SECURITE INFORMATIQUE

LA CYBERCRIMINALITÉ

La protection des systèmes d'information est principalement mais non exclusivement organisée à travers les articles 323-1 et suivants du code pénal.
Les atteintes aux systèmes d'information en tant que systèmes de traitement automatisé de données sont sanctionnées au titre de la réglementation sur la fraude informatique contenue aux articles 323-1 et suivants du Code pénal.

Ce dernier interdit notamment :

L'accès illicite, c'est-à-dire toute introduction dans un système informatique par une personne non autorisée (article 323-1 du Code pénal).
La notion d'accès s'entend de tout système de pénétration tel que la connexion pirate tant physique que logique, l'appel d'un programme alors que l'on ne dispose pas d'habilitation, l'interrogation d'un fichier sans autorisation.

Le maintien frauduleux, c'est-à-dire le maintien sur le système informatique après un accès illicite et après avoir pris conscience du caractère « anormal » de ce maintien (article 323-3 du Code pénal).
Le maintien frauduleux est notamment caractérisé par des connexions, visualisations ou opérations multiples, alors que l'accédant a pris conscience que ce maintien est « anormal ».

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 susvisés (article 323-3-1).

L'entrave du système, c'est-à-dire toute perturbation volontaire du fonctionnement d'un système informatique (article 323-2 du Code pénal).
L'entrave au système est appréhendée de manière extrêmement large car il suffit d'une influence « négative » sur le fonctionnement du système pour que le concept d'entrave soit retenu.

L'altération des données, c'est-à-dire toute suppression, modification ou introduction de données « pirate », avec la volonté de modifier l'état du système informatique les exploitant et ce, quelle qu'en soit l'influence (article 323-1 du Code pénal).

Il en est ainsi pour les bombes logiques, l'occupation, la saturation de la capacité mémoire, la mise en place de codification, de barrage, ou tout autre élément retardant un accès normal.
Par ailleurs, la création de faux et leur usage, constitue un délit autonome sanctionné au titre de faux en écriture privée, publique ou de commerce.
L'utilisateur doit impérativement adopter un comportement exempt de toute fraude car à défaut, il s'expose à de sévères sanctions pénales et disciplinaires.

Les textes : Modifiés par LOI n°2015-912 du 24 juillet 2015 - art. 4

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 puni de **deux ans** d'emprisonnement et de **60 000 €** 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 €** d'amende. »

« Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à **cinq ans** d'emprisonnement et à **150 000 €** d'amende. »

Article 323-2 du code pénal

« **Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données** est puni de **cinq ans** d'emprisonnement et de **150 000** € d'amende. »

« Lorsque cette infraction **a été commise à l'encontre** d'un système de traitement automatisé de données à caractère personnel mis en œuvre par **l'Etat**, la peine est portée à **sept ans** d'emprisonnement et à **300 000 €** d'amende. »

Article 323-3 du code pénal

« Le fait d'**introduire frauduleusement des données** dans un système de traitement automatisé, d'**extraire**, de **détenir**, de **reproduire**, de **transmettre**, de **supprimer** ou **de modifier** frauduleusement les données qu'il contient est puni de **cinq ans** d'emprisonnement et **de 150 000 €** d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à **sept ans** d'emprisonnement et à **300 000 €** d'amende. »

Article 323-3-1 du code pénal

« Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Article 323-4 du code pénal

« La **participation à un groupement formé ou à une entente établie** en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

L'Etat :
https://www.legifrance.gouv.fr/affichCode.do;jsessionid=38818154B5C119409AFA1C616C6A1185.tpdjo15v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=

https://www.ssi.gouv.fr/administration/bonnes-pratiques/
https://www.cnil.fr/fr/les-sanctions-penales
https://ssi.ac-strasbourg.fr/

Pro. :

https://clusif.fr
https://www.lesassisesdelasecurite.com/

Formations :
https://www.secnumacademie.gouv.fr/
https://www.fun-mooc.fr/

CISSP, expert sécurité certifié isc2
PECB certification iso 27005 risk manager + EBIOS
Certified Ethical Hacker v13

LES RÈGLES FONDAMENTALES DE LA SÉCURITÉ

Utiliser des mots de passe de qualité.
Le dictionnaire définit un mot de passe "comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé". Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.

Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc.
La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.

Effectuer des sauvegardes régulières.
Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.

Ne pas cliquer trop vite sur des liens.
Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

Ne jamais utiliser un compte administrateur pour naviguer.
L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'internet. En limitant les droits d'un utilisateur on limite aussi les risques d'infection ou de compromission de l'ordinateur.

Contrôler la diffusion d'informations personnelles.
L'internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…

Ne jamais relayer des canulars.
Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

Soyez prudent : l'internet est une rue peuplée d'inconnus !
Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou tout autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants.
Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme par exemple une pièce jointe appelée "photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. A l'inverse quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus "inerte" possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations