Droit des TIC

Partie 3:
La loi belge sur la criminalité informatique :

Aspects matériels

Franck Dumortier
Franck.dumortier@unamur.be

La loi du 28 novembre 2000

- Code pénal (droit matériel : 4 types d'infractions)
  - 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

- 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

Terminologie

- système informatique: « par système informatique, on entend tout système permettant le stockage, le traitement ou la transmission de données. A ce propos, on pense principalement aux ordinateurs, aux cartes à puce, etc., mais également aux réseaux et à leurs composants ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information »

- données: « par données, on entend les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique. Ce dernier morceau de phrase est ajouté de loi chaque fois qu'une confusion est possible avec la signification générale et beaucoup plus large de la notion de «données». La forme matérielle que revêtent ces données - qu'elle soit électromagnétique, optique ou autre - n'a pas d'importance »

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION

1. Le faux en informatique

Le faux en informatique (1)

Article 210 bis du Code Pénal :

« Celui qui commet un faux en **introduisant** dans un système informatique, en **modifiant** ou **effaçan**t 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** »

Le faux en informatique (2)

- « dissimulation intentionnelle de la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique »

- « toute falsification, par le biais de la manipulation de données, de données informatiques pertinentes » (Doc. parl.)

- Ex. : confection ou falsification de carte de crédit, faux contrat numérique (lorsque les données juridiquement pertinentes ne sont plus imprimées sur papier, ni signées à la main), introduction d'un faux n° de carte de crédit…

Le faux en informatique (3)

Éléments constitutifs :

- Éléments matériels :
  - Une « écriture » = introduction, modification ou effacement de données dans un système informatique ou modification de l'utilisation qui peut être faite de ces données
  - Altération de la vérité par un des modes légaux
  - Modification de la portée juridique des données (infraction de résultat)
- Elément moral :
  - Dol spécial : intention frauduleuse/dessein de nuire (cfr. 193 C. pén.)

- Peine : [6m-5a] - [am. 26-100.000 EUR]

Le faux en informatique (4)

Exemple : falsification de contrats digitaux

- en modifiant certaines dispositions (par ex. le montant dû pour la prestation convenue, la période d'exécution);
- en effaçant (par ex. la disposition d'une clause pénale est effacée);
- ou en introduisant (par ex. alors que l'offre acceptée n'en comportait pas, elle ajoute une clause pénale).

Le faux en informatique (5)

Un cas concret :

- Un habitant d'Alvin (USA) âgé de 36 ans a réussi le casse numérique du siècle. Andy Surface s'est contenté d'envoyé un seul message électronique et il a récolté en retour 8 millions de dollars.
- Il a tout simplement envoyé une facture accompagnée d'une demande de paiement à Condé Nast, une grosse maison d'édition américaine qui édite notamment Vogue et le New Yorker. Le message imitait ceux envoyés par Quad/Graphics, un sous-traitant du groupe de presse.
- Tout s'est déroulé début novembre 2010. L'e-mail est arrivé dans les bureaux new-yorkais de Condé Nast. Le formulaire avait vraiment l'air de provenir de Quad/Graphics, et demandait un paiement direct sur le compte du sous-traitant, dont les informations étaient fournies. L'éditeur n'a rien vu venir, il a rempli le document et l'a renvoyé par Fax au numéro indiqué à l'intérieur. Suite à cela, un virement bancaire a été effectué... d'une hauteur de 8 millions de dollars, comme demandé.
- Pour que tout ait l'air plus crédible, Andy avait crée une entreprise au nom très proche de Quad/Graphics ("Quad Graph").

Le faux en informatique (6)

Cas de jurisprudence 1 : Corr. Dendermonde, 28 novembre 2005

- Un journaliste d'investigation avait créé une fausse adresse e-mail au nom d'une personne tierce (E.V.M., échevin de sa commune) et envoyé un e-mail via cette adresse à un autre échevin de cette même commune (J.M.). Via la Computer Crime Unit de Termonde, l'adresse IP, puis l'identité de l'émetteur de cet e-mail furent trouvées.
- Le tribunal de Termonde jugea qu'il s'agissait d'un faux et usage de faux en informatique, soulignant qu'il y eut bien une manipulation de données juridiquement pertinentes (la modification de la portée juridique des données manipulées est un élément constitutif de l'infraction de faux en informatique).
- Pour qu'il y ait infraction de faux en informatique, il faut néanmoins qu'il y ait aussi un dol spécial. Le tribunal en confirme l'existence en s'appuyant d'une part sur le fait que l'acte d'envoi de cet e-mail n'était pas purement impulsif (comme l'affirmait le prévenu), car il avait nécessité des actes préparatoires (création d'une fausse adresse e-mail), et d'autre part sur le fait que le prévenu avait avoué que le but de l'e-mail était de « provoquer E.V.M. », ce qui, selon le tribunal, suppose une intention de nuire.

Le faux en informatique (7)

Cas de jurisprudence 2 : Corr. Dendermonde (13e ch.), 25 mai 2007

Un étudiant de l'Université d'Anvers avait tenté de s'introduire dans l'espace réservé aux professeurs du système informatique de l'université en envoyant au service informatique de l'université un faux e-mail émanant soi-disant d'un de ses professeurs. Dans cet e-mail, le « professeur » demandait un nouveau log-in et mot de passe prétextant ayant perdu les siens. Le service informatique, suspectant une tentative d'intrusion, fournit alors de fausses données. Ceci lui permit d'identifier l'adresse IP du pirate qui tenta peu après – mais en vain – de s'introduire dans l'espace réservé aux professeurs du système informatique de l'université.

Facebook: créer un faux profil est désormais condamnable en Belgique

C'est une première en Belgique. Une femme vient d'être condamnée par le tribunal correctionnel de Gand pour avoir créé un faux profil Facebook. Il s'agit d'un signal clair envoyé à la société.

21 Septembre 2011 12h19

A+ A- Imprimer

Le tribunal correctionnel de Gand a condamné à sept mois de prison avec sursis et une amende de 550 euros une femme qui avait créé un faux profil Facebook au nom de son ancien patron pour l'accuser d'adultère. Son mari, qui comparaissait également, a été acquitté.

Un signal à la société

Il s'agit du premier procès en Belgique pour faux profil Facebook. Le juge, par sa décision, a donné un signal clair à la société. Les prévenus sont une femme et un homme âgés tous deux de 38 ans et habitant à Kortemark. Ils ont créé l'an dernier un profil au nom de l'ancien employeur de la femme, un chef d'entreprise de 36 ans. Ils ont ensuite posté plusieurs faux messages qui devaient faire croire que l'homme commettait l'adultère. Les faits se sont produits entre juin et décembre l'an dernier et se sont arrêtés après qu'une enquête concernant les adresses

A SAVOIR

Appel à témoins

Dans le cadre d'un de nos reportages, nous recherchons des personnes ayant été piégées par un faux profil Facebook. Si vous êtes concernés ou connaissez quelqu'un qui l'est, vous pouvez nous envoyer un mail à l'adresse redactionrtlinfo@rtl.be

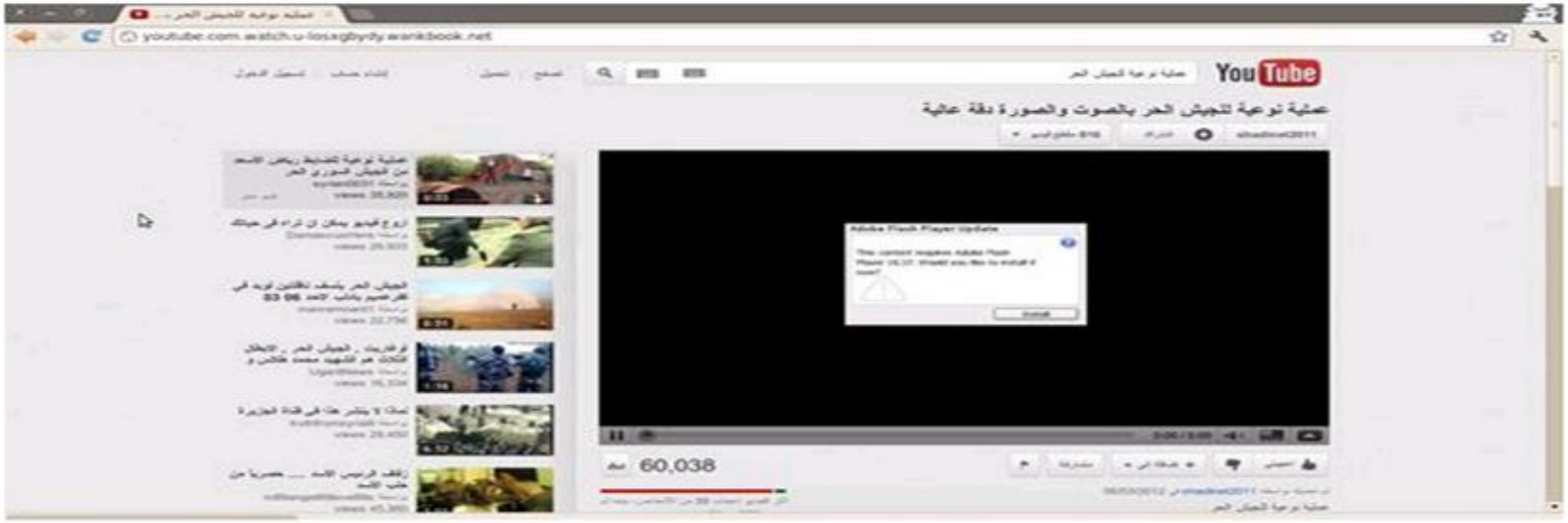
Un faux YouTube pour piéger les activistes syriens - LeMonde.fr - Windows Internet Explorer provided by JIO

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

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 (J)



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.

Le faux en informatique (8)

- Usage de faux (210bis § 2) :
  - « celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses »
  - Peine = peine du faux
- Tentative (210bis §3) :
  - ne concerne pas l'usage de faux
  - peine : [6m-3a] - [am. 26-50.000 EUR]
- Récidive (210bis § 4) :
  - peine doublée si récidive dans les 5 ans du prononcé
  - ceci est dérogatoire au droit commun de la récidive en matière délictuelle : l'article 56 al. 2 et s. C. pén. prévoit la récidive en cas de nouvelle infraction commise dans un délai de 5 ans à dater du jour où le condamné a subi ou prescrit sa peine

Le faux en informatique (9)

- Au contraire du faux en écritures de droit commun (193 C. pén.), le faux en informatique est « unique » (pas de classification : authentique, privé)

- Remarque :

  Si un ordinateur ou un programme informatique est utilisé pour constituer un « faux » papier (via un logiciel de traitement de texte, par exemple), les dispositions classiques de faux en écritures trouveront à s'appliquer dès lors que ce faux aura été imprimé

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION

2. La fraude informatique

La fraude informatique (1)

Article 504 quater du Code Pénal :

« 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 »

La fraude informatique (2)

Pour rappel :

- Escroquerie : fraude de droit commun qui consiste à tromper une personne (art. 496 C. pén.)

- Fraude informatique : fraude qui consiste à ‘tromper une machine’

La fraude informatique (3)

Eléments constitutifs:

- **Eléménts matériels**
  - Manipulation de données ou de l'utilisation normale des données
  - Avantage économique (depuis la loi du 15 mai 2006, la seule tentative d'obtenir un avantage économique illégal suffit).
  - Pour soi-même ou pour autrui

- **Elémént moral**
  - Dol spécial : intention frauduleuse d'obtenir sans droit un bénéfice économique illégal pour soi-même ou pour autrui

La fraude informatique (4)

- Peine : [6m-5a] - [am. 26-100.000 EUR]
- Tentative (504quater §2) : [6m-3a] - [am. 26-50.000 EUR]
- Récidive (504quater § 3) : si dans les 5 ans du prononcé

  ceci est dérogatoire au droit commun de la récidive en matière délictuelle : l'article 56 al. 2 et s. C. pén. prévoit la récidive en cas de nouvelle infraction commise dans un délai de 5 ans à dater du jour où le condamné a subi ou prescrit sa peine

La fraude informatique (5)

Contre-Exemple: L'arnaque nigériane

Dear friend,

Based on the further explicit investment information about your country from my research i wish to invest in your country under your supervision.

I am Prince Fayed W. Bolkiah, the eldest son of Prince Jeffrey Bolkiah former finance minister of Brunei, the tiny oil-rich sultanate on the Gulf Island of Borneo. I save your time by not amplifying my extended royal family history, which has already been disseminated by the international media during the controversial dispute that erupted between my father and his tepbrother, the sultan of Brunei Sheik Muda Hassanal Bolkiah.

As you may know from the international media,The sultan had accused my father of financial mismanagement and impropriety of us$14.8 billion dollars this was as a result of the Asian Financial crisis that made my father company Amedeo Development Company and government owned Brunei investment company to be declared bankrupt during his tenure in the office. However my father was kept under house arrest, his bank account and private properties including a crude oil export refinery were later confiscated by the sultanate to avoid further prosecution from the sultan and his security operatives, but before I could do that I was placed under house arrest by the sultan and not have access to phone but I have a palm V hand -held computer from which I am sending you this mail. Some of the guard here are still loyal to me, so they would be my contact with you if there is any documents I need to send to you to enable you have access to this funds and invest it for me.

Before my in-castration, I went ahead to dispatch the sum of five undred million United States Dollars {USD$500,000,000.00} in cash under special arrangement into the custody of different private Banks and trust company's for safe keeping abroad. The money where splited and kept in the following countries, : in Canada, France, Spain, Holland andin London. Firstly, you will be required to travel to London to claim the money there before prceeding to other countries.

I seek your good assistance to invest these funds into a profitable investment in your country to facilitate future survival for my family abroad. After due deliberation with my aids we decides to offer a certain percentage to you as compensation for your co-operation and kind sincerity to carry out this assignment.

Since there will be an expenditure from your side, I will advice you not to worry about it because you will be reimburse any amount you may spend as to enable this transaction get to it's final dream, for both local and international expenses will be given to you back while you will be part of the beneficiary of any investment made with this cash, to add to that, I will like to let to your understand that all this is not part of your financial compensation that will be given to you.

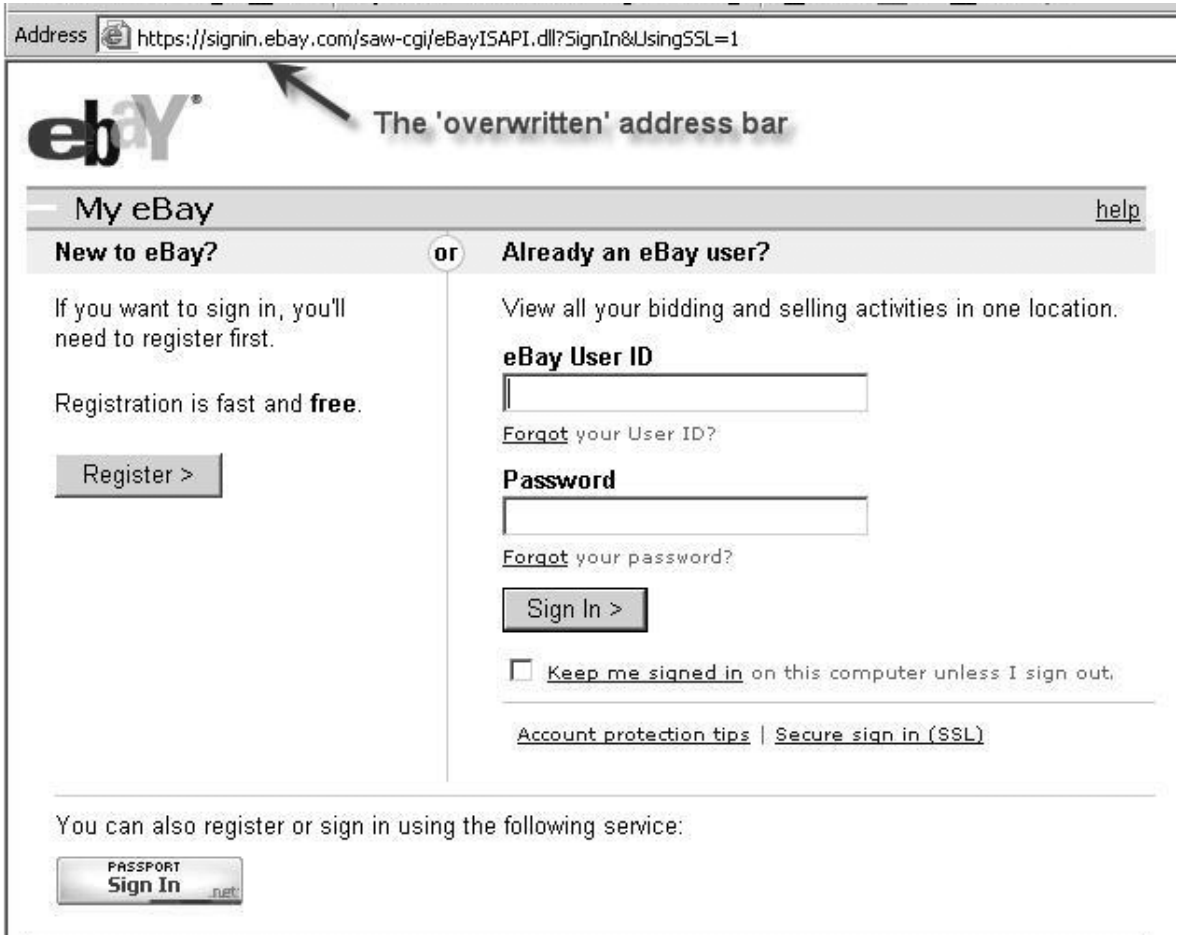
During this dispensation Please I count on your absolute confidentiality, transparency and trust while looking forward to your prompt reply towards a swift conclusion of this transaction. Many thanks and blessing remains with you.

Finally, your financial compensation will be the 15% of the total cash. That is 15% of (u.s $500,000,000.00).

Thanks.
Prince Fayed.W. Bolkiah.

La fraude informatique (6)

Exemple 1 : le phishing



Security key: qlgarixmqjt

citi

Dear Citibank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
https://web.da-us.citibank.com/cgi-bin/help_desk/verify.asp
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citibank Business Development; this process cannot be externally requested through Customer Support.

Sincerely,
Citibank.com
Security Department.

Notice the random text at the bottom - a spam sign

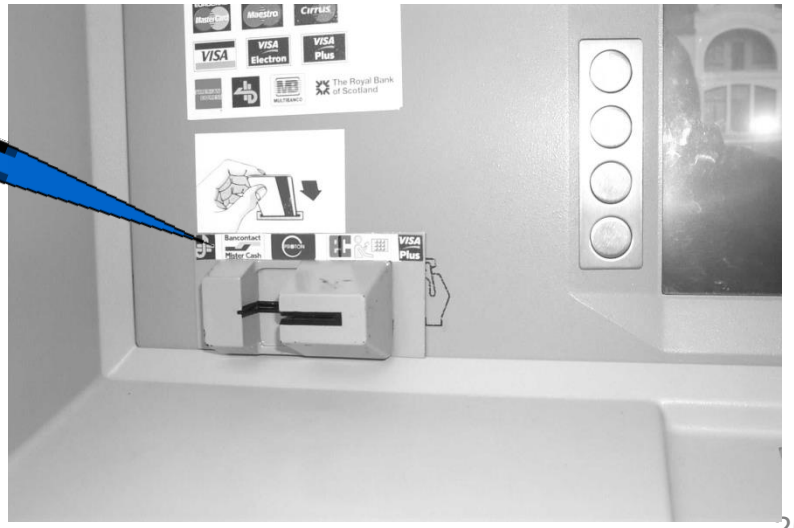
brcffq

Autre illustration de fraude : le skimming (1)

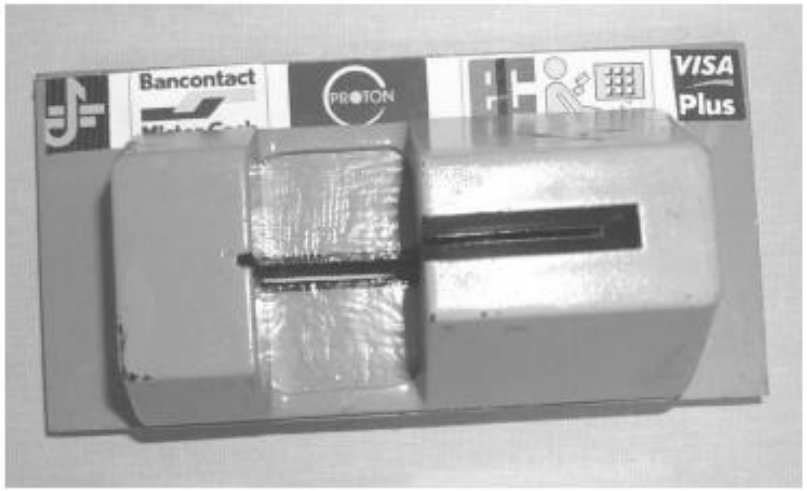
- ✓ « Skimming » ? : procédé qui consiste à copier électroniquement les informations d'une piste magnétique d'une carte valide vers une autre carte sans que le vrai Titulaire s'en rende compte.

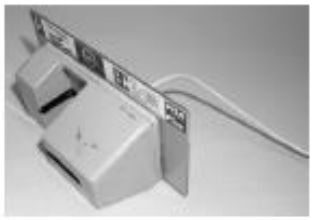
- Faux informatique
- Fraude informatique

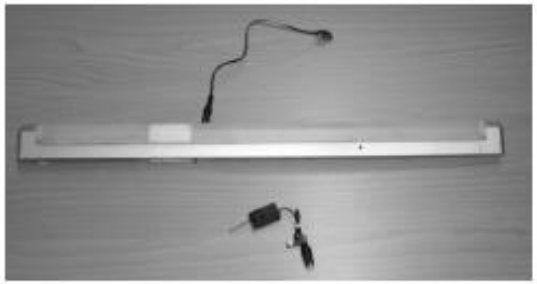
Autre illustration de fraude : le skimming (2)

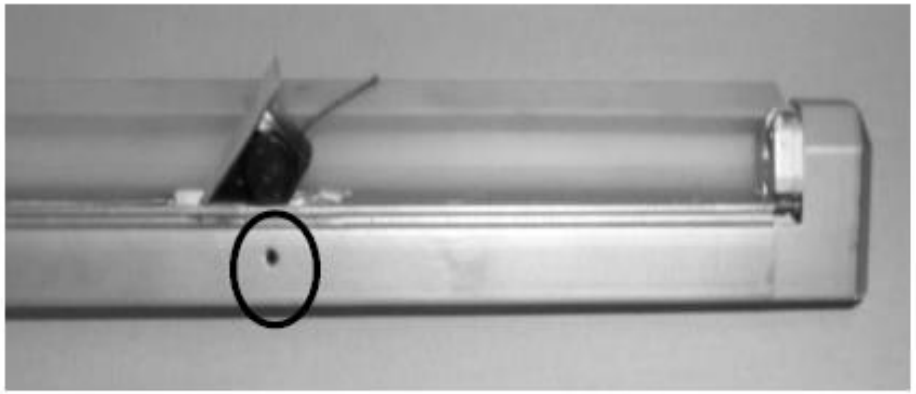


Autre illustration de fraude : le skimming (3)









Autre illustration de fraude : le skimming (4)

Autre illustration de fraude : le skimming (5)

La fraude informatique (7)

Cas de jurisprudence :

- Cass. (2e ch.) RG P.03.0366.N, 6 mai 2003 (utilisation de carte de carburant volée)
- Anvers 28 mai 2008 (utilisation d'une carte VISA de l'employeur pour des raisons personnelle et non professionnelles)
- Dépassement irrégulier de la limite de sa propre carte de crédit
- Beaucoup de cas de Skimming
  - Corr. Bruxelles, 6 janvier 2004, inédit,
  - Corr. Dendermonde, 7 juin 2004, inédit,
  - Corr. Brugge, 8 juin 2004, inédit
- Anvers 10 septembre 2008 (utilisation d'une carte bancaire au-delà de l'autorisation donnée par le propriétaire de la carte)

3. Le hacking

Le hacking (1)

Article 550 bis du Code Pénal :

« §1er Celui qui, **sachant qu'il n'y est pas autorisé, accède** à un système informatique ou s'y maintient, est puni …

Si l'infraction est commise avec une intention frauduleuse, la peine…

§2 Celui qui avec une intention frauduleuse ou dans le but de nuire, **outrepasse son pouvoir d'accès** à un système informatique, est puni… »

Différence entre §1 et §2 ???

Le hacking (2)

Hacking externe

- Dol général (protection accrue, éviter mise en danger des réseaux)
- Difficulté de déterminer s'il y a autorisation dans le cas de réseaux interconnectés dont certains sont de libre accès
- Pas besoin de dommage pour qu'il y ait délit
- Pas besoin d'effraction d'un système de sécurité (alors que vol classique puni si avec effraction, violence, menace ou la nuit)
- Coup d'œil sur un écran : non. Acte positif : oui
- Ordinateur, GSM, PDA, etc.

Hacking interne

- Dol spécial (int. Frauduleuse (appât de gain illicite/ intention de nuire)
- Il faut un droit d'accès partiel et outrepasser ce pouvoir (espace, fonction ou temps)
- Autorisation?

- Pas besoin de dommage

Le hacking (3)

Article 550 bis du Code Pénal : Circonstances aggravantes

« §3 Celui qui se trouve dans une de ces situations et:

1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique (ex: espionnage informatique)

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers; (ex : botnets)

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système; est puni … »

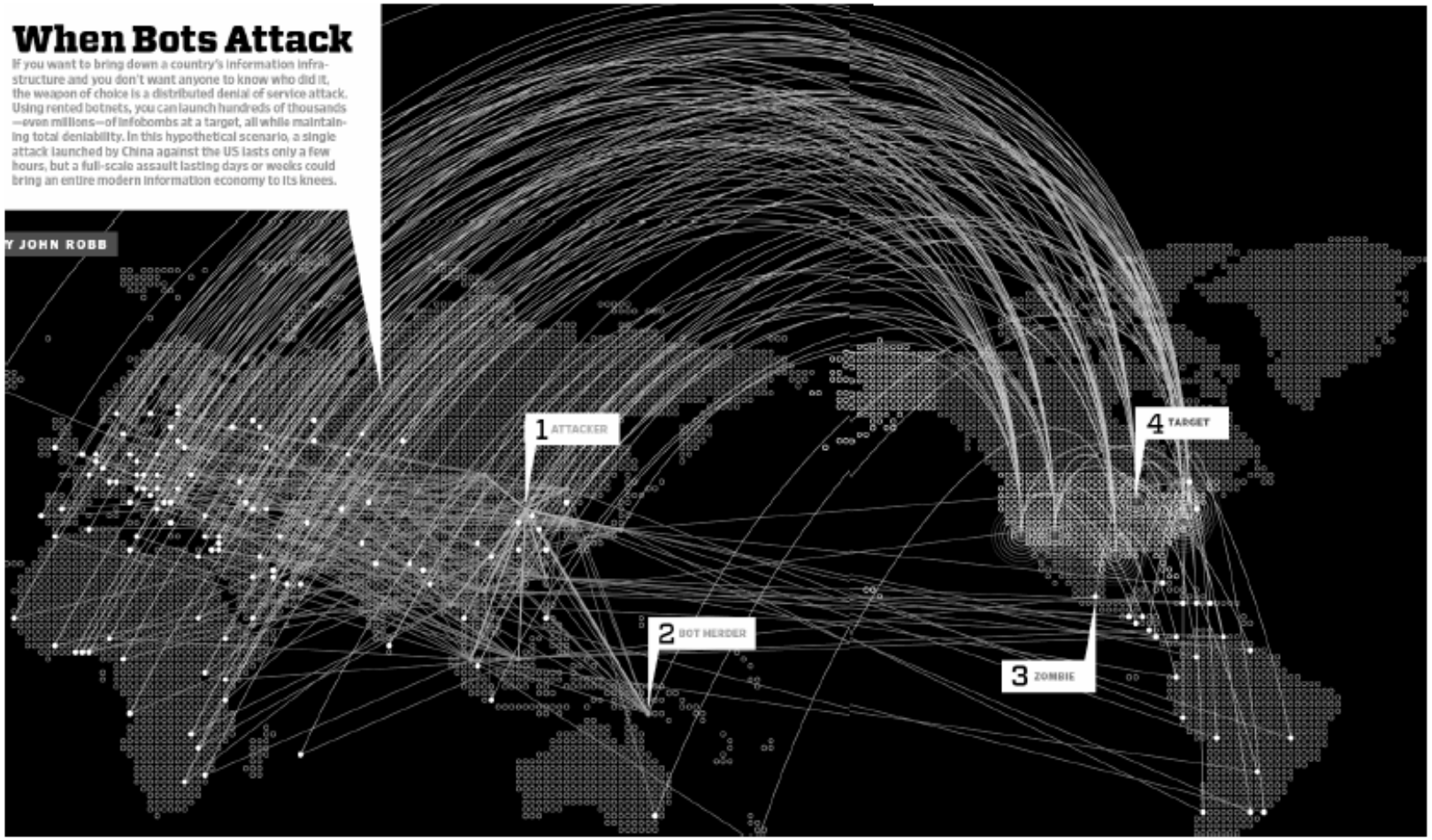
Le hacking (4)

Sont aussi incriminés:

- La tentative
- Les actes préparatoires
  - hackertools – informatiques, ou autres
  - + loi du 12 mai 2003 (dispositifs illicites d'accès à un service protégé de la société d'information)
- Provocation à commettre du hacking
- Recel de données
- Récidive

Le hacking (5)

Exemple :



Le hacking (6)

Exemples :

- Des hackers informatiques qui accèdent au réseau sans fil d'autrui; ils écument un quartier avec leur ordinateur portable en quête d'endroits où l'ordinateur recherche lui-même l'accès à un réseau non protégé et s'y connecte. Ces réseaux sans fil constituent en effet un système informatique au sens de la loi. Si, en plus, l'auteur utilise l'accès au réseau sans fil ainsi obtenu pour surfer sur internet, la circonstance aggravante de l'article 550bis, § 3, 2° du Code pénal est applicable. Le fait que le réseau informatique ne soit pas protégé ne supprime pas le caractère punissable étant donné que le dol général suffit pour le hacking externe.

- Consultation de SMS stockés dans la mémoire d'un GSM

Le hacking (7)

Réfléchir le numérique
Numerama

Accueil | Magazine | Tests | Achats au meilleur prix | Téléchargements | Forums

Vous êtes ici : Numerama > Magazine > Société 2.0

Suicidé, Aaron Swartz devient martyr de la libre diffusion du savoir

Guillaume Champeau - publié le Lundi 14 Janvier 2013 à 09h50 - posté dans Société 2.0

Tweet 97 | +1 26 | J'aime 106 | RSS

Creative Commons, Piratage, Twitter, Wikileaks, Anonymous,

11 commentaire(s)

Pour la famille d'Aaron Swartz, ça ne fait aucun doute. Le jeune homme aurait été poussé au suicide par la pression judiciaire dont il faisait l'objet après avoir piraté une base de données de publications universitaires, dans le but de les rendre accessibles au plus grand nombre. En quelques jours, Aaron Swartz semble en passe de devenir un martyr du combat pour la libération de l'accès aux oeuvres et au savoir.

Le hacking (8)

Cas de jurisprudence 1: Corr. Hasselt, 21 janvier 2004

- Une personne – par ailleurs gestionnaire de réseau – avait remarqué que le système de Netbanking de la Banque DEXIA n'était pas sécurisé. Il pouvait télécharger les listes des bénéficiaires d'autres utilisateurs du Netbanking de la banque, modifier les numéros de comptes bancaires de la liste des bénéficiaires de ces clients et remettre la liste ainsi modifiée sur leur disque dur.
- Lors d'un virement d'un client vers un de ses bénéficiaires, c'est le compte modifié par le pirate qui sera crédité. Pétri de bonnes intentions, ce white hat hacker laissa une trace claire, mais subtile (« calling card »), de son passage espérant que la banque sécurise son système ; Quinze jours plus tard, vu l'absence de réaction de la banque, il la prévint par e-mail de problème de sécurité de son système
- La Banque porta plainte quelques jours plus tard.

4. Le sabotage informatique

Le sabotage informatique (1)

Article 550 ter du Code Pénal :

« 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 est puni d'un emprisonnement…

Si l'infraction est commise avec une intention frauduleuse ou dans le but de nuire, la peine est de…»

Le sabotage informatique (2)

Eléments constitutifs :

- Dol général (celui qui transmet un virus à son insu : non)
- Dol spécial = circ. aggr.
- Pas nécessairement de dommage (= circ. agg.)
- Circonstances aggravantes :
  - Dol spécial
  - Dommage aux données
  - Dommage au système (dommage informatique ou physique)
- Sont aussi incriminés :
  - Dispositifs de sabotage
  - Récidive
  - tentative

Franck Dumortier
Senior Researcher
Centre de Recherches Informatique et Droit (CRID)
franck.dumortier@unamur.be
www.crid.be