 10 COMMANDEMENTS DE LA CYBERSÉCURITÉ

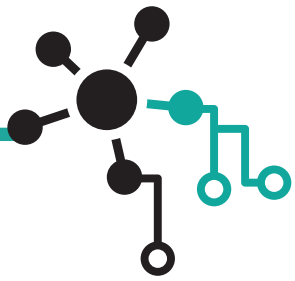
POUR PROFITER DU NUMÉRIQUE EN TOUTE SÉCURITÉ



.nordnet.
nos solutions Internet vous ouvrent le monde

SOMMAIRE

ÉDITO



A l'heure de l'hyper-connexion et du développement des cyberattaques, près d'un français sur deux souhaiterait être mieux informé des risques liés à Internet et des bonnes pratiques à appliquer pour s'en prémunir (source : étude IFOP/ Nordnet 2017 « Les français face à la protection de leurs smartphones »).

Ce guide pratique de la cybersécurité vise à la fois à vous sensibiliser aux menaces qui pèsent sur votre vie numérique et à démystifier ces menaces.

En effet, les cyber-risques se multiplient essentiellement parce que nous les sous-estimons et les méconnaissons. Il s'agit pourtant bien souvent de risques qui existent dans le monde réel et que nous avons appris à maîtriser. Par exemple, on évite de se confier à n'importe qui ou de laisser la porte de sa maison ouverte !

Se protéger des cyber-menaces nécessite de développer quelques réflexes et de s'équiper des bons outils. Vous trouverez dans ce guide nos conseils et bonnes pratiques pour utiliser vos appareils connectés en toute tranquillité.

Une check-list cybersécurité est disponible à la fin de ce guide pour vous rappeler les bonnes pratiques à adopter pour bien vous protéger.

1 PROTÉGER SES APPAREILS CONTRE LES VIRUS

Le virus informatique ressemble trait pour trait à son cousin, le virus biologique. Il est invisible, infectieux et contagieux ! C'est devenu le nom générique donné à toute sorte de logiciels malveillants :

- Le « cheval de Troie » a l'air inoffensif, alors qu'en réalité il introduit un virus dans l'ordinateur.
- Le « logiciel espion », comme son nom l'indique, espionne et transmet des informations sur votre activité.
- La « bombe logique » est programmée pour devenir active à un moment précis et perturber ou empêcher le fonctionnement normal de l'ordinateur.
- Le ransomware (rançongiciel en français) chiffre les données de votre disque dur et vous promet un déchiffrement en échange d'une rançon. Généralement, une somme est exigée, cependant des rançons d'un nouveau genre apparaissent : elles ne demandent pas d'argent mais des photos de vous dans le plus simple appareil !

source : MalwareHunterTeam

COMMENT ATTRAPE-T-ON UN VIRUS ?

En le laissant s'introduire dans son ordinateur, sa tablette ou son smartphone, autrement dit par sa connexion à Internet en Wi-Fi ou filaire, ou par un appareil que l'on branche (un lecteur de DVD, une clé USB…). Le programme malveillant peut être caché dans une pièce jointe, dans un fichier téléchargé ou sur un site Internet. Il s'active quand l'utilisateur ouvre la pièce jointe ou clique sur l'adresse.

QUELS SONT LES DANGERS LIÉS AUX VIRUS ?

Tous les virus sont nocifs, mais certains plus que d'autres. Les premiers virus qui sont apparus avaient vocation à se propager rapidement pour contaminer le plus grand nombre d'ordinateurs. Les dégâts qu'ils causaient étaient relativement limités. Puis les virus sont devenus plus dangereux : ils volent l'identité et les données de l'utilisateur, exploitent son ordinateur à son insu, surveillent son activité, enregistrent ce qu'il tape sur son clavier ou ce qu'il copie sur une clé USB.

COMMENT SE PROTÈGE-T-ON D'UN VIRUS ?

Les logiciels antivirus protègent les appareils en surveillant ce qui y entre, en détectant les logiciels malveillants et en les détruisant. Ils détectent les nouveaux virus dès qu'ils apparaissent – et il en apparaît des milliers chaque jour. Ils enregistrent leur « signature » dans leurs bases de données qu'ils partagent avec tous leurs utilisateurs, pour éviter que votre smartphone, votre tablette ou votre ordinateur n'attrape une mauvaise maladie ! Or, selon une étude Ifop/Nordnet, seuls 45% des français possèdent un antivirus sur leurs smartphones… Pour protéger vos données, il est désormais primordial d'installer un antivirus sur tous vos appareils connectés à Internet. Ils sont tous exposés aux mêmes risques.

CONSEIL Installez une suite de sécurité sur tous vos appareils connectés à Internet. Par exemple, Nordnet propose Securitoo Intégral et avec un seul abonnement, vous pouvez sécuriser jusqu'à 5 appareils (PC, Mac, et mobiles sous Android™) avec des modules de protection adaptés à chacun.

2 NE PAS MORDRE À L'HAMEÇON

Qui n'a jamais reçu un e-mail avec le logo de sa banque ou de son opérateur mobile lui demandant de vérifier ses coordonnées ou de payer une facture en attente ? Ces messages sont souvent frauduleux. Ce sont des e-mails de « hameçonnage », traduction de l'anglais « phishing ». Ils vous invitent à vous connecter sur un site et à saisir des informations confidentielles comme votre numéro de carte bancaire et votre mot de passe, par exemple. À l'aide de ces informations, les fraudeurs peuvent alors procéder à des achats avec votre carte bancaire ou retirer de l'argent sur votre compte en banque. Ils peuvent aussi revendre ces informations à d'autres pirates.

COMMENT REPÉRER UN PHISHING ? L'OBSERVATION AVANT TOUT :

Les meilleures protections contre le phishing restent… le bon sens et l'observation ! Les e-mails de hameçonnage comportent généralement des fautes d'orthographe, le logo de l'émetteur ressemble vaguement à celui qu'on a l'habitude de voir... Ces e-mails n'affichent pas les coordonnées de l'établissement ou les habituelles « petites notes en bas de page ». Leur présentation est généralement peu soignée mais certains sont parfois extrêmement ressemblants, vous obligeant à redoubler de vigilance. Souvent, il s'agit de banques ou d'opérateurs dont vous n'êtes même pas client. Dans ce cas, supprimez simplement le message.

LES BONS REFLEXES À ADOPTER POUR NE PAS MORDRE À L'HAMEÇON !

Si vous êtes bien client de l'établissement qui envoie le message, procédez à une première vérification simple, celle de l'adresse de l'émetteur. En cliquant dessus, elle s'affichera en entier. Si elle ne mentionne pas le nom de la banque ou de l'opérateur et que le suffixe « .fr » est remplacé par un couple de lettres que vous ne reconnaissez pas, méfiez-vous. De la même façon, vous pouvez vérifier l'adresse de réponse. En règle générale, il vaut mieux se connecter au site de son opérateur Internet, de son fournisseur d'énergie ou de sa banque en tapant l'adresse directement dans un navigateur et éviter de cliquer sur un lien dans un e-mail dont on se méfie. Aucun organisme ne vous demandera d'envoyer des informations personnelles par e-mail.

LES FAKE NEWS, QU'EST CE QUE C'EST ?

Le phishing peut aussi se cacher derrière de fausses informations, photos ou vidéos, appelées communément « fake news » qui se multiplient sur Internet, notamment via les réseaux sociaux. Les fake news n'ont qu'un seul but, délivrer en masse de mauvaises informations et manipuler le lectorat, ce qui peut être un réel danger pour la démocratie. En 2017 en France, les fake news se sont par exemple multipliées durant la campagne présidentielle. Comment, face à cet océan de données, repérer les informations qui ont été manipulées ? Si ce n'est pas toujours évident, il existe des astuces pour identifier les intox : regardez quelle est la source de l'actualité, est-ce un site parodique ? Un site de divertissement ? Un site d'info ? N'hésitez pas à aller sur la section « en savoir plus » ou « à propos » du site. C'est souvent là qu'est précisée la nature du site. Demandez-vous aussi qui parle ou diffuse le message : est-ce une source officielle (gouvernement, police, gendarmerie, pompiers…) ? Il est désormais possible de signaler sur Facebook les publications qui semblent être des "fake news". Des médias partenaires sont alors chargés de vérifier l'information.

CONSEIL

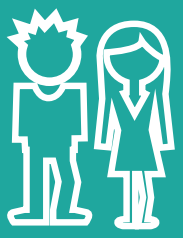
Signalez le phishing à l'entreprise qui en est victime pour qu'elle puisse le faire bloquer et ainsi limiter les dégâts pour les autres utilisateurs ! Par exemple, si vous recevez un e-mail qui vous semble provenir de Nordnet mais qu'il ne vous parait pas tout à fait clair, transférez-le à : abuse@nordnet.com.

3 PRÉSERVER SA VIE PRIVÉE

Ils font partie de notre quotidien ! Quels que soient notre âge, notre métier ou notre lieu d'habitation, nous utilisons quasiment tous des réseaux sociaux. Et nous y partageons beaucoup d'informations avec nos amis ou nos relations professionnelles. Nous n'hésitons pas à y mettre les photos des dernières vacances, celles de la maison que l'on vient de rénover ou celle du billet d'avion pour dire que l'on part – enfin ! – en vacances…

Autant d'informations qui n'intéressent pas que vos « amis ». Dire que vous partez en vacances quelques semaines après avoir « posté » la photo du tout nouveau home cinéma que vous venez d'acheter peut attirer bien des convoitises. Sur les réseaux sociaux, vos informations ne sont pas aussi protégées que celles que vous communiquez à l'administration ou à votre entreprise. Pour les pirates, c'est l'endroit rêvé pour trouver, voler et détourner des données d'identité. Savez-vous par exemple que le code barre qui figure sur un billet d'avion comporte des informations sur vous, votre destination, le moyen de paiement que vous avez utilisé, le repas que vous avez commandé, votre fréquence de voyage… ? De quoi réfléchir à deux fois avant de poster sur Facebook la photo de son billet pour les Baléares !

LES ADOS : PREMIÈRE CIBLE VIA LES RÉSEAUX SOCIAUX



Sur l'écran de leur smartphone, ils pensent être dans un environnement aussi protégé que celui de leur chambre. Il n'en est rien. Lorsqu'un nouvel « ami », même inconnu, apparait dans la liste de leurs contacts, ils sont souvent ravis d'engager la conversation. Il leur arrive de confier des informations sur eux-mêmes et sur les autres parce qu'ils ne pensent pas à remettre en question l'identité de ce nouvel ami et font confiance à sa photo de profil, sans imaginer que ce dernier se fait peut-être passer pour quelqu'un d'autre… Pour éviter les situations dramatiques, n'hésitez pas à engager le dialogue avec votre ado au sujet de son utilisation des réseaux sociaux afin de vérifier que les précautions de base sont bien respectées.

COMMENT SE PROTÉGER DES DANGERS LIÉS AUX RÉSEAUX SOCIAUX ?

Pour éviter le vol de données, le détournement d'identité ou le harcèlement, les réseaux sociaux demandent un minimum de prudence. Comme dans n'importe quel espace numérique, il ne faut pas communiquer d'informations trop personnelles, ni d'identifiants et surtout pas de mots de passe ! Ne cédez pas aux promesses trop belles pour être vraies, comme des jeux en ligne qui proposent des gains mirobolants en échange de quelques informations.

CONSEIL

Vérifiez la véracité des messages, des appels aux dons ou des propositions curieuses que vous recevez via les réseaux sociaux en consultant un site anti-canular comme, par exemple, www.hoaxbuster.com.

4 CHOISIR UN BON MOT DE PASSE

Chaque site Internet, chaque application, et presque tous les appareils électroniques de notre quotidien sont désormais accessibles à l'aide d'un identifiant et d'un mot de passe. L'identifiant est généralement le nom et le prénom de l'utilisateur, un surnom ou un mot en relation avec le site. C'est l'équivalent, dans le monde numérique, du numéro et du nom de la rue dans une adresse. Mais le mot de passe, lui, est l'équivalent de la clé qui ouvre la porte de la maison à cette adresse. Et si votre adresse postale ne permet pas à un voleur de rentrer chez vous, votre mot de passe lui ouvre les portes de vos comptes en banque, de vos informations personnelles, de vos comptes client sur les sites d'achat, de vos données médicales, d'assurance, etc.

LE CASSE-TÊTE DES MOTS DE PASSE

41% des utilisateurs de smartphones avouent avoir stocké des mots de passe sur leur mobile *(Source : étude IFOP/Nordnet 2017 « Les français face à la protection de leurs smartphones »).*

En cause, l'obligation de créer des mots de passe différents d'un site à l'autre, qui comportent au moins 12 caractères avec des lettres, des chiffres, des signes de ponctuation et des symboles…Dur de se souvenir de tout cela ! C'est pourquoi nous les notons sur un papier dans le tiroir à côté de l'ordinateur ou sur les notes du smartphone et continuons donc de créer des mots de passe faciles à mémoriser, donc faciles à trouver pour les pirates.

Les mots de passe les plus fréquemment utilisés en France sont les suites de chiffres de 1 à 8 ou 8 fois le même chiffre, les suites de lettres dans l'ordre du clavier (azertyuiop), les mots football, password (mot de passe en anglais)… Bref, des mots de passe que les pirates en quête de facilité parviennent à casser en moins d'une seconde avec leurs outils.

COMMENT CRÉER UN BON MOT DE PASSE ET LE MÉMORISER FACILEMENT ?

Il existe différentes techniques pour créer des mots de passe compliqués mais dont on peut se souvenir. Le site de la CNIL (https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe) les explique et donne des exemples. La méthode la plus accessible consiste à choisir une phrase, une citation, le titre de votre morceau de musique ou de votre livre préféré. Vous prenez la première lettre de chaque mot, vous remplacez le i par un point d'exclamation ou le S majuscule par le chiffre 5, vous rajoutez un / ou un – pour séparer le titre du roman du nom de l'auteur, etc. Vous composez ainsi un mot de passe complexe, qui vous est propre et que vous pouvez mémoriser.

Et si même cela vous rebute, il existe des gestionnaires de mots de passe qui génèrent, enregistrent et mémorisent des mots de passe complexes et différents pour chaque site. Vous ne devrez créer et mémoriser qu'un seul mot de passe pour y accéder. Facile !

CONSEIL

Un bon mot de passe comporte des lettres, des chiffres et des signes de ponctuation. Exemple : !jMsc2Bh. Pour vous en souvenir facilement, prenez la première lettre de chaque mot d'une phrase dont vous vous rappellerez toute votre vie. Par exemple : « Harry Potter et l'enfant maudit 2016 » devient « HPelem2016 ».

5 CRYPTER SES DONNÉES

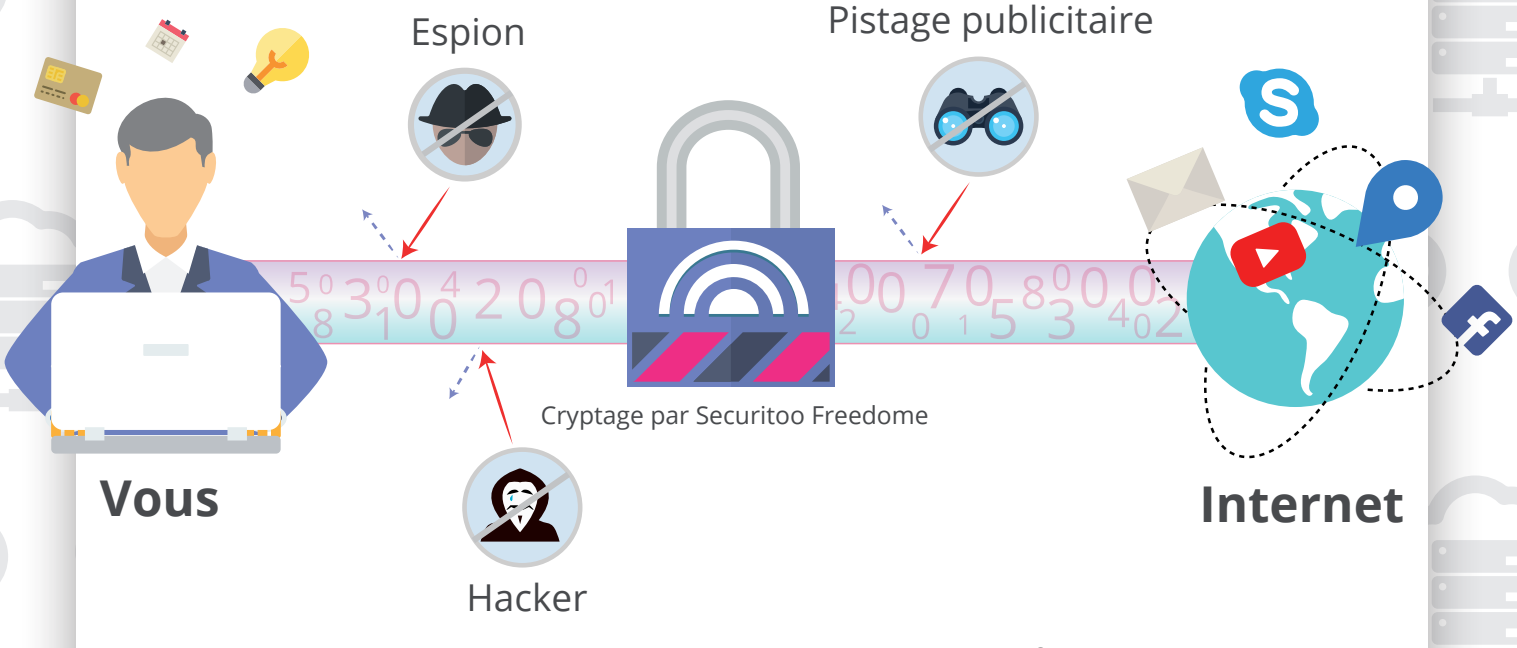
Vous avez sûrement déjà entendu parler de chiffrement ou de cryptage. Il s'agit de techniques informatiques utilisées pour qu'un message ne soit lisible que par son destinataire, qui dispose de la « clé de déchiffrement ». C'est ainsi que les militaires communiquent afin que leurs ennemis ne puissent pas capter les messages qu'ils s'échangent. C'est la même méthode que l'on utilise pour les VPN : Virtual Private Network alias réseau privé virtuel.

UN VPN, COMMENT ÇA MARCHE ?

C'est un logiciel que l'on installe sur son ordinateur, son smartphone ou sa tablette. Il crée un tuyau opaque entre votre appareil et les services Internet auxquels il accède, il encode votre message, vos données, vos fichiers afin que personne ne puisse les lire.

Quand vous vous connectez à Internet en Wi-Fi dans un lieu public ou lorsque vous utilisez votre carte de crédit pour payer un achat en ligne sur votre smartphone, le VPN empêche ainsi que vos données soient captées et lues par un espion. Non seulement, votre communication est protégée de toute intrusion, mais les sites ne peuvent pas vous suivre, vous tracer, et les sites malveillants sont bloqués.

Utiliser un VPN, c'est un peu comme circuler sur l'autoroute dans un fourgon blindé sur une voie qui vous est réservée. Autrement dit, en toute sécurité !



Fonctionnement du VPN Securitoo Freedome de Nordnet

6 SÉCURISER SA CONNEXION

C'est tellement pratique de pouvoir se connecter depuis la gare lorsque l'on attend son train, dans le hall de l'hôtel pour dire qu'on est bien arrivé ou dans un bar le soir pour donner l'adresse aux copains. Oui mais voilà, se connecter à Internet sur un réseau public pour surfer sur les réseaux sociaux ou pour lire ses e-mails présente quelques risques.

Pour pouvoir s'y connecter, on accepte les conditions d'utilisation, les fameuses CGU, sans les lire. Dommage, car elles autorisent parfois le fournisseur à récupérer votre adresse de connexion ou même à regarder ce que contiennent vos messages…

Mais ce n'est pas le plus grave. Pour se connecter depuis un café, par exemple, on saisit son identifiant et son mot de passe, et là c'est plus risqué. N'importe quel pirate bien équipé peut « lire » le flux à distance et s'emparer de vos identifiants. Il pourra alors détourner votre profil sur les réseaux sociaux ou accéder à votre compte en banque.

Et lorsque les utilisateurs connaissent les risques, ils ne sont pourtant pas prêts à changer leurs habitudes. Ils sont pourtant réels : sur les réseaux publics, il existe plusieurs façons de vous pirater, la plus courante étant l'attaque du « man in the middle » consistant à intercepter le trafic entrant et sortant de votre appareil pour voler vos identifiants de connexion ou de vos informations bancaires par exemple. Mais il existe d'autres méthodes d'attaques et des solutions pour s'en protéger.

COMMENT PROTÉGER VOS DONNÉES SUR LES RÉSEAUX WI-FI PUBLICS ?

La première précaution à prendre en toutes situations est de protéger vos appareils avec un antivirus firewall (pare-feu) et plus seulement un simple anti-virus qui vous protège uniquement des attaques virales. L'anti-virus firewall détecte lorsque qu'un intrus tente d'accéder au contenu de votre ordinateur et lui bloque totalement l'accès à vos fichiers. Vous êtes alerté en temps réel.

LES BONS RÉFLEXES

- Apprenez à repérer un réseau public qui n'est pas protégé : si aucune authentification ne vous est demandée, le réseau est ouvert à tous et facilement piratable.
- Vérifiez la présence du « https » et de l'icône du petit cadenas dans l'adresse des sites que vous consultez si vous comptez y réaliser des achats. Le certificat SSL vous indique que le site est sécurisé.
- Utilisez un VPN : cela permet de chiffrer toutes les données qui transitent, et leur déchiffrement est assez laborieux pour décourager la plupart des hackers.
- Désactivez la connexion automatique aux réseaux Wi-Fi sur chacun de vos appareils.

7 UTILISER UN CONTRÔLE PARENTAL

Quel que soit leur âge, les enfants utilisent des appareils numériques, tablettes, smartphones ou ordinateurs, de plus en plus souvent. Les plus jeunes jouent et regardent des dessins animés sur Internet. Les pré-ados surfent de site en site et téléchargent des jeux, de la musique ou des vidéos. Quant aux adolescents, en plus de télécharger, ils passent des heures sur les réseaux sociaux, soucieux de rester connectés en permanence à leurs amis. Mais Internet n'est pas sans risques et cela peut inquiéter les parents. Ils veulent que toute la famille puisse surfer sereinement, sans tomber de manière inopinée sur des images violentes ou pornographiques, sans être victime de harcèlement, de vol d'identité…

QUELLE EST LA MEILLEURE PROTECTION SUR INTERNET EN FONCTION DE L'ÂGE ET DES USAGES DES ENFANTS?

Les logiciels de contrôle parental permettent de définir des profils en fonction de l'âge de l'enfant et des choix d'éducation des parents. Ces outils bloquent l'accès à des sites (liste noire) ou n'autorisent l'accès qu'à une liste de sites précis (liste blanche). Certains permettent de définir des plages horaires pendant lesquelles l'enfant peut aller sur Internet.

Mais ce ne sont là que des outils. Les listes ne sont pas toujours exhaustives et les enfants ont de l'imagination dès lors qu'il s'agit de contourner une règle trop contraignante. C'est pourquoi **la mise en place d'une solution de contrôle parental doit se faire avec l'enfant.** Il faut lui expliquer pourquoi il ne peut pas accéder à tout, voir avec lui de temps en temps les sites qu'il consulte et surtout, lui montrer qu'on lui fait confiance !

8 SAUVEGARDER SES DONNÉES

Vous enregistrez surement une multitude de fichiers auxquels vous tenez sur vos appareils connectés : photos de vacances, musique, les premiers pas du petit dernier, les numéros de téléphone de tout vos contacts, les rendez-vous et leur adresse… Et plus encore pour ceux qui utilisent aussi leur ordinateur ou leur téléphone le soir ou le weekend pour des raisons professionnelles.

Si on vous vole cet appareil, s'il tombe en panne ou qu'un violent orage provoque une coupure électrique pendant qu'il est en charge, vous êtes totalement désemparé. Adieu les photos des dernières vacances, les coordonnées personnelles ou professionnelles, le film que vous veniez tout juste de télécharger, ou même au revoir au dossier que vous aviez rapporté chez vous pour y mettre votre dernière touche.

UNE SOLUTION SIMPLE ET EFFICACE POUR CONSERVER SES DONNÉES : LA SAUVEGARDE (= LE BACKUP)

Régulièrement, il faut prendre le temps de copier ses données sur un support externe (disque dur, clé USB) ou dans le Cloud, c'est-à-dire sur un serveur à distance chez son opérateur. Un smartphone peut être synchronisé régulièrement sur un ordinateur ou dans le Cloud. Si un jour l'appareil est endommagé, les données, elles au moins, existent ailleurs et seront faciles à retrouver et à recopier.

CAS PARTICULIER : QUE FAIRE EN CAS DE VOL DE MATÉRIEL ?

Les smartphones et les tablettes coûtent cher. Certains coûtent même plus cher qu'un ordinateur. Ce qui attire inévitablement la convoitise. Lorsque vous perdez ou vous faites voler un appareil, vous vous sentez bien souvent totalement démuni ! D'autant plus si vous ne disposez d'aucune sauvegarde de vos données personnelles, voire professionnelles.

Pas de panique ! Il faut tout d'abord verrouiller son appareil avec un mot de passe compliqué. Evitez « 1234 » ou « 0000 » que les voleurs essaieront en premier. Pensez à copier quelque part le numéro d'identification, le numéro IMEI, qui apparaît en clair dans les Réglages. Cela pourra contribuer à bloquer l'appareil ou le retrouver s'il est volé.

Il existe des solutions de sécurité qui rendent l'appareil inutilisable par les voleurs et localisable à distance. Il suffit de prévenir son opérateur ou son fournisseur d'accès pour qu'il bloque immédiatement le smartphone, qu'il en efface tout le contenu à distance et qu'il le localise grâce au GPS. Si votre téléphone dispose d'une caméra avant, il est même possible de photographier le voleur !

Et si vous avez sauvegardé votre contenu dans le Cloud, vous pourrez le réinstaller immédiatement sur un nouvel appareil.

ASTUCE

Programmez dans votre calendrier une alerte une fois par mois, pour faire une sauvegarde de vos données sur une clé USB ou un disque externe, et créez ainsi une sorte d'automatisme pour enregistrer les données de l'ordinateur.

9 EFFACER SES TRACES

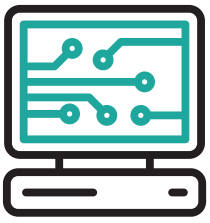
Qu'il soit sur votre smartphone, sur votre tablette ou votre ordinateur, votre historique est précieux. De nombreux historiques existent sans que vous en soyez bien informés, voici ceux que nous vous conseillons de bien contrôler.

VOS APPAREILS ENREGISTRENT TOUT

Le plus connu de tous est l'historique de votre navigateur. Lorsque vous naviguez sur un site web, de nombreuses informations sont conservées comme l'historique des pages visitées et des fichiers téléchargés, mots de passe, champs de formulaire… Certaines informations peuvent être étudiées par des sites web tiers qui vous proposent alors un contenu personnalisé. La géolocalisation de votre smartphone est également passée au crible ! À moins d'avoir pris ses précautions, par défaut, votre appareil peut vous pister ponctuellement. Il récupère votre localisation à intervalles réguliers et en profite pour l'ajouter à votre historique personnel. Enfin, si vous êtes connecté à un compte YouTube / Google l'historique des vidéos que vous avez regardées est lui aussi enregistré par défaut. Vous pouvez désactiver cette fonction par souci de confidentialité ou pour éviter que quelqu'un ne tombe par hasard sur cet historique.

BON À SAVOIR

Vous avez sûrement déjà entendu parler des « cookies informatiques » ? Il s'agit de petits fichiers déposés sur votre appareil par le site internet ou l'application que vous consultez. Ils sont inoffensifs mais enregistrent l'essentiel de votre activité en ligne. Pensez-donc à les effacer régulièrement. Et si vous ne savez pas comment faire, il suffit de taper sur votre moteur de recherche « comment effacer les cookies ? »



ATTENTION À VOTRE SESSION UTILISATEUR !

Que ce soit votre boîte e-mails, votre profil Facebook ou LinkedIn, votre compte Amazon… désormais la plupart de vos sessions sont enregistrées sur tous vos appareils : ordinateur, tablette, smartphone et même sur votre montre connectée ! Si vous fermez un onglet, cela ne veut pas dire pour autant que vous êtes déconnecté. La personne qui utilisera l'appareil après vous pourra tout à fait se retrouver sur votre profil Facebook par exemple.

Pour la sécurité de vos données, il est donc important de contrôler quels sont les appareils et applications qui ont accès à vos comptes. Imaginez un peu la catastrophe si votre compte était piraté et qu'on avait accès à vos données personnelles ou à vos coordonnées bancaires… Pour éviter les mésaventures, il suffit de vous déconnecter systématiquement de votre session utilisateur quand vous quittez un appareil.

ASTUCE

Pensez à ouvrir une nouvelle fenêtre ou un nouvel onglet « navigation privée » quand vous utilisez un appareil qui n'est pas le vôtre.

10 RESPECTER CES BONNES PRATIQUES !

Vous l'avez compris en feuilletant ce guide, le monde numérique n'est ni plus sûr ni plus dangereux que le monde réel. Tout y est affaire de bon sens. Si vous ne les protégez pas, les informations et les données que vous mettez dans votre appareil peuvent être lues, copiées et même revendues par des tiers mal intentionnés. Vous ne laissez pas les clés dans votre voiture ou sur votre porte. De la même façon, apprenez les gestes qui protègent votre vie numérique.

Créez-vous un ou plusieurs mot(s) de passe difficile(s) à deviner.

Gardez secrets vos identifiants et vos mots de passe.

Installez une suite de sécurité (au minimum un antivirus + un firewall).

Soyez conscients que les réseaux sociaux sont comme la « place du village », ce que vous y dites ou postez peut être lu et vu par tous ceux qui passent !

Expliquez à vos enfants que les risques sont les mêmes sur Internet que dans le monde réel, apprenez-leur à se poser les bonnes questions avant de poster des images sur leur réseau social.

Eteignez votre appareil si vous ne vous en servez pas pendant plusieurs heures, la nuit par exemple et effacez son historique régulièrement.

Faites régulièrement une copie de vos données.

Méfiez-vous des fausses informations qui circulent sur les réseaux sociaux. Vérifiez toujours l'origine de l'article.

CONTACTEZ-NOUS AU

3420

OU RENDEZ-VOUS SUR

WWW.NORDNET.COM

NOS GUIDES SONT DISPONIBLES EN TÉLÉCHARGEMENT SUR NOTRE SITE
WWW.NORDENT.COM/GUIDES

nordnet

nos solutions Internet vous ouvrent le monde