

LA CRIMINALITÉ INFORMATIQUE

Antoine Delforge

antoine.delforge@unamur.be

Chercheur au CRIDS/NADI



Introduction

• Tentative de définition (Nations Unies):

« Toute infraction susceptible d’être commise à l’aide d’un système ou d’un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique. »

- Distinctions entre 2 catégories d'infractions informatiques:
 - Celles dans lesquelles l'informatique est l'objet de l'infraction (computer-focused crime) et "Vise toute atteinte à la sécurité des systèmes et réseaux informatiques ou des données informatiques"
Exemples : cracking, intrusion, défiguration de sites web, virus, fausse carte de banque, spamming, fishing, malware, ransomware, hacking de compte facebook, téléchargement illégal...

- Celles dans lesquelles l'informatique est le moyen de commission d'une infraction classique (computer-assisted crime)

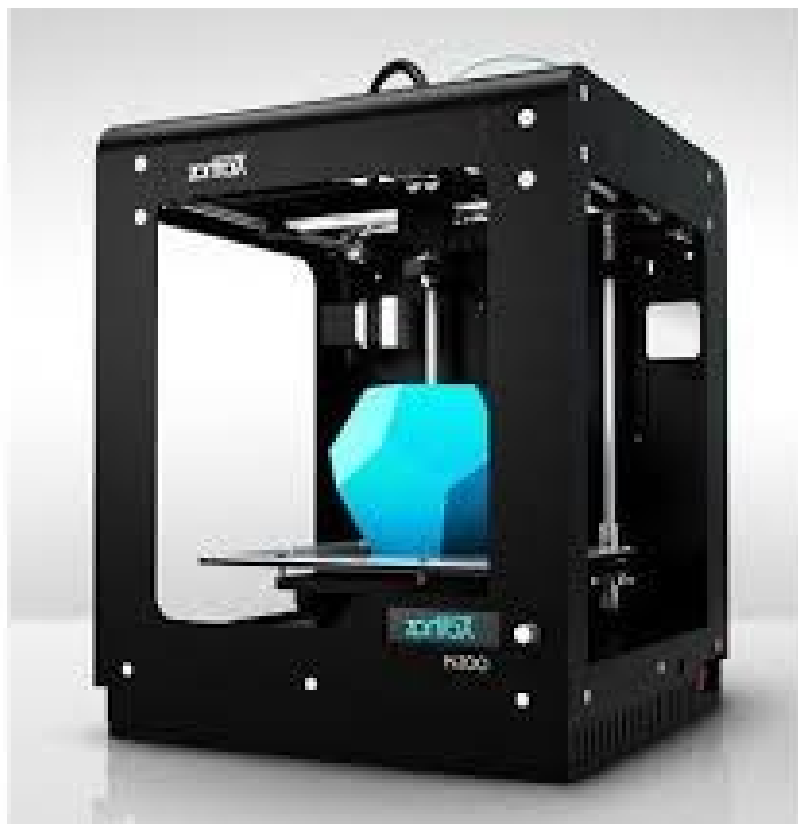
Exemple: le vol, l'escroquerie, l'espionnage, l'atteinte à l'honneur, la pornographie infantine, fabrication de fausses cartes de crédit ... qui se retrouvent facilitées par les TIC

A large, red, pixelated arrow pointing to the right, with a dashed outline.

Le « cybercrime » englobe donc, en principe, toute infraction susceptible d'être commise dans un environnement électronique

- ◉ Fragilité et volatilité des éléments constitutifs
 - ➔ Nécessité de préserver les informations numériques nécessaires aux poursuites (preuve)
- ◉ Facilité du recours à l'anonymat sur les réseaux
 - ➔ Difficultés d'identification et de localisation nécessaires pour permettre l'imputabilité des infractions (+ conflit avec vie privée)
- ◉ Transnationalité des réseaux
 - ➔ Eléments de l'infraction peuvent être dispersés sur les territoires de plusieurs pays dont les législations peuvent être différentes (conflits de souveraineté)
- ◉ Caractère dynamique et évolutif de cette criminalité
 - ➔ Criminalité se développe aussi rapidement que les TIC >< principe de prévisibilité du droit pénal. La rigidité du principe de légalité qui limite le pouvoir d'interprétation devient un obstacle à la réactivité de la répression.

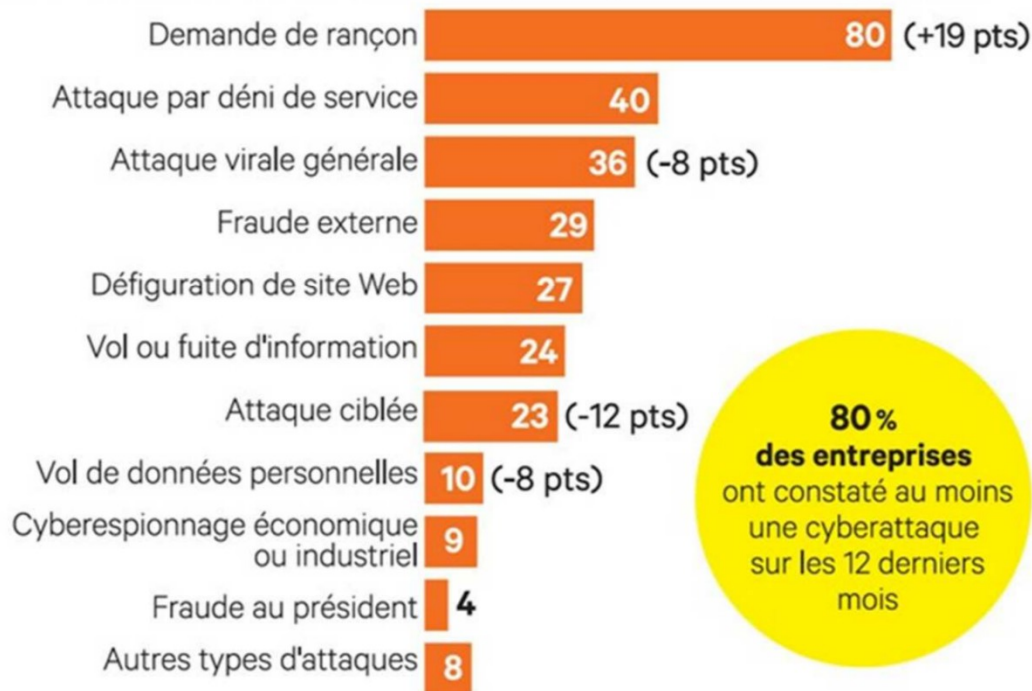
- Atteinte à la vie privée
- Infractions liées aux contenus (pédopornographie...)
- Infractions économiques (blanchiment...)
- Atteinte à la propriété intellectuelle
- Cyber-terrorisme



- 388 milliards de \$ de coûts liés à des cyberattaques en 2011 (Symantec)
- 1 000 milliards de \$ de fraude (McAfee en 2008)
- La criminalité informatique coûterait plus cher aux entreprises que la criminalité classique (Etude IBM 2006)
- En Belgique, sur une année, le piratage informatique +16,6% et les faux informatiques +27,2% (chiffres police de 2014)
- Augmentation exponentielle chaque année. Encore pire durant cette crise du coronavirus
- En Belgique :
 - – 4 faits en 2000 – 11.835 faits en 2009 – 15.496 faits en 2011 – 21.304 faits en 2012
 - En 2017 : 9.745 fraudes informatiques, 1.427 shouldersurfing, 238 ransomware...
 - 65 % de la criminalité économique actuellement

Les attaques subies par les entreprises

«Quel type de cyberattaque votre entreprise a-t-elle constatée au cours des douze derniers mois», en % (plusieurs réponses possibles)



«LES ÉCHOS» / ENQUÊTE OPINIONWAY RÉALISÉE AUPRÈS DE 141 MEMBRES DU CESIN

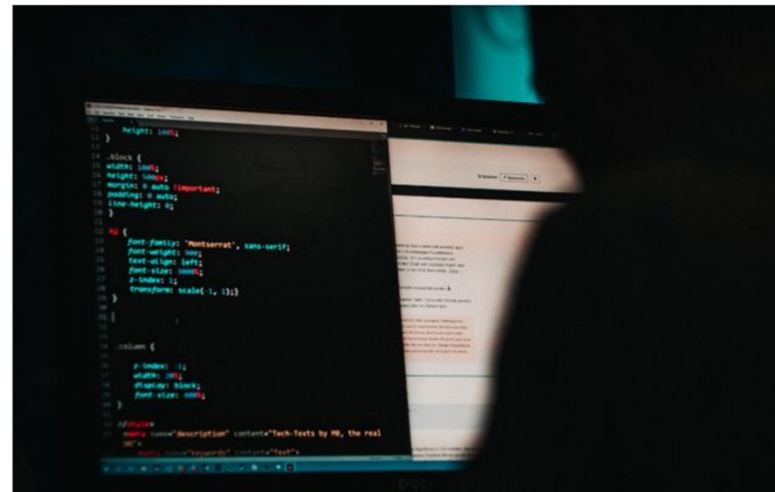
La cybercriminalité se chiffre désormais à 1000 milliards de dollars dans le monde

Accueil » Sécurité » La cybercriminalité se chiffre désormais à 1000 milliards de dollars dans le monde

Sécurité Par Remi Lou le 08 décembre 2020 à 15h50

1 commentaire

Une étude de McAfee révèle que le coût de la cybercriminalité à l'échelle mondiale explose, pour se retrouver aux alentours des 1000 milliards de dollars.



Cybercriminalité : augmentation de près de 30% des activités criminelles en 2019



32.943 cas de "criminalité informatique" recensés en 2019. - © Issaro Prakalung / EyeEm - Getty Images/EyeEm

Belga

Publié le vendredi 24 juillet 2020 - Mis à jour le vendredi 24 juillet 2020 à 15h05



217

La police fédérale a constaté une **nette hausse de la cybercriminalité en 2019**, avec 32.943 cas de "**criminalité informatique**" recensés l'an dernier, soit une **augmentation de 29,2% par rapport à 2018**. Les statistiques policières de criminalité annuelles publiées ce vendredi révèlent aussi que le nombre total de faits criminels enregistrés l'année passée est lui resté stable.

Newsletter info

Recevez chaque matin l'essentiel de l'actualité.

OK

Le glissement vers une criminalité en ligne "*est une réalité depuis plusieurs années*", souligne la police fédérale dans un communiqué vendredi mais ce basculement a été plus prononcé en 2019. **Les chiffres de la cybercriminalité ne cessent d'augmenter, avec une hausse de 29,2% en 2019 et de 18,1% en 2018**. Ces données portent sur la "*criminalité informatique*", soit des atteintes à la sécurité d'un système informatique ou à l'intégrité des données stockées dans un tel système.

Actu Impôts Immo Succession et donations Pension Banque et Assurances Carrière Budget Energie Voyages Epargne et placements

L'Echo

Mon Argent La réponse à toutes vos questions d'argent

Mon Argent > Budget

Faut-il souscrire une assurance "cybercriminalité"?

BUDGET

Caroline Sury
Aujourd'hui à 07:27

Avec Cyber Care, Proximus propose une assurance destinée à protéger la vie numérique de ses clients. Qu'est-ce qui est exclu et couvert? Quid ailleurs?



Ce type d'assurance couvre généralement les sinistres liés à des cas d'hameçonnage.
©Shutterstock

En début d'année, un nouveau produit est apparu discrètement dans la gamme des services proposés par Proximus: [Cyber Care](#). Il s'agit d'une assurance - développée en partenariat avec Axa Partners - destinée "à protéger votre vie numérique et votre famille contre tous les dangers du net", selon l'opérateur.

Moyennant une **mensualité de 4,99 euros**, cette assurance offre une **protection contre le vol d'identité, la fraude aux moyens de paiement, les risques liés au shopping en ligne, la récupération de données et enfin le harcèlement en ligne et la diffamation.**

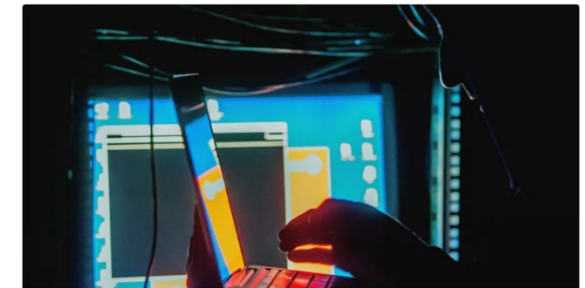
Posez ici votre qu...

Par exemple: Quels sont les frais à l'achat d'une maison ou d'un appartement?

Cybercriminalité : à Amilly, la mutuelle MNH sous le feu d'une attaque informatique avec demande de rançon

La MNH est victime depuis le 5 février dernier d'une attaque qui paralyse son système informatique. À Amilly, où se situe son siège, l'activité est à l'arrêt. "Il faut d'abord identifier ce logiciel, puis le retirer et relancer la machine", explique-t-on du côté de la mutuelle.

Publié le 13/02/2021 à 17h13



*Des hackers menacent de
publier le code source de
Cyberpunk 2077*

François Manens - 09 février 2021

Accueil > Des hackers menacent de publier le code source de Cyberpunk 2077

ACCUEIL > CYBERSÉCURITÉ

Victime d'une cyberattaque, l'hôpital de Dax fonctionne au ralenti

Le système d'information de l'hôpital de Dax a été mis hors service à la suite d'une attaque informatique. Les dossiers patients entièrement numérisés ne sont plus accessibles, de même que certains équipements médicaux, tels que les stérilisateurs utilisés dans les blocs opératoires. Une enquête judiciaire a été ouverte.

ALICE VITARD

PUBLIÉ LE 10 FÉVRIER 2021 À 12H14

CYBERSÉCURITÉ, SANTÉ, INFORMATIQUE

rtbf

ACCUEIL VIDEO AUDIO MON CHOIX CHAINES THEMATIQUES PLUS

REGIONS LIEGE

Face à la cybercriminalité, il est important pour les pouvoirs locaux de renforcer leur sécurité informatique



EN CHIFFRES

Cybercriminalité : 4 chiffres sur l'explosion des rançongiciels en France 🇫🇷

Entre 2019 et 2020, les plaintes après des attaques par rançongiciel en France ont augmenté de 32 %, selon une étude du ministère de l'Intérieur. L'industrie et les administrations publiques en sont les premières victimes. Voici les principaux chiffres qui illustrent un phénomène grandissant.

Selon une étude réalisée par MasterCard, il y aurait jusqu'à 3 fois plus de cyberattaques qu'avant la crise sanitaire. L'administration publique, les soins de santé et le retail figurent parmi les secteurs les plus vulnérables, alors que les banques belges obtiennent un score de sécurité bien supérieur à la moyenne mondiale.

Guerre en Ukraine: des conséquences possibles pour la cybersécurité belge

La présence de nombreuses institutions internationales sur le sol belge fait du pays une cible de choix.

Article réservé aux abonnés



Journaliste au pôle Multimédias
Par **Thomas Casavecchia**

- Droit pénal avant tout
- mais pas que
 - ⇒ Sources législatives multiples
 - ⇒ Ex: Code pénal, Loi du 13 juin 2005 relative aux communications électroniques, RGPD...
 - ⇒ Plusieurs matières se croisent : Droit pénal, droit de la propriété intellectuelle, droits de l'Homme, droit du commerce électronique...
- Identifier les impacts des « autres » branches du droit

- Un seul fait peut être constitutif de plusieurs infractions:
 - Particulièrement en criminalité informatique car définitions proches (cumul possible en crim. aspécifique et aspécifique)
 - ✓ ex: Arnaque sur Ebay: faux informatique, usage de faux informatique, fraude informatique, association de malfaiteurs...
- Infractions commises en ligne \neq infractions « classiques » ?
 - Ex: vol de données ?
 - Contre-ex: pédopornographie

- La législation en matière de cybercriminalité doit assurer :
 - la sécurité des réseaux : assurer la confidentialité, la disponibilité et l'intégrité des SI et des données
 - la sécurité sur les réseaux:
 - des personnes : dignité humaine (xénophobie, pornographie infantine)
vie privée (droit à l'image, correspondance)
honneur (injure, diffamation)
 - des biens : appropriations frauduleuses (vol, escroquerie,
espionnage)
propriété intellectuelle
 - des institutions : intérêts de la nation (blanchiment, espionnage, terrorisme)
défense nationale
 - une répression efficace des cyberdélicts : procédures d'enquête, preuve, saisies, conservation, coopération policière et judiciaire...

Au niveau international...

Problème / riposte international(e)

- Face à une criminalité mondiale, l'approche purement nationale est dépourvue de sens
- Nécessité de:
 - coordination
 - normes minimales obligatoires
 - harmonisation
- Sources d'harmonisation internationales:
 - Nations-Unies (approche incitative)
 - Conseil de l'Europe (approche contraignante)
 - OCDE (lignes directrices)

Au parquet, on espère que la guerre en Ukraine n'affectera pas la lutte contre la pédopornographie

Charleroi

Frédéric Ngom

Publié le 24-03-22 à 18h37 - Mis à jour le 24-03-22 à 19h21

Un sexagénaire possédant des images pédopornographiques a été repéré par la section "Child Abuse" des forces anti-cybercriminalité russes.



- **Recommandation n° R (89) 9**: fixe la définition précise d'une liste minimum d'abus que les Etats se doivent d'ériger en infractions pénales dans leur droit positif
- **Recommandation n° R (95) 13**: vise à instaurer une approche commune des problèmes de procédure pénale
- **Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité** : **premier instrument contraignant**
- **Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (28 janvier 2003)**

Le caractère universel de la convention

- Le caractère ouvert permet d'accueillir des Etats non Européens
- L'espace couvert par la convention représente actuellement plus de **80%** des infrastructures en matière de réseaux.

Toute la dynamique de normalisation et d'harmonisation au niveau international se construit autour de cette convention

Au niveau belge...

- La loi du 28 novembre 2000
 - Code d'instruction criminelle et autres lois (procédure)
 - Saisie
 - Recherche sur les réseaux
 - Obligation d'information et de collaboration
 - Ecoutes téléphoniques et interception des télécommunications
 - Obligation de conservation des données
 - Code pénal
 - Faux en informatique
 - Fraude informatique
 - Infractions contre la confidentialité, intégrité, disponibilité des systèmes informatiques et des données stockées, traitées, transmises par ces systèmes
 - Le sabotage des données et informatique
- Modifications ultérieures

La Loi belge

Le Code d'instruction criminelle

Code d'Instruction criminelle et autres lois:

- Saisie
- Recherche sur les réseaux
- Obligation d'information et de collaboration
- Ecoutes téléphoniques et interception des télécommunications
- Infiltrations sur internet
- (Obligation de conservation des données)

1. Saisie

"...les règles de ce code [le code d'instruction criminelle] relatives à la saisie, (...), sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique... "

Article *39 bis CIC*

Art. 39 *bis* CIC

SAISIE traditionnelle = dépossession

MAIS si saisie support souhaitable

- Copie des données sur des supports *ad hoc*
- et blocage de l'accès aux données et aux copies (mesures de sécurité)
- Données contraires aux bonnes mœurs : rendre inaccessible

2. Perquisition dans les systèmes informatiques

"La recherche dans un système informatique ou une partie de celui-ci qui a été saisi, peut être décidée par un officier de police judiciaire.

Sans préjudice de l'alinéa 1er, le procureur du Roi peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.

Les recherches visées aux alinéas 1er et 2 peuvent uniquement s'étendre aux données sauvegardées dans le système informatique qui est soit saisi, soit susceptible d'être saisi. A cet effet, chaque liaison externe de ce système informatique est empêchée avant que la recherche soit entamée."

Article 39bis, §2 CIC

"Le procureur du Roi peut **étendre la recherche** dans un système informatique ou une partie de celui-ci, entamée sur la base du paragraphe 2, vers un système informatique ou une partie de celui-ci qui se trouve dans un **autre lieu** que celui où la recherche est effectuée:

- si cette **extension est nécessaire** pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et
- ▢ si **d'autres mesures seraient disproportionnées**, ou s'il existe un risque que, sans cette extension, des **éléments de preuve soient perdus**.

*L'extension de la recherche dans un système informatique **ne peut pas excéder** les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont **spécifiquement accès**.*

"

Perquisition dans les systèmes informatiques (2)

- En principe : Domicile physique
- Possibilité pour le JI de perquisitionner d'autres systèmes informatiques « non saisis »
- Extension vers le « Domicile informatique » : pas d'unité de lieu
- hacking des autorités policières (sujet à contrôle par l'autorité judiciaire)

Perquisition dans les systèmes informatiques (2)

- On ne peut aller que dans des systèmes informatiques auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès (sinon espace infini) à condition que:
 - nécessaire pour la manifestation de la vérité ET si autres moyens disproportionnés
 - Et risque de perte de preuves...
- Y compris à l'étranger** (sans commission rogatoire avec simple information a posteriori des autorités étrangères) mais seule copie possible

Lors de recherches, si nécessité d'aide d'un tiers:

art. 88quater CIC + art 90quater § 4 CIC

COOPERATION

TEMOIGNAGE

EXPERTISE

**= REQUISITION DE PRETER
ASSISTANCE AUX AUTORITES
JUDICIAIRES**

Que faire ?

- Obligation d'information sur le S.I. + sur l'accès aux données ⚙ « **Rechercher, rendre accessible, copier, rendre inaccessible, retirer les données pertinentes qui sont stockées, traitées, transmises par le système** » et ce, dans la forme demandée
- Obligation de mettre en fonctionnement (remise des clés de décryptage, mot de passe, ...)
- Pouvoir du JI, pas de la police (simple demande alors, pas d'obligation)

Coopération des tiers

- Refuser de fournir son aide ➡ sanctions
- Obligation de secret des informations recueillies

Qui doit collaborer (sous peine de sanctions pénales)?

- **Toute personne présumée avoir une connaissance particulière du système**
ou des services (très large ! y compris FAI, autorités de certification..)
- **Sauf « droit au silence » !!!!** (article 90quater, §4 ne le prévoit pas mais principe général)

4. Interception des communications

art. 90 ter et quater CIC

La surveillance des communications est **strictement réglée** (autorisation du juge, indices concrets,...)

Les mêmes règles concernant les interceptions, repérages et identifications d'appel s'appliquent à toute communication **numérique** (mail...)

4. Interception des communications

Conditions

- Ordonnance du J d' I sauf urgence Proc. du Roi.
- Proportionnalité
- Uniquement pour infractions visées à l'article 90 ter CIC
(Extension importante des infractions visées)

+ Obligation de collaboration des opérateurs de services de télécommunications sur ordre du J. d'Instruction à l'interception de toute communication numérique

- Art. 46sexies C.I.Cr. encadre maintenant cette méthode

- Seulement si
 - Nécessaire
 - Proportionné
 - Indices sérieux

La Loi belge

Le Code Pénal

"(...) **commet un faux**, en introduisant dans un système informatique, en **modifiant** ou effaçant **des données**, qui sont stockées, traitées ou transmises par un système informatique, **ou en modifiant par tout moyen technologique l'utilisation possible des données** dans un système informatique, et par là **modifie la portée juridique** de telles données, ... "

Article **210bis** du Code pénal

1. Faux en informatique (2)

- Nouvelle règle en plus du 'faux' classique (en écriture)
- Conditions:
 - Introduction, modification, effacement de données ou modification de l'utilisation possible de ces données
 - 'données' : notion très large
 - Pas applicable si utilisation d'un ordi pour imprimer un texte (faux classique)
 - Modification de la portée juridique de ces données
 - Le juge apprécie

1. Faux en informatique (2)

- Intention frauduleuse ou dessein de nuire
 - L'infraction est commise dans le but de se procurer ou de procurer à un tiers un avantage illicite, le plus souvent au détriment d'une personne ou de la collectivité
- Infraction annexe : Usage de ce faux (210bis §2 Code Pénal)

Souvent les 2 infractions sont commises en même temps

2. Fraude informatique

"Celui qui **cherche à se procurer**, pour lui-même ou pour autrui, **avec une intention frauduleuse, un avantage économique illégal** en introduisant dans un système informatique, **en modifiant** ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, **ou en modifiant par tout moyen technologique l'utilisation normale des données** dans un système informatique ... "

Article *504quater* du *Code pénal*

- ⊙ « fraude » : acte dont le but est de préjudicier des droits à respecter (acte illicite et moyens illégaux ou même acte illicite avec moyens réguliers)
- ⊙ Conditions:
 - Intention frauduleuse
 - Avantage économique
 - Pour soi-même ou pour autrui
 - En introduisant, modifiant effaçant des données ou leur utilisation, contrairement à leur utilisation normale

3. Infractions contre la confidentialité, intégrité, disponibilité des SI et des données



CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ



Article 550 *bis* Code pénal

"§ 1er. Celui qui, **sachant qu'il n'y est pas autorisé**, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er, est commise avec une **intention frauduleuse**, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Celui qui, **avec une intention frauduleuse ou dans le but de nuire, outrepassé son pouvoir d'accès** à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement. "

3. Infractions contre la confidentialité, intégrité, disponibilité des SI et des données (2)



CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ



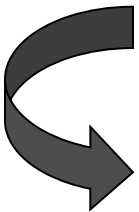
- ◉ §1: L'accès et le maintien non autorisé dans un système informatique
 - Savoir qu'on n'est pas autorisé
 - Si intention frauduleuse : peine plus lourde
- ◉ §2: Outrepasser son pouvoir d'accès (hacking interne vs. hacking externe)
 - Intention de nuire ou but frauduleux pour hacking interne
- ◉ Circonstances aggravantes
 - Reprendre des données du système en question (traitées, stockées, transmises)
 - Faire un usage du système (toujours!) ou se servir du système pour accéder à un autre
 - Causer un dommage (même sans intention)

+ tentative

3. Infractions contre la confidentialité, intégrité, disponibilité des systèmes des SI et données (3)

- Article 550*bis* Code pénal (Suite)

"§ 5. Celui qui, **indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif**, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 4, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement."



Produire, vendre, posséder, obtenir pour utiliser, diffuser, mettre à disposition un « hackertool »: dispositif conçu ou adapté pour commettre une des infractions citées

3. Infractions contre la confidentialité, intégrité, disponibilité des systèmes des SI et données (4)

- Article 550*bis* Code pénal (Suite)

« § 6. Celui qui ordonne la commission d'une des infractions visées aux §§ 1er à 5 ou qui y incite, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de cent [euros] à deux cent mille [euros] ou d'une de ces peines seulement.

§ 7. Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement.

§ 8. Les peines prévues par les §§ 1er à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550ter,"

»

3. Infractions contre la confidentialité, intégrité, disponibilité des systèmes des SI et données (5)

- Ordonner la commission d'une infraction
- Révéler, transmettre des données obtenues par infraction (le savoir)

+ récidive

4. Le sabotage des données

"§1. Celui qui, **sachant qu'il n'y est pas autorisé**, directement ou indirectement, **introduit dans un système informatique, modifie ou efface des données**, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique...

La même peine sera appliquée lorsque l'infraction visée à l'alinéa 1er est commise contre un système informatique d'une infrastructure critique comme visée dans l'article 3, 4°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni ...

§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni ..."

Article **550ter** du Code pénal

4. Le sabotage des données

§ 4. Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 3, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni ...

§ 5. Les peines prévues par les §§ 1er à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent le prononcé d'une condamnation pour une de ces infractions ou pour une des infractions visées aux articles 210bis, 259bis, 314bis, 504quater ou 550bis.

§ 6. La tentative de commettre l'infraction visée au § 1er est punie des mêmes peines.

Article **550ter** du Code pénal

4. Le sabotage des données (2)

- Savoir qu'on n'est pas autorisé
- Si intention frauduleuse : peine plus lourde
- + Concevoir, mettre à disposition, etc. des « hackertools » pour commettre ces infractions
- + récidive
- + tentative

Demande de Partenariat très Sérieuse Svp
Nom : Anita Bamba.

Bonjour/Votre Attention

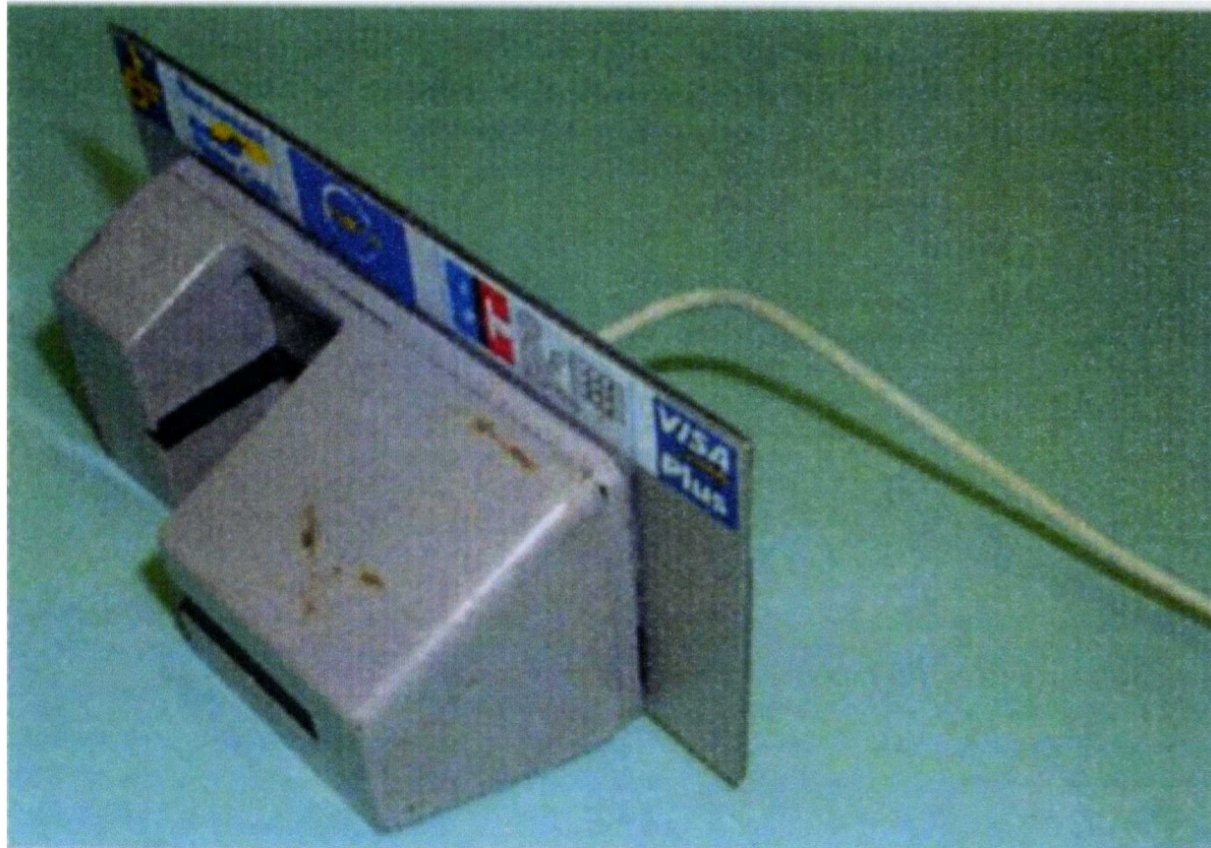
Mes sincères salutations et mes excuses à votre égard. Je voudrais m'excuser de mon intrusion dans votre vie privée. Je me nomme Mme ANITA BAMBA, Cadre au Département de la Comptabilité à Ecobank Côte d'Ivoire. Un compte a été ouvert au sein de notre banque en 2005 et depuis 2011, aucune opération ne s'est effectuée. Ce compte présente à ce jour dans nos livres, un compte créditeur de Quatre Millions Cinq Cent Mille Euros. 4.500.000 € Après avoir consulté tous les dossiers relatifs à ce compte, je me suis rendue compte que je pouvais disposer aisément de cet argent si je réussissais à le virer sur un compte à l'extérieur donc je suis à la recherche d'un partenaire honnête.

Le possesseur de ce compte feu ABDELLAH BAHA, un expatrié de Petrol-Technical Support Services Inc, décédé suite à un accident de la circulation. Personne ne sait à ce jour l'existence de ce compte. Ce compte ne possède aucun autre proche parent.

J'aimerais que vous m'aidiez à transférer cet argent pour investir dans votre domaine. Après le transfert je vous offre 40% pour votre aide. Soyez sûr que c'est une véritable opportunité que je vous offre.

Très sincèrement,
Mme Anita

Exercices



Jne attaque informatique de portée mondiale crée la panique

es hôpitaux britanniques et des entreprises espagnoles ont été touchés par es virus, vendredi. Ils bloquent l'accès aux fichiers d'un ordinateur afin 'obtenir une rançon.

E MONDE | 12.05.2017 à 18h43 • Mis à jour le 19.05.2017 à 16h38

Abonnez vous à partir de 1 € Réagir Ajouter Partager (1 250) Tweeter

es autorités américaines ont mis en garde vendredi 12 mai contre une vague e cyberattaques simultanées qui a touché des dizaines de pays dans le monde, recommandant de ne pas payer de rançon aux pirates informatiques. eux-ci ont apparemment exploité une faille dans les systèmes Windows, ivulguée dans des documents piratés de l'agence de sécurité américaine NSA.

Nous avons reçu de multiples rapports d'infection par un logiciel de rançon, a crit le ministère américain de la sécurité intérieure dans un communiqué. 'articuliers et organisations sont encouragés à ne pas payer la rançon car cela e garantit pas que l'accès aux données sera restauré. »



Lawrence Dunhill

@LawrenceDunhill

Suivre

Here's the malware attack which appears to have hit NHS hospitals right across England today



07:06 - 12 mai 2017

Exercices

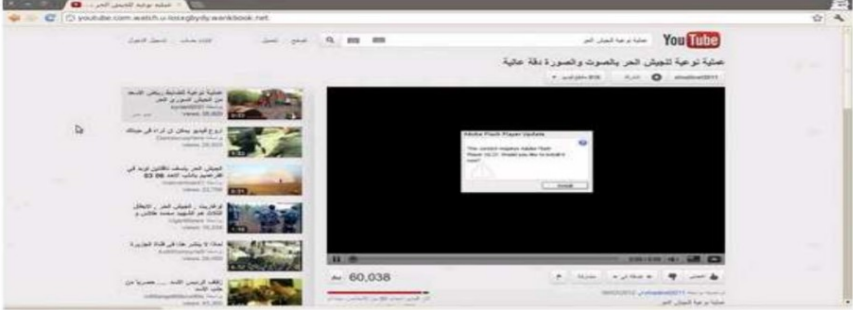
Un faux YouTube pour piéger les activistes syriens - LeMonde.fr - Windows Internet Explorer provided by JIORT

http://www.lemonde.fr/technologies/article/2012/03/15/un-faux-youtube-pour-pieger-les-activistes-syriens

File Edit View Favorites Tools Help

Favorites Suggested Sites Web Slice Gallery Customize Links

Mail :: Inbox (1) Loft - Immoweb r... Un faux YouTu... Home Feeds (1)



LE MONDE.FR - Un faux site YouTube tentant de piéger les activistes syriens a fait son apparition en ligne, avant d'être supprimé, alerte l'organisation américaine Electronic Frontier Foundation. La page, se présentant comme une page classique de YouTube dédiée aux vidéos d'opposants syriens, contenait en réalité deux pièges : elle tentait de voler les mots de passe des utilisateurs qui souhaitaient commenter une vidéo, et demandait aussi aux internautes de "mettre à jour" leur player Flash.

En réalité, si l'internaute acceptait cette "mise à jour", son ordinateur téléchargeait un premier maliciel, qui se connectait alors à un serveur situé en Syrie et installait plusieurs autres logiciels malveillants sur l'ordinateur. Le contrôleur des maliciels obtenait ainsi un accès complet à l'ordinateur de l'internaute.

Error on page.

UN IMMEUBLE HACKÉ DEVIENT UN TETRIS GÉANT

Posted by [GOLEM13](#) on avril 23, 2012 · [Laisser un commentaire](#)



CASTRES : UN COLLEGIEN AURAIT RÉUSSI À MODIFIER SES NOTES PAR INTERNET

Posted by [GOLEM13](#) on mars 19, 2015 · [Laisser un commentaire](#)



En 1983, dans le film Wargames, Matthew Broderick piratait le système informatique de son lycée depuis sa chambre. Pas si loin de ce personnage de fiction américaine, La Dépêche du Midi nous rapporte l'affaire d'un collégien de Castres (Tarn) qui aurait usurpé l'identité du principal de son établissement afin de se connecter au système informatique et de [...]

- Faux profil Facebook?
- Défaçage de site web?
- Utiliser le wifi du voisin?
 - Non-protégé
 - Protégé
- Attaque DDOS?

MERCI DE VOTRE ATTENTION

DES QUESTIONS ?

antoine.delforge@unamur.be