Sensibilisation à la CyberSécurité

SOMMAIRE

1

Les mots de passe

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe.

Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple.

Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès.

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

Question ouverte

Qu’est ce qu’un bon mot de passe ?

TOP 20

Des pires mots de passe en 2019

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123
- abc123
- qwerty123
- 1q2w3e4r
- admin
- qwertyuiop
- 654321
- 555555
- lovely
- 7777777
- welcome

UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe.

Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde.

Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux. (personnellement, je préconise 20 signes minimum au vu des dernières techniques utilisées)

Estimated Password Recovery Times — 1x Terahash Brutalis, 44x Terahash Inmanis (448x Nvidia RTX 2080)

Full US keyboard mask attack with Terahash Hashstack

	Speed	Length 4	Length 5	Length 6	Length 7	Length 8	Length 9	Length 10	Length 11	Length 12	Length 13
NTLM	31.82 TH/s	Instant	Instant	Instant	Instant	3 mins 29 secs	5 hrs 30 mins	3 wks 0 day	5 yrs 7 mos	538 yrs 1 mo	51.2 mil
MD5	17.77 TH/s	Instant	Instant	Instant	Instant	6 mins 14 secs	9 hrs 50 mins	1 mo 1 wk	10 yrs 1 mo	963 yrs 4 mos	91.6 mil
NetNTLMv1 / NetNTLMv1+ESS	16.82 TH/s	Instant	Instant	Instant	Instant	6 mins 35 secs	10 hrs 24 mins	1 mo 1 wk	10 yrs 8 mos	1 mil	96.8 mil
LM	15.81 TH/s	Instant	Instant	Instant	Instant						
SHA1	5.89 TH/s	Instant	Instant	Instant	Instant	18 mins 47 secs	1 day 5 hrs	3 mos 3 wks	30 yrs 7 mos	2.9 mil	276.3 mil
SHA2-256	2.42 TH/s	Instant	Instant	Instant	Instant	45 mins 39 secs	3 days 0 hr	9 mos 1 wk	74 yrs 4 mos	7.1 mil	671.9 mil
NetNTLMv2	1.22 TH/s	Instant	Instant	Instant	Instant	1 hr 30 mins	5 days 23 hrs	1 yr 6 mos	147 yrs 10 mos	14.1 mil	1335.5 mil
SHA2-512	801.9 GH/s	Instant	Instant	Instant	1 min 28 secs	2 hrs 17 mins	1 wk 2 days	2 yrs 4 mos	224 yrs 9 mos	21.4 mil	2029.7 mil
descrypt, DES (Unix), Traditional DES	647.59 GH/s	Instant	Instant	Instant	1 min 48 secs	2 hrs 50 mins	1 wk 4 days	2 yrs 11 mos	278 yrs 3 mos	26.5 mil	2513.3 mil
Kerberos 5, etype 23, TGS-REP	206.97 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	870 yrs 10 mos	82.8 mil	7864 mil
Kerberos 5, etype 23, AS-REQ Pre-Auth	206.78 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	871 yrs 8 mos	82.9 mil	7871.2 mil
md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)	7.61 GH/s	Instant	Instant	1 min 37 secs	2 hrs 33 mins	1 wk 3 days	2 yrs 7 mos	249 yrs 5 mos	23.7 mil	2252.6 mil	213995.1 mil
LastPass + LastPass sniffed	1.78 GH/s	Instant	Instant	6 mins 52 secs	10 hrs 52 mins	1 mo 1 wk	11 yrs 2 mos	1.1 mil	101.1 mil	9600.8 mil	912079.6 mil
macOS v10.8+ (PBKDF2-SHA512)	335.09 MH/s	Instant	Instant	36 mins 34 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 7 mos	5.7 mil	538.2 mil	51127.7 mil	4857134 mil
WPA-EAPOL-PBKDF2	277.23 MH/s					9 mos 0 wk	72 yrs 0 mo	6.8 mil	650.5 mil	61799.3 mil	5870931.8 mil
TrueCrypt RIPEMD160 + XTS 512 bit	211.78 MH/s	Instant	Instant	57 mins 52 secs	3 days 19 hrs	11 mos 3 wks	94 yrs 3 mos	9 mil	851.6 mil	80899.5 mil	7685455.6 mil
7-Zip	181.51 MH/s	Instant	Instant	1 hr 7 mins	4 days 10 hrs	1 yr 1 mo	110 yrs 0 mo	10.5 mil	993.6 mil	94389.2 mil	8966975.1 mil
sha512crypt 6, SHA512 (Unix)	119.46 MH/s	Instant	1 min 5 secs	1 hr 42 mins	6 days 18 hrs	1 yr 9 mos	167 yrs 2 mos	15.9 mil	1509.7 mil	143419.6 mil	13624861.4 mil
DPAPI masterkey file v1	47.23 MH/s	Instant	2 mins 44 secs	4 hrs 19 mins	2 wks 3 days	4 yrs 5 mos	422 yrs 10 mos	40.2 mil	3818.1 mil	362723.1 mil	34458696.1 mil
RAR5	28.15 MH/s	Instant	4 mins 35 secs	7 hrs 15 mins	4 wks 0 day	7 yrs 5 mos	709 yrs 7 mos	67.4 mil	6407.6 mil	608720.6 mil	57828453.9 mil
DPAPI masterkey file v2	27.82 MH/s	Instant	4 mins 39 secs	7 hrs 20 mins	4 wks 1 day	7 yrs 6 mos	717 yrs 10 mos	68.2 mil	6482.1 mil	615797.6 mil	58500769.5 mil
RAR3-hp	20.84 MH/s	Instant	6 mins 12 secs	9 hrs 47 mins	1 mo 1 wk	10 yrs 1 mo	958 yrs 2 mos	91.1 mil	8652.3 mil	821972.3 mil	78087367.8 mil
KeePass 1 (AES/Twofish) and KeePass 2 (AES)	17.6 MH/s	Instant	7 mins 15 secs	11 hrs 28 mins	1 mo 2 wks	11 yrs 9 mos	1.1 mil	106.7 mil	10131.9 mil	962529.5 mil	91440305.8 mil
bcrypt $2*$, Blowfish (Unix)	11.37 MH/s	Instant	11 mins 21 secs	17 hrs 57 mins	2 mos 1 wk	18 yrs 5 mos	1.8 mil	167 mil	15860.3 mil	1506727.9 mil	143139150.9 mil
Bitcoin/Litecoin wallet.dat	3.55 MH/s	Instant	36 mins 18 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 1 mo	5.6 mil	534.1 mil	50743.7 mil	4820655.6 mil	457962282.7 mil

UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe.

Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré.

Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

EXEMPLE

CRÉER UN MOT DE PASSE SOLIDE

LA MÉTHODE DES PREMIÈRES LETTRES

Un tiens vaut mieux que deux tu l'auras

1tvmQ2tl'A

LA MÉTHODE PHONÉTIQUE

J'ai acheté huit CD pour cent euros cet après-midi

ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement.

Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès.

Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès.

EXEMPLE

KEEPASS

UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre est en français, certifié (et c'est le seul) par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

https://keepass.info

CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater.

N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

NE COMMUNIQUEZ JAMAIS VOTRE MOT DE PASSE À UN TIERS

Votre mot de passe doit rester secret.

Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone.

Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

N’UTILISEZ PAS VOS MOTS DE PASSE SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel.

Si vous êtes obligé d’utiliser un ordinateur partagé ou qui n’est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d’éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n’enregistrez jamais vos mots de passe dans le navigateur.

Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l’ordinateur partagé.

ACTIVEZ LA « DOUBLE AUTHENTIFICATION »
LORSQUE C'EST POSSIBLE

Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option.

En plus de votre nom de compte et de votre mot de passe, ces services vous demandent un code provisoire que vous pouvez recevoir, par exemple, par SMS sur votre téléphone mobile ou qui peut être généré par une application ou une clé spécifique que vous contrôlez.

Ainsi grâce à ce code, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés.

EXEMPLE

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook, Gmail, Yahoo Mail…
- Facebook, Instagram, LinkedIn, Twitter…
- Skype, WhatsApp…
- Amazon, eBay, Paypal…
- Apple iCloud, Dropbox,
- Google Drive, OneDrive…

CHANGEZ LES MOTS DE PASSE PAR DÉFAUT DES DIFFÉRENTS SERVICES AUXQUELS VOUS ACCÉDEZ

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer.

Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

CHOISISSEZ UN MOT DE PASSE PARTICULIÈREMENT ROBUSTE POUR VOTRE MESSAGERIE

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes.

Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.

Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger.

2

Les réseaux sociaux

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles.

Aujourd'hui installés dans les usages personnels des internautes, mais aussi dans les usages professionnels des entreprises qui les utilisent comme vitrine de leur activité, ils n'échappent pas aux activités malveillantes.

Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux.

Voici 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux.

Question ouverte

Qu’elles sont les réseaux sociaux que vous utilisés ?

PROTÉGEZ L'ACCÈS À VOS COMPTES

Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels.

Pour vous assurer que personne ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l'accès à votre compte en utilisant des mots de passe différents et suffisamment robustes.

Si le service le propose, activez également la double authentification.

VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email...) et de vos publications sont souvent très ouverts. Vos données peuvent ainsi être partagées à tous les abonnés du réseau social.

Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités.

Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

MAÎTRISEZ VOS PUBLICATIONS

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser.

Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez.

Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire.

Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise.

Enfin, respectez évidemment la loi.

INFORMATION

RESPECTEZ LA LOI

Internet n’est pas une zone de non-droit et l’anonymat n’y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l’atteinte au droit à l’image ou au droit d’auteur… sont punis par la loi.

En vertu de la loi n°2018-493 du 20 juin 2018 – Article 20, un mineur peut consentir seul à un traitement de ses données à caractère personnel à partir de quinze ans. Avant cet âge, le consentement du titulaire de l'autorité parentale est requis.

CONTRÔLEZ LES APPLICATIONS TIERCES

Certaines applications proposent d'interagir avec votre compte de réseau social.

Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte.

Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés…

Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus.

Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas.

Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS

Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel.

Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte.

Évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre.

Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous.

VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE

La plupart des réseaux sociaux offrent des fonctionnalités qui vous permettent de voir les connexions ou sessions actives sur votre compte depuis les différents appareils que vous utilisez pour y accéder.

Consultez régulièrement ces informations.

Si vous détectez une session ou une connexion inconnue ou que vous n'utilisez plus, déconnectez là.

Au moindre doute, considérez qu'il peut s'agir d'un piratage et changez immédiatement votre mot de passe.

FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES

Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification.

Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément.

Avec la puissance des réseaux sociaux, ces fausses informations (appelées « fake news » en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes. Aussi, avant de considérer ou relayer une information, efforcez-vous d'en vérifier la véracité.

UTILISEZ EN CONSCIENCE L'AUTHENTIFICATION AVEC VOTRE COMPTE DE RÉSEAU SOCIAL SUR D'AUTRES SITES

Pour s'y connecter, certains sites Internet vous proposent d'utiliser votre compte de réseau social.

Cette fonctionnalité peut sembler pratique car elle évite de créer un compte et un mot de passe supplémentaires, mais cela signifie que vous allez communiquer au réseau social des informations sur ce que vous faites sur le site concerné, et à l'inverse que vous allez peut-être donner au site des droits d'accès sur votre compte de réseau social.

De plus, si votre compte de réseau social était un jour piraté, le cybercriminel pourrait automatiquement accéder à tous ces sites en usurpant votre identité.

Aussi, avant d'utiliser cette fonctionnalité, ayez bien conscience des risques et vérifiez attentivement les autorisations que vous délivrez.

SUPPRIMEZ VOTRE COMPTE SI VOUS NE L'UTILISEZ PLUS

Pour éviter que vos informations ne soient récupérées par des tiers ou que votre compte ne soit utilisé à votre insu, notamment pour usurper votre identité, supprimez-le si vous ne l'utilisez plus.

INFORMATION

QUE FAIRE EN CAS DE PROBLÈME ?

- Réagir en cas de piratage de votre compte de réseau social – Les conseils de la CNIL :

www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux

- Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux – Les conseils de la CNIL :

www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer

- Signaler une situation de cyber harcèlement : contacter Net Écoute gratuitement au 0800200000 et sur www.netecoute.fr

- Signaler un contenu illicite sur les réseaux sociaux – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr

3

Les appareils mobiles

Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel.

Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs.

Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler.

Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles.

METTEZ EN PLACE LES CODES D'ACCÈS

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations.

Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple).

Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

INFORMATION

CODE D'ACCÈS ET CODE PIN

DEUX PROTECTIONS COMPLÉMENTAIRES

Mot de passe, signe, combinaison de touches ou biométrie : le code de verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas.

Composé de 4 chiffres, le code PIN bloque quant à lui l'accès à votre carte SIM et empêche donc de pouvoir s'en servir dans un autre appareil si on ne le connaît pas.

CHIFFREZ LES DONNÉES DE L'APPAREIL

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations.

Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation.

Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ

Qu’il s’agisse du système d’exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu’elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

FAITES DES SAUVEGARDES

Votre appareil mobile contient généralement des informations que vous n’avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos…

Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)…

Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau.

Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

N’INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées.

Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu’ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées.

Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d’installer une nouvelle application.

Au moindre doute, n’installez pas l’application et choisissez-en une autre.

CONTRÔLEZ LES AUTORISATIONS DE VOS APPLICATIONS

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer.

Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ».

Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect.

Au moindre doute, n'installez pas l'application et choisissez-en une autre.

NE LAISSEZ PAS VOTRE APPAREIL SANS SURVEILLANCE

Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil.

Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

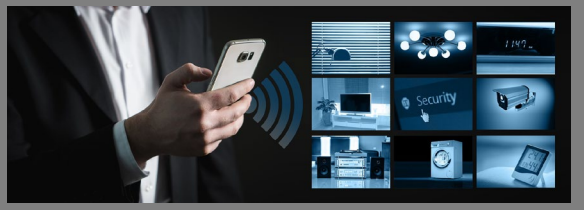
ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux.

D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil.

De plus, elles épuisent votre batterie inutilement.

Dans ce cas préféré un point d'accès WIFI avec votre portable en faisant attention à vos données internet (attention à votre forfait)



NE STOCKEZ PAS D'INFORMATIONS CONFIDENTIELLES SANS PROTECTION

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile.

Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer.

En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle.

Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

INFORMATION

CONSERVEZ LE CODE IMEI

DE VOTRE APPAREIL MOBILE

Composé de 15 à 17 chiffres, le code IMEI est le numéro de série de votre appareil mobile.

Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.

Notez le soigneusement et si vous l'avez égaré vous pouvez le récupérer en tapant *#06# sur votre clavier.

4

LES SAUVEGARDES

Dans nos usages personnels ou professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de vos données.

Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme.

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos sauvegardes.

EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES DE VOS DONNÉES

En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports.

Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.).

Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.

IDENTIFIEZ LES APPAREILS ET SUPPORTS QUI CONTIENNENT DES DONNÉES

Dans notre vie quotidienne, nous utilisons un nombre croissant d'appareils et de supports qui enregistrent et stockent nos fichiers et nos données : ordinateurs, serveurs, tablettes, téléphones mobiles (smartphone), disques durs, clés USB, etc.

Prenez le temps de les identifier.

DÉTERMINEZ QUELLES DONNÉES DOIVENT ÊTRE SAUVEGARDÉES

Il n’est pas toujours possible ni nécessaire de sauvegarder la totalité de ses données. Sélectionnez donc les données à protéger, notamment celles qui sont stockées sur vos appareils (dans le disque dur de votre ordinateur ou dans la mémoire de votre téléphone mobile).

Pour savoir si des données doivent être sauvegardées ou non, posez-vous les questions suivantes :

- quelles données ne peuvent pas être récupérées par ailleurs en cas de perte ?
- quelles données je consulte régulièrement ou celles qui me sont le plus souvent demandées ?

CHOISISSEZ UNE SOLUTION DE SAUVEGARDE ADAPTÉE À VOS BESOINS

Il existe des solutions gratuites ou payantes qui répondent à différents besoins.

Identifiez-les et déterminez quelles sont les fonctionnalités attendues, l'espace de stockage requis et la facilité d'utilisation de la solution.

Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe, une clé USB, etc.

Enfin, la plupart des systèmes d'exploitation proposent des fonctionnalités de sauvegarde sur le support de votre choix ou sur un service en ligne.

Si vous avez des besoins particuliers, renseignez-vous auprès de professionnels ou de sites Internet spécialisés.

PLANIFIEZ VOS SAUVEGARDES

Lorsqu'un fichier régulièrement mis à jour est perdu ou supprimé par erreur, sa restauration dans sa version la plus récente est nécessaire.

La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière.

Vérifiez qu'elle est bien activée et que la fréquence de vos sauvegardes est adaptée à vos besoins.

Si vous n'utilisez pas de solution dédiée, réalisez des sauvegardes manuelles régulièrement.

DÉCONNECTEZ VOTRE SUPPORT DE SAUVEGARDE APRÈS UTILISATION

Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait les détruire.

Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique ou mettez-le hors ligne lorsque vous ne l'utilisez plus.

PROTÉGEZ VOS SAUVEGARDES

Les risques de perte, de vol, de panne, de piratage ou de destruction peuvent également affecter vos sauvegardes.

Protégez-les au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports.

Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre.

Si vous estimez que vos données sont suffisamment sensibles pour les chiffrer ou en limiter l'accès, ou si un règlement vous y oblige, faites-en de même avec vos sauvegardes.

TESTEZ VOS SAUVEGARDES

Parfois, le processus de sauvegarde ne s’effectue pas correctement.

Aussi, assurez-vous régulièrement que votre sauvegarde fonctionne, par exemple, en la copiant dans le système original.

VÉRIFIEZ LE SUPPORT DE SAUVEGARDE

Tout comme les supports qui permettent de stocker les données originales, les supports sur lesquels sont réalisées les sauvegardes peuvent être endommagés.

Vérifiez leur état, de manière à prévenir toute défaillance ou panne.

Soyez également vigilant sur la durée de vie de votre support car certains conservent les données sur une durée plus ou moins longue.

Par exemple, la durée de vie moyenne d'un DVD gravé est de 10 à 15 ans.

SAUVEGARDEZ LES LOGICIELS INDISPENSABLES À L'EXPLOITATION DE VOS DONNÉES

La défaillance d'un appareil entraîne non seulement la perte des données produites par son utilisateur mais également du système d'exploitation de l'appareil comme MS Windows, iOS, Android, et des logiciels qui y sont installés.

Si les données sauvegardées sont dépendantes d'un système d'exploitation, d'un logiciel ou d'une configuration particulière, sauvegardez vos données ainsi que celles nécessaires à leur exploitation.

Les systèmes d'exploitation récents proposent des fonctionnalités de sauvegarde du système qui permettent de le restaurer.

Reportez-vous à sa documentation pour plus d'information.

LEGISLATION

Professionnels, associations, collectivités : tenez compte du cadre juridique applicable

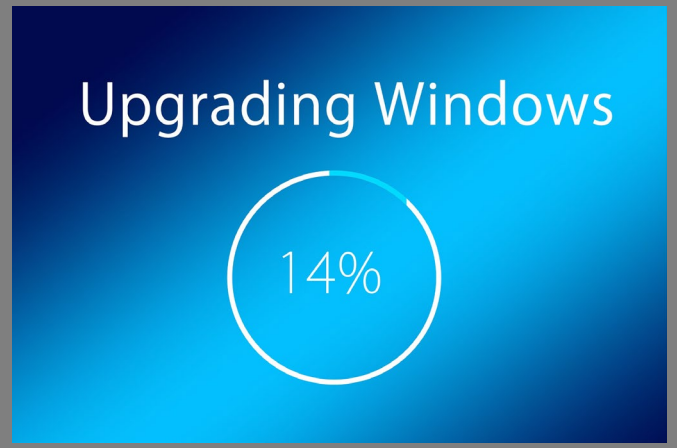
Quelle que que soit leur nature, vos sauvegardes sont soumises à de nombreux régimes juridiques au même titre que vos données originales.

S'agissant de données personnelles, votre responsabilité civile ou pénale peut être engagée en cas de manquement avéré.

De même, le Règlement Général sur la Protection des Données (RGPD) et la Loi Informatique et Libertés sont applicables.

Quelques textes :

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Article 34 (Modifié par Loi n°2004-801 du 6 août 2004)
- Article 226-17 du Code Pénal (relatif au traitement et à la protection des données personnelles)
- Article 1242 du Code Civil (relatif à la responsabilité civile liée à un dommage causé à autrui)



5

Les mises à jour

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité.

Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'une montre connectée ou d'un équipement mobile.

Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (*patch* en anglais) visant à corriger ces failles.

Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger.

Voici 10 bonnes pratiques à adopter pour vos mises à jour.

PENSEZ À METTRE À JOUR SANS TARDER L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés... nous utilisons un grand nombre d'appareils et de logiciels.

Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique.

Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jours que vous allez installer ne sont pas infectées par un virus.

A l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou **cases précochées** qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

IDENTIFIEZ L'ENSEMBLE DES APPAREILS ET LOGICIELS UTILISÉS

Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour.

Certains fournisseurs d'accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique.

Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabriquant ou des éditeurs des applications installées.

ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE DES MISES À JOUR

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement.

Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur.

Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

INFORMATION

DIFFÉRENTS TYPES DE MISES À JOUR

- Les mises à jour importantes ou critiques corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.

- Les mises à jour de version apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

DÉFINISSEZ LES RÈGLES DE RÉALISATION DES MISES À JOUR

Pour assurer votre sécurité numérique, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise.

Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

PLANIFIEZ LES MISES À JOUR LORS DE PÉRIODES D'INACTIVITÉ

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte.

En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas.

Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit…).

MÉFIEZ-VOUS DES FAUSSES MISES À JOUR SUR INTERNET

En navigant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran :

fausses publicités sur des sites Internet ou fenêtres (*pop-up* en anglais) malveillantes.

Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

EXEMPLE

Arnaques aux fausses mises à jour

Un exemple d'arnaque aux fausses mises à jour est l'enquête faite par Micode « youtuber » :

Chapitre 1 : https://www.youtube.com/watch?v=gbYdQOde6EU

Chapitre 2 : https://www.youtube.com/watch?v=0M4k-j-8LXY

Chapitre 3 : https://www.youtube.com/watch?v=5vCdM4RvoiQ

INFORMEZ-VOUS SUR LA PUBLICATION RÉGULIÈRE DES MISES À JOUR DE L'ÉDITEUR

L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques.

Si les mises à jour ne sont plus proposées, ils sont plus vulnérables.

Aussi, avant l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication régulière des mises à jour de l'éditeur ou du fabricant, ainsi que la date de fin de leur mise à disposition.

Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils afin de rester protégé.

TESTEZ LES MISES À JOUR
LORSQUE CELA EST POSSIBLE ET FAITES DES SAUVEGARDES

Il arrive que la mise à jour d'un équipement ou d'un logiciel entraîne des conséquences inattendues, comme de rendre incompatible la solution qui vient d'être mise à jour avec un autre équipement ou logiciel.

Il convient donc de tester les mises à jour lorsque cela est possible.

Par ailleurs, n'hésitez pas à réaliser une sauvegarde de vos données et de vos logiciels avant une opération de mise à jour pour pouvoir revenir en arrière si nécessaire.

PROTÉGEZ AUTREMENT LES APPAREILS QUI NE PEUVENT PAS ÊTRE MIS À JOUR

Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément.

Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

BON À SAVOIR

Mises à jour et sauvegardes

En entreprise, s'il existe un service informatique, il est généralement chargé de la mise à jour des appareils et des logiciels.

Dans le cas contraire, ce sont les collaborateurs qui effectuent cette opération, sous l'autorité du chef d'entreprise.

6

Les usages pro-perso

La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien.

Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel :

la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse.

Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre entreprise ou votre organisation, que votre espace de vie privée.

Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.

UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR TOUS LES SERVICES PROFESSIONNELS ET PERSONNELS AUXQUELS VOUS ACCÉDEZ

Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux…).

Si vous utilisez ce même mot de passe pour accéder au système informatique de votre entreprise, c'est elle que vous mettez aussi en péril, car un cybercriminel pourrait utiliser vos identifiants de connexion pour voler ou détruire des informations.

NE MÉLANGEZ PAS VOTRE MESSAGERIE PROFESSIONNELLE ET PERSONNELLE

Ce serait, en effet, le meilleur moyen de ne plus s'y retrouver et de commettre des erreurs, notamment des erreurs de destinataires.

Celles-ci pourraient avoir pour conséquences de voir des informations confidentielles de votre entreprise vous échapper vers des contacts personnels qui pourraient en faire un mauvais usage, ou à l'inverse de voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaiteriez pas.

Enfin, comme votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle, vous faire pirater votre compte pourrait mettre en danger votre entreprise si un cybercriminel accédait à des messages professionnels confidentiels que vous auriez gardés dans votre messagerie personnelle.

AYEZ UNE UTILISATION RESPONSABLE D'INTERNET AU TRAVAIL

Si l'utilisation d'une connexion Internet professionnelle à des fins personnelles est tolérée, il est important d'avoir à l'esprit que votre utilisation peut mettre en cause votre entreprise qui pourra se retourner contre vous si vous commettiez des actes répréhensibles comme du téléchargement illégal, de l'atteinte au droit d'auteur ou si vous publiez des propos qui pourraient être condamnables.

De plus, vous devez avoir à l'esprit que votre entreprise est en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition.

N'utilisez donc pas votre connexion professionnelle pour des choses qui n'ont, selon vous, pas à être connues de votre entreprise.

MAÎTRISEZ VOS PROPOS SUR LES RÉSEAUX SOCIAUX

Quand vous parlez de votre travail ou de la vie de votre entreprise (ambiance, nouveaux projets…) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas vos lecteurs :

la rediffusion ou l'interprétation qu'ils peuvent faire de vos informations pourraient nuire à votre entreprise.

À l'inverse, et pour les mêmes raisons, vous n'avez pas forcément envie que certains propos que vous pouvez tenir sur les réseaux sociaux et qui concernent votre vie privée puissent être connus de votre entreprise.

Sur les réseaux sociaux, verrouillez votre profil pour que tout ne soit pas public et avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice, ou à votre entreprise, si d'aventure vos propos ou messages étaient relayés par une personne malintentionnée.

N’UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES

Ou du moins pas sans l'autorisation de votre employeur et sans avoir pris les mesures de sécurité qui s’imposent.

Ces services de stockage en ligne d’informations (Cloud en anglais) généralement gratuits pour les particuliers sont certes pratiques, mais d’un niveau de sécurité qui ne se prête pas forcément aux exigences des entreprises pour protéger leurs informations.

Ils ne sont pas conçus pour cela. Pour les besoins des entreprises, il existe des solutions professionnelles et sécurisées.

L’utilisation d’un service de stockage en ligne personnel pour des usages professionnels pourrait mettre en danger votre entreprise si votre compte d’accès à ce service était piraté alors qu’il contenait des informations confidentielles.

FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, il est important d'installer sans tarder les mises à jour dès qu'elles sont publiées.

Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations ou à celles de votre entreprise.

UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, utilisez une solution antivirus et tenez-la à jour.

Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques que peuvent subir vos équipements comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)…

Si un cybercriminel prenait le contrôle de vos équipements personnels, il pourrait accéder à toutes vos informations, mais aussi au réseau de votre entreprise si vous vous y connectez avec ce matériel.

N’INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Que ce soit pour vos usages personnels ou professionnels si cela relève de votre responsabilité, et même s’ils ne sont pas infaillibles, seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées par un virus qui permettrait à un cybercriminel de prendre le contrôle de votre équipement.

Méfiez-vous des sites « parallèles » qui ne contrôlent pas les applications qu’ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées.

Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d’installer une nouvelle application.

Au moindre doute, ne l’installez pas et choisissez-en une autre.

MÉFIEZ-VOUS DES SUPPORTS USB

Vous trouvez ou on vous offre une clé USB (ou tout autre support à connecter).

Partez du principe qu'elle est piégée et que même les plus grands spécialistes pourraient avoir du mal à s'en apercevoir.

Ne la branchez jamais sur vos moyens informatiques personnels et encore moins sur vos moyens informatiques professionnels au risque de les compromettre en ouvrant un accès à un cybercriminel.

Utilisez une clé USB pour vos usages personnels et une autre pour vos usages professionnels afin d'éviter que la compromission de l'une ne puisse infecter l'autre.

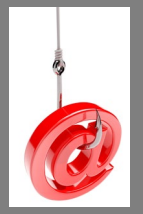
ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et ainsi récupérer au passage vos comptes d'accès et vos mots de passe personnels ou professionnels, vos messages, vos documents ou même vos données de carte bancaire… afin d'en faire un usage délictueux.

Depuis un réseau Wi-Fi public ou inconnu, n'échangez jamais d'informations confidentielles.

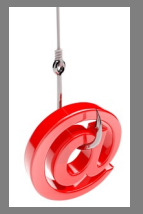
7

Phishing ou l’hameçonnage



L’hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l’internaute pour l’inciter à communiquer des données personnelles (comptes d’accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

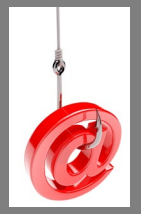
Il peut s’agir d’un faux message, SMS ou appel téléphonique de banque, de réseau social, d’opérateur de téléphonie, de fournisseur d’énergie, de site de commerce en ligne, d'administrations, etc.



BUT RECHERCHÉ

VOLER DES INFORMATIONS PERSONNELLES OU PROFESSIONNELLES

(comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.



SI VOUS ÊTES VICTIME

Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier et déposez plainte au commissariat de police ou à la gendarmerie la plus proche.

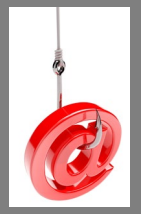
Si vous avez constaté que des éléments personnels servent à usurper votre identité, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie la plus proche.

Si vous êtes victime d'une usurpation de votre adresse de messagerie ou de tout autre compte, **CHANGEZ IMMÉDIATEMENT VOS MOTS DE PASSE**.

Si vous avez reçu un message douteux sans y répondre, **SIGNALEZ-LE À SIGNAL SPAM** (https://www.signal-spam.fr/).

Vous pouvez également **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE** (https://phishing-initiative.fr/contrib/) qui en fera fermer l'accès.

Pour être conseillé en cas d'hameçonnage, contactez INFO ESCROQUERIES **AU 0 805 805 817** (numéro gratuit).



MESURES PRÉVENTIVES

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

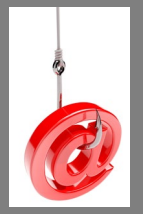
Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Utilisez des mots de passes différents et complexes pour chaque site et application afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

Si le site vous le permet, **activez la double authentification pour sécuriser vos accès.**



LES INFRACTIONS

• Escroquerie (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

•Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal) : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.

•Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal) : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

•Contrefaçon et usage frauduleux de moyen de paiement (articles L163-3 et L163-4 du code monétaire et financier) : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.

• Usurpation d'identité (article 226-4-1 du code pénal) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

•Contrefaçon des marques (logos, signes, emblèmes…) utilisées lors de l'hameçonnage, prévu par les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle. Délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.

8

Ransomware ou les rançongiciels

Un rançongiciel (*ransomware* en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système.

Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

BUT RECHERCHÉ

EXTORQUER DE L'ARGENT à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues.

Certaines attaques visent juste à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

SI VOUS ÊTES VICTIME

DÉBRANCHEZ LA MACHINE D'INTERNET ou du réseau informatique.

En entreprise, **ALERTEZ IMMÉDIATEMENT VOTRE SERVICE INFORMATIQUE.**

NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

DÉPOSEZ PLAINTE auprès de la police ou de la gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites-vous, au besoin, assister par un avocat spécialisé.

IDENTIFIEZ LA SOURCE DE L'INFECTION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT, lorsqu'elle existe. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez le poste et réinstallez un système sain puis restaurez les copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur https://www.cybermalveillance.gouv.fr/ des prestataires spécialisés susceptibles de pouvoir vous apporter leur assistance.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés (notre fiche dédiée aux mots de passe sur www.cybermalveillance.gouv.fr).

Éteignez votre machine lorsque vous ne vous en servez pas.

LES INFRACTIONS

• De tels procédés relèvent de l'extorsion de fonds et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende* ».

• L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra aussi être retenue (article 323-1 du code pénal) soit du fait d'une modification frauduleuse de données soit d'une entrave au bon fonctionnement d'un STAD. La loi du 24 juillet 2015 relative au renseignement a doublé les peines d'amende encourues de 75 000 euros à 150 000 euros.

Par ailleurs, depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines.

Dans le cadre des atteintes aux STAD, la circonstance aggravante de bande organisée est très souvent retenue. En effet, la commission de ces infractions requiert en principe la mise en oeuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, injection du virus, expédition du mail infecté, collecte de la rançon.

9

Faux support technique

L’arnaque au faux support technique (Tech support scam en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l’apparition d’un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l’usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles.

Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ

SOUTIRER DE L'ARGENT à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

SI VOUS ÊTES VICTIME

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL.** Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRUS approfondie de votre machine.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE, ET CHANGEZ TOUS VOS MOTS DE PASSE.** En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre équipement par vous-même, vous pouvez faire appel à un prestataire référencé sur https://www.cybermalveillance.gouv.fr/.

Si vous avez fourni vos coordonnées bancaires ou n° de carte de crédit, **FAITES OPPOSITION** sans délai. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

Si vous avez été contacté par un faux support technique, **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR** sur sa plateforme https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites vous, au besoin, assister par un avocat spécialisé.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.

Tenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu mais dont la structure du message est inhabituelle ou vide.

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.

Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

LES INFRACTIONS

• L'incrimination principale qui peut être retenue est l'escroquerie. L'article 313-1 du code pénal dispose que : « *l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge* ». L'escroquerie est passible de cinq ans d'emprisonnement et de 375 000 euros d'amende.

• Si la victime est menacée de suppression de ses fichiers ou en est victime, de tels procédés relèvent de l'extorsion de fonds. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou la destruction de fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende.

• L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra également être retenue. Les articles 323-1 à 323-7 du code pénal disposent que : « *le fait d'accéder ou de se maintenir frauduleusement* » *dans un STAD, « la suppression ou la modification de données contenues dans le système* », ou l'« *altération du fonctionnement de ce système* » sont passibles de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.

10

CHANTAGE À L'ORDINATEUR OU À LA WEBCAM PRÉTENDUMENT PIRATÉS

Le chantage à l'ordinateur ou à la webcam prétendus piratés (ou « **cryptoporno** ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés.

Il prend généralement la forme d'un message reçu, essentiellement par courriel (mail), de la part d'un inconnu qui se présente comme un pirate informatique.

Ce « hacker » prétend avoir pris le contrôle de l'ordinateur de la victime suite à la consultation d'un site pornographique et annonce avoir obtenu des vidéos compromettantes avec sa webcam.

Le cybercriminel menace de les publier aux contacts (personnels et/ ou professionnels) de la victime si elle ne lui paie pas une rançon, souvent réclamée en monnaie virtuelle (généralement en Bitcoin).

Parfois, pour attester de la prise de contrôle de l'ordinateur auprès de la victime, les cybercriminels vont jusqu'à lui écrire avec sa propre adresse mail ou lui dévoiler l'un de ses mots de passe.

BUT RECHERCHÉ

Soutirer de l'argent sous la menace de divulguer des vidéos compromettantes de la victime à ses contacts.

SI VOUS ÊTES VICTIME

NE PANIQUEZ PAS. En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

NE RÉPONDEZ PAS. Il ne faut jamais répondre à de telles menaces de chantage qui montrent aux cybercriminels que votre adresse de messagerie est « valide » et que vous portez de l'intérêt au message de chantage qu'ils vous ont envoyé.

NE PAYEZ PAS LA RANÇON. Et ce, même si vous aviez un doute. En effet, aucune mise à exécution des menaces n'a été démontrée jusqu'à présent et vous alimenteriez donc inutilement ce système criminel.

CONSERVEZ LES PREUVES. Faites des captures d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE partout où vous l'utilisez s'il a été divulgué ou au moindre doute et choisissez-en un solide.

CONTACTEZ VOTRE BANQUE si vous avez payé la rançon pour essayer de faire annuler la transaction.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la république du tribunal de grande instance dont vous dépendez.

MESURES PRÉVENTIVES

Faites régulièrement les mises à jour de sécurité de tous vos appareil.

Utilisez un antivirus et tenez-le à jour.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

Utilisez des mots de passe suffisamment complexes et **changez-les au moindre doute.**

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

Masquez votre webcam quand vous ne vous en servez pas (un simple morceau de ruban adhésif opaque sur l'objectif peut suffire).

LES INFRACTIONS

L'incrimination principale qui peut être retenue est **l'extorsion de fonds. L'article 312-1 du Code pénal** dispose que « l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ». L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.

11

LES FAUSSES OFFRES D'EMPLOI CRÉÉES PAR DES FRAUDEURS

Certaines offres d’emplois diffusées sur Internet n’amènent pas à de vrais recrutements. Elles sont en apparence identiques à de véritables offres, le plus souvent très attractives pour les candidats, et respectent les réglementations légales en matière de droit du travail (durée du travail, rémunération, etc.). Ces fausses offres sont créées par des fraudeurs qui se font passer pour de vrais recruteurs en usurpant le nom d’une entreprise, son adresse, l’identité d’un salarié ou d’un responsable de l’entreprise, ou son numéro de SIRET.

BUT RECHERCHÉ

SOUTIRER DE L'ARGENT OU DÉROBER DES INFORMATIONS PERSONNELLES (données bancaires, numéro de sécurité sociale) pour en faire un usage frauduleux.

SI VOUS ÊTES VICTIME

En cas de doute, **SIGNALEZ LES FAITS AU MINISTÈRE DE L'INTÉRIEUR sur sa plateforme** internet-signalement.gouv.fr

INTERROMPEZ IMMÉDIATEMENT TOUTE RELATION AVEC LE PSEUDO RECRUTEUR même si ce dernier se montre menaçant par message ou par téléphone.

Si vous avez transmis des données personnelles (numéro de sécurité sociale…), **INFORMEZ-EN L'ORGANISME CONCERNÉ** (Sécurité sociale, Pôle emploi, Caisse d'Assurance Maladie).

Si vous avez transmis des informations bancaires, **INFORMEZ-EN VOTRE BANQUE ET SURVEILLEZ RÉGULIÈREMENT LES OPÉRATIONS** sur votre compte bancaire.

INFORMEZ IMMÉDIATEMENT L'ORGANISME DONT L'IDENTITÉ A ÉTÉ USURPÉE OU LE SITE D'EMPLOI QUI A DIFFUSÉ L'ANNONCE avec, si possible, son numéro de référence.

Que vous soyez victime d'une tentative d'escroquerie, d'un vol de données personnelles ou d'une escroquerie financière, **DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie, ou en écrivant au procureur de la République dont vous dépendez. Ce dépôt de plainte vous aidera dans vos futures démarches en cas d'usurpation de votre identité. Il est possible de déposer une pré-plainte en ligne. Pour qu'elle soit enregistrée comme une plainte, vous devrez cependant signer cette déclaration auprès d'une unité de gendarmerie ou un service de police de votre choix.

MESURES PRÉVENTIVES

Méfiez-vous d'une offre trop attractive, voire hors norme. N'hésitez pas à en parler à votre entourage ou un professionnel de l'emploi (Pôle emploi...).

Méfiez-vous des annonces contenant des fautes d'orthographe ou qui demandent de répondre à une adresse de messagerie « publique ». Une grande entreprise vous adressera ainsi toujours un message émis depuis son nom de domaine (exemple : XX@pole-emploi.fr et non pas pole-emploi@XX.com).

Ne transmettez jamais à un recruteur vos données personnelles (RIB, numéro de sécurité sociale, de compte ou de carte bancaire) tant que vous ne l'avez pas rencontré.

Ne versez aucune somme d'argent à un employeur potentiel quel que soit le motif évoqué (contrat de travail potentiel ou suivi d'une formation préalable à l'embauche) et le mode de transfert (achat de cartes ou de coupons prépayés, virement express à l'international).

N'achetez jamais du matériel pour le compte de l'entreprise et n'acceptez jamais de recevoir un chèque ou un virement bancaire pour effectuer des achats nécessaires à votre prise de poste.

N'acceptez aucune rétribution de votre futur employeur tant que vous n'avez pas signé le contrat de travail.

Assurez-vous de l'existence juridique (SIRET) de l'entreprise à l'origine de l'offre d'emploi.

Soyez vigilant lorsqu'un recruteur vous contacte à un horaire atypique ou s'il ne peut vous rencontrer sous prétexte qu'il est à l'étranger.

Soyez attentif aux propos du recruteur en particulier lorsque par exemple, en cours d'entretien, il vous propose un poste différent de celui mentionné dans l'annonce.

Ne poursuivez pas la communication si vous doutez de l'honnêteté de votre interlocuteur.

Prenez le temps de lire avec attention tous les documents qui vous sont communiqués et n'apposez jamais votre signature sur un document sans savoir précisément ce à quoi vous vous engagez.

N'encaissez jamais de chèques qui ne seraient pas de votre employeur. Même si le montant d'un chèque déposé à votre banque apparaît en crédit sur votre compte, la banque, une fois les vérifications réalisées (chèque volé...), a plusieurs semaines pour valider l'opération ou l'annuler en débitant votre compte du même montant.

Tenez à jour votre antivirus et votre système d'exploitation.

LES INFRACTIONS

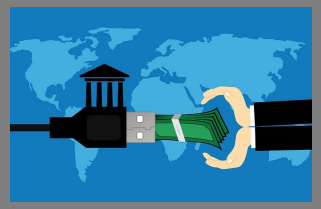
• **Escroquerie** (article 313-1 du code pénal) : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

• **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** (article 226-18 du code pénal) : le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

• **Usurpation d'identité** (article 226-4-1 du code pénal) : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

12

L'ESCROQUERIE AUX FAUX ORDRES DE VIREMENT (FOVI)



L’escroquerie aux faux ordres de virement (**FOVI**) désigne un type d’arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié.

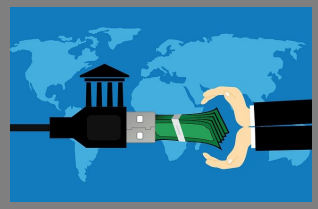
Parfois présenté comme émanant d’un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « **d’arnaque au Président** ».

Une variante consiste à usurper l’identité d’un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement.

Une autre variante consiste à usurper l’identité d’un salarié de l’organisation pour demander le changement des coordonnées bancaires où virer son salaire.

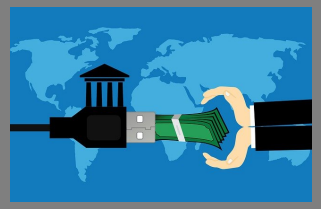
Le compte bancaire appartenant à l’escroc est souvent situé à l’étranger.

Cette catégorie d’escroquerie est généralement réalisée par téléphone et/ou par messages électroniques, voire les deux, et concerne tous les types d’organisation.



BUT RECHERCHÉ

Escroquerie financière en usurpant l'identité d'un dirigeant, d'un fournisseur ou d'un employé visant à faire verser de l'argent sur un compte bancaire détenu par les cybercriminels. Dans certains cas, cette fraude fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.



SI VOUS ÊTES VICTIME

IDENTIFIEZ LES VIREMENTS FRAUDULEUX. Identifiez tous les virements exécutés, en instance ou à venir à destination de l'escroc. Informez votre hiérarchie ainsi que le service comptable et demandez le blocage des coordonnées bancaires frauduleuses dans les applications métiers.

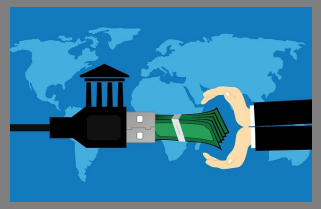
DEMANDEZ LA SUSPENSION DU VIREMENT. Si le virement n'est pas encore effectué, contactez immédiatement votre service comptable pour suspendre la demande de virement frauduleuse.

ALERTEZ IMMÉDIATEMENT VOTRE BANQUE ET DEMANDEZ LE RETOUR DES FONDS. Si le virement a été réalisé, contactez au plus vite votre banque pour demander le retour des fonds. Votre dépôt de plainte pourra être exigé de votre banque pour récupérer les sommes.

CONSERVEZ LES PREUVES et en particulier les numéros de téléphones, les messages reçus, les ordres de virement, les factures et toutes informations qui pourront vous servir pour signaler l'escroquerie aux autorités.

SI LA FRAUDE A PU ÊTRE PERMISE PAR LE PIRATAGE D'UN COMPTE DE MESSAGERIE, CHANGEZ IMMÉDIATEMENT SON MOT DE PASSE. Utilisez des mots de passe différents et complexes pour chaque site et application utilisés.

DÉPOSEZ PLAINTE. En parallèle des démarches auprès de votre banque, déposez plainte sans tarder au commissariat de police ou à la gendarmerie dont vous dépendez en fournissant toutes les preuves en votre possession.



MESURES PRÉVENTIVES

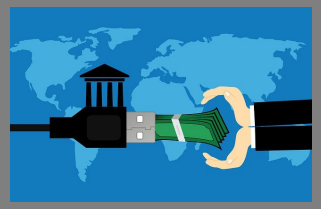
Sensibilisez vos collaborateurs et cadres aux risques notamment de réception de messages frauduleux d'hameçonnage (phishing) visant à leur dérober leurs mots de passe et en particulier si vos services de messagerie sont hébergés ou accessibles en externe.

Diffusez des procédures claires aux collaborateurs mandatés sur les règles d'authentification des émetteurs et de confirmation des demandes de virement imprévues ou de validation des changements de coordonnées bancaires.

Mettez en place une procédure de vérification et de validation hiérarchique interne non dérogeable des demandes de virement imprévues ou d'acceptation de changements de coordonnées bancaires.

Veillez à limiter la publication d'informations (site Internet, réseaux sociaux…) permettant d'identifier et de contacter vos collaborateurs habilités à réaliser des demandes de virement ou des modifications de coordonnées bancaires.

Généralisez l'utilisation de mots de passe solides pour les comptes de messagerie et activez la double authentification pour limiter les risques de piratage (tous nos conseils pour gérer vos mots de passe).



LES INFRACTIONS

• **Escroquerie (article 313-1 du code pénal).** L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (**article 313-3 du code pénal**).

• **Usurpation d'identité (article 226-4-1 du code pénal).** Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende. La tentative d'escroquerie est passible des mêmes peines (**article 225-5 du code pénal**).

• **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal).** Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. La tentative des délits prévus par les articles 323-1 à 323-3-1 est passible des mêmes peines.

13

LE PIRATAGE DE COMPTE

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne.

En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières : le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (phishing en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

BUT RECHERCHÉ

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS**. Si ce n'est pas le cas, changez-les immédiatement.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE et choisissez en un solide (voir notre fiche sur la gestion des mots de passe). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION**.

CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.

PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

MESURES PRÉVENTIVES

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Maintenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.

N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.

Évitez les sites non sûrs ou illicites, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.

Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.

Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics. Non maîtrisés, ils peuvent être contrôlés par un pirate.

Déconnectez-vous systématiquement de votre compte après utilisation pour éviter que quelqu'un puisse y accéder après vous.

LES INFRACTIONS

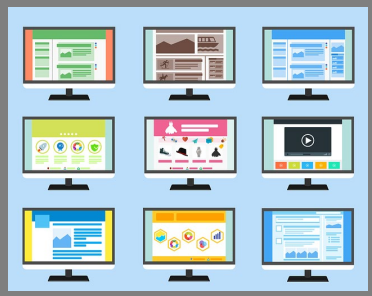
• **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal)** : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

Dans le cas d'un piratage d'un compte de messagerie :

• **Atteinte au secret des correspondances (article 226-15 du code pénal)** : délit passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende. Dans le cas de collecte de données à caractère personnel quel que soit le compte :

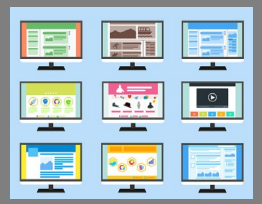
• **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Si le compte a été détourné pour usurper votre identité :

• **Usurpation d'identité par voie de télécommunication (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.



14

LA DÉFIGURATION DE SITE WEB



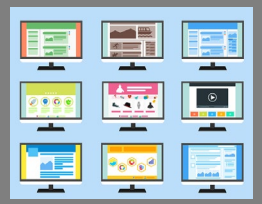
La défiguration est l'altération par un pirate de l'apparence d'un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ».

La défiguration est le signe visible qu'un site internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu.

Durant l'attaque, le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité.

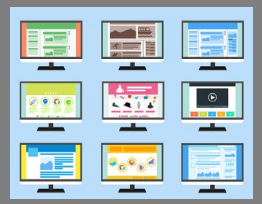
Par ailleurs, en étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales…) :

ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…



BUT RECHERCHÉ

DÉMONTRER UNE PRISE DE CONTRÔLE DU SITE ET LE FAIRE SAVOIR avec différents objectifs : la recherche de notoriété, la revendication politique ou idéologique, l'atteinte directe à l'image du site, et/ou le vol d'informations sensibles.



SI VOUS ÊTES VICTIME

Si possible, **DÉCONNECTEZ D'INTERNET** la machine concernée.

RÉCUPÉREZ LES FICHIERS DE JOURNALISATION (logs) de votre pare-feu, serveur mandataire (proxy) et des serveurs touchés qui seront des éléments d'investigation.

RÉALISEZ UNE COPIE COMPLÈTE DE LA MACHINE attaquée et de sa mémoire.

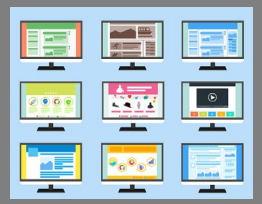
IDENTIFIEZ LES ÉLÉMENTS SENSIBLES qui ont pu être copiés ou détruits.

IDENTIFIEZ LE VECTEUR qui a permis de prendre le contrôle de la machine.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie dont vous dépendez et tenez à disposition des enquêteurs tous les éléments de preuves en votre possession.

Lorsque vous aurez repris le contrôle de la machine touchée, **CORRIGEZ TOUTES LES VULNÉRABILITÉS ET CHANGEZ TOUS LES MOTS DE PASSE** avant de la remettre en ligne.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur www.cybermalveillance.gouv.fr des prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.



MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système d'exploitation et des logiciels installés sur vos serveurs.

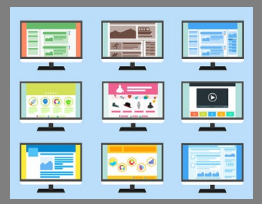
Ayez un pare-feu correctement paramétré : fermez tous les ports inutilisés et ne laissez que les adresses des machines indispensables accéder aux fonctionnalités d'administration du site.

Consultez régulièrement les fichiers de journalisations (logs) de votre pare-feu afin de détecter toute tentative d'intrusion, ainsi que les logs de vos serveurs exposés pour identifier les tests de mots de passe suspects en particulier.

Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement, mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés (fiche mots de passes sur www.cybermalveillance.gouv.fr).

Sensibilisez les utilisateurs à ne jamais communiquer d'éléments d'accès administrateurs et d'authentification à un tiers non identifié (ingénierie sociale, hameçonnage, etc.).

Ne conservez pas de manière accessible la liste nominative des personnes possédant les droits d'administrateur sur le serveur.



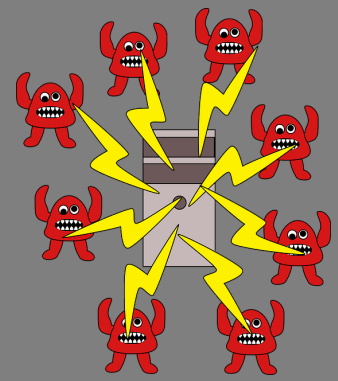
LES INFRACTIONS

L'incrimination principale qui peut être retenue ici est celle de **l'entrave à un système de traitement automatisé de données** (STAD ou système d'information).

Les **articles 323-1 à 323-7 du code pénal** disposent que :

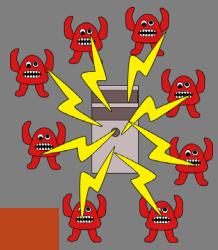
- « le fait d'accéder ou de se maintenir, frauduleusement » dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité).
- « le fait d'introduire frauduleusement des données » dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site. La défiguration désigne la modification non sollicitée de la présentation d'un site Web, à la suite d'un piratage du site.
- le fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données » d'un système de traitement automatisé de données. La copie frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement.
- « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ».
- les tentatives de ces infractions sont punies des mêmes peines.

En fonction du cas d'espèce, les peines encourues sont de deux ans à sept ans d'emprisonnement et de 60 000 euros à 300 000 euros d'amende.



15

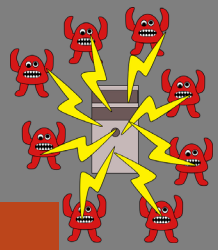
LE DÉNI DE SERVICE



Une attaque en déni de service ou en déni de service distribué (**DDoS** pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité.

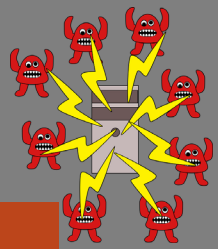
L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales…) : ce qui porte directement atteinte à l'image et donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…



BUT RECHERCHÉ

RENDRE UN SERVICE INDISPONIBLE. Le cybercriminel agit pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence).

Cette attaque peut être utilisée pour faire diversion d'une autre attaque visant à voler des données sensibles de sa cible.



SI VOUS ÊTES VICTIME

En cas de menace d'attaque, **NE PAYEZ PAS LA RANÇON** car vous alimenteriez le système mafieux, sans garantie que l'attaque n'aura pas lieu ou même qu'elle aurait pu avoir lieu.

FILTREZ LES REQUÊTES DE L'ATTAQUANT au niveau de votre pare-feu ou de votre hébergeur.

RÉCUPÉREZ LES FICHIERS DE JOURNALISATION (logs) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.

RÉALISEZ UNE COPIE COMPLÈTE DE LA MACHINE attaquée et de sa mémoire.

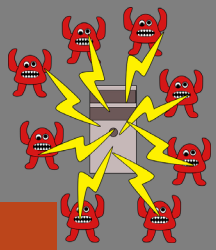
ÉVALUEZ LES DÉGÂTS CAUSÉS et les éventuelles informations perdues.

Assurez-vous que l'attaquant n'a pas profité du déni de service pour accéder à des informations sensibles, y compris sur d'autres systèmes. En cas de doute, **CHANGEZ TOUS LES MOTS DE PASSE D'ACCÈS** aux serveurs suspectés touchés et envisagez leur réinstallation complète à partir de sauvegardes réputées saines.

Avertissez vos écosystème, vos fournisseurs d'accès (FAI) et les institutions compétentes comme la CNIL et l'ANSSI.

FAITES VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS pour la remise en production et la sécurisation des serveurs touchés. Vous trouverez sur www.cybermalveillance.gouv.fr des prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie dont vous dépendez et tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.



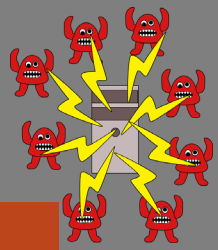
MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Ayez un pare-feu correctement paramétré : fermez tous les ports inutilisés et ne laissez que les adresses des machines indispensables accéder à distance aux fonctionnalités d'administration du site.

Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement, mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés.

Sollicitez votre hébergeur afin qu'il prévoie une réponse à ce type d'attaque au niveau de ses infrastructures.



LES INFRACTIONS

L'incrimination principale qui peut être ici retenue est celle d'**entrave à un système de traitement automatisé de données** (STAD ou système d'information).

Les **articles 323-1 à 323-7 du code pénal** disposent que :

• **Article 323-2 du code pénal** : « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ». Cet article pourra être appliqué dans l'hypothèse d'une attaque par « déni de service ». Il est passible d'une peine de cinq ans d'emprisonnement et de 150 000 euros d'amende. « Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende ».

• **Article 323-1 du code pénal** : « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données » est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. « Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système », les auteurs sont passibles de trois ans d'emprisonnement et de 100 000 euros d'amende. « Lorsque les infractions […] ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 euros d'amende »..

Les tentatives de ces infractions sont passibles des mêmes peines.

Si l'attaque fait suite à un « chantage » : les faits peuvent être qualifiés juridiquement de **tentative d'extorsion**, punie et réprimée par l'**article 312-1 du code pénal** : « L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ». L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende.

16

Mémos

MEMO : LES MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque service
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Utilisez un gestionnaire de mots de passe
5. Changez votre mot de passe au moindre soupçon
6. Ne communiquez jamais votre mot de passe à un tiers
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
8. Activez la double authentification lorsque c'est possible
9. Changez les mots de passe par défaut des différents services auxquels vous accédez
10. Choisissez un mot de passe particulièrement robuste pour votre messagerie
11.
12.
13.
14.
15.
16.

MEMO : LES RÉSEAUX SOCIAUX

1. Protégez l'accès à vos comptes
2. Vérifiez vos paramètres de confidentialité
3. Maîtrisez vos publications
4. Faites attention à qui vous parlez
5. Contrôlez les applications tierces
6. Évitez les ordinateurs et les réseaux Wi-Fi publics
7. Vérifiez régulièrement les connexions à votre compte
8. Faites preuve de discernement avec les informations publiées
9. Utilisez en conscience l'authentification avec votre compte de réseau social sur d'autres sites
10. Supprimez votre compte si vous ne l'utilisez plus
11.
12.
13.
14.
15.
16.

MEMO : LES APPAREILS MOBILES

1. Mettez en place les codes d'accès
2. Chiffrez les données de l'appareil
3. Appliquez les mises à jour de sécurité
4. Faites des sauvegardes
5. Utilisez une solution de sécurité contre les virus et autres attaques
6. N'installez des applications que depuis les sites ou magasins officiels
7. Contrôlez les autorisations de vos applications
8. Ne laissez pas votre appareil sans surveillance
9. Évitez les réseaux Wi-Fi publics ou inconnus
10. Ne stockez pas d'informations confidentielles sans protection
11.
12.
13.
14.
15.
16.

MEMO : LES SAUVEGARDES

1. Effectuez des sauvegardes régulières de vos données
2. Identifiez les appareils et supports qui contiennent des données
3. Déterminez quelles données doivent être sauvegardées
4. Choisissez une solution de sauvegarde adaptée à vos besoins
5. Planifiez vos sauvegardes
6. Déconnectez votre support de sauvegarde après utilisation
7. Protégez vos sauvegardes (perte, vol, casse...)
8. Testez vos sauvegardes
9. Vérifiez le support de sauvegarde
10. Sauvegardez les logiciels indispensables à l'exploitation de vos données
11.
12.
13.
14.
15.
16.

MEMO : LES MISES À JOUR

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels
2. Téléchargez les mises à jour uniquement depuis les sites officiels
3. Identifiez l'ensemble des appareils et logiciels utilisés
4. Activez l'option de téléchargement et d'installation automatique des mises à jour
5. Définissez les règles de réalisation des mises à jour
6. Planifiez les mises à jour lors de périodes d'inactivité
7. Méfiez-vous des fausses mises à jour sur Internet
8. Informez-vous sur la publication régulière des mises à jour de l'éditeur
9. Testez les mises à jour lorsque cela est possible et faites des sauvegardes
10. Protégez autrement les appareils qui ne peuvent pas être mis à jour
11.
12.
13.
14.
15.
16.

MEMO : LES USAGES PRO-PERSO

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez
2. Ne mélangez pas votre messagerie professionnelle et personnelle
3. Ayez une utilisation raisonnable d'Internet au travail
4. Maîtrisez vos propos sur les réseaux sociaux
5. N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles
6. Faites les mises à jour de sécurité de vos équipements
7. Utilisez une solution de sécurité contre les virus et autres attaques
8. N'installez des applications que depuis les sites ou magasins officiels
9. Méfiez-vous des supports USB
10. Évitez les réseaux Wi-Fi publics ou inconnus
11.
12.
13.
14.
15.
16.