www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 juin 2013 T-CY (2013)8F Rev

Comité de la Convention Cybercriminalité (T-CY)

Note d'orientation n° 4 du T-CY
Fraude par usurpation d'identité et hameçonnage

Adoptée lors de la 9e réunion plénière du T-CY (juin 2013)

Contact :

Alexander Seger
Secrétaire du Comité de la Convention Cybercriminalité
Chef de la Division Protection des données et cybercriminalité
Direction générale des droits de l'homme et de l'état de droit
Conseil de l'Europe, Strasbourg, France

Tél. +33-3-9021-4506
Télécopie +33-3-9021-5650
Courriel alexander.seger@coe.int

1 Introduction

Lors de sa 8e session plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, y compris à la lumière des nouveautés juridiques, politiques ou techniques[1].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question de la fraude par usurpation d'identité et hameçonnage (« phishing ») ou par des pratiques analogues[2].

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[3]. Cela vise à garantir que les nouvelles formes de criminalité seront toujours couvertes par la Convention.

Cette note d'orientation montre dans quelle mesure différents articles de la convention s'appliquent à l'usurpation d'identité par voie informatique en lien avec la fraude.

2 Usurpation d'identité et hameçonnage

Il n'existe pas de définition universellement acceptée de ce qui constitue une usurpation d'identité. Malgré le caractère fluctuant de l'usage de cette notion, on entend communément par « usurpation d'identité » des infractions pénales qui consistent à obtenir et à utiliser de façon frauduleuse (à son insu et sans son consentement) les données personnelles d'une autre personne. Le terme « fraude à l'identité » est parfois employé comme synonyme, bien que cette notion englobe également le fait d'utiliser une fausse identité, qui n'est pas forcément réelle.

Les renseignements personnels d'une personne réelle ou fictive peuvent être utilisés à mauvais escient pour commettre de nombreux actes illicites. La présente note d'orientation ne traite cependant que des usurpations d'identité liées à la fraude.

Cela peut impliquer l'appropriation frauduleuse d'informations relatives à l'identité (par exemple nom, date de naissance, adresse actuelle ou adresses antérieures) d'une autre personne, à son insu et sans son consentement. Ces renseignements personnels sont ensuite utilisés pour obtenir des biens et services en son nom.

Ce type d'agissements peut prendre plusieurs formes comme le « phishing », le « pharming », le « spear phishing », le « spoofing » ou toute autre conduite analogue visant, par exemple, à obtenir un mot de passe ou d'autres clés d'accès, souvent par le biais de courriers électroniques ou de sites web falsifiés.

L'usurpation d'identité est un véritable fléau qui touche les gouvernements, les entreprises et les citoyens. Ce phénomène mine la confiance dans les technologies de l'information.

---

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[2] Ces pratiques sont connues sous des appellations diverses : spear phishing ou « harponnage », SMiShing, pharming et vishing.

[3] Paragraphe 36 du rapport explicatif.

La plupart des systèmes juridiques ne prévoient pas de délit spécifique d'usurpation d'identité. Les auteurs d'usurpation d'identité sont normalement inculpés de délits plus graves (comme la fraude financière). L'obtention d'une fausse identité implique normalement la commission d'une infraction, comme la falsification de documents ou l'altération de données informatiques. Une fausse identité facilite la perpétration de nombreux crimes dont l'immigration illégale, la traite des êtres humains, le blanchiment d'argent, le trafic de drogue et la fraude financière contre les gouvernements et le secteur privé, mais est généralement associée à la fraude.

Sur le plan conceptuel, une usurpation d'identité peut se décomposer en trois étapes :

- Phase 1 – L'obtention des renseignements personnels par des moyens divers tels que le vol physique, l'utilisation de moteurs de recherche, des attaques de l'intérieur ou de l'extérieur (accès illicite aux systèmes informatiques, Trojans, « keyloggers », logiciels espions et autres programmes malveillants), ou bien par le recours au hameçonnage ou à d'autres techniques d'ingénierie sociale.
- Phase 2 – La possession et la cession des renseignements personnels (par exemple, la vente de ces informations à des tiers).
- Phase 3 – L'utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions, par exemple en prenant l'identité d'une autre personne pour exploiter des comptes en banque ou des cartes de crédit, ouvrir de nouveaux comptes, contracter des prêts et crédits, commander des biens et services ou diffuser des programmes malveillants.

En conclusion : l'usurpation d'identité (y compris le hameçonnage et les conduites analogues) sert généralement à la préparation de nouveaux agissements criminels, comme la fraude informatique. Bien que l'usurpation d'identité ne constitue pas une infraction en elle-même, les services chargés de l'application des lois peuvent engager des poursuites pour les infractions connexes.

3 Interprétation de la pénalisation de la fraude par usurpation d'identité donnée par le T-CY au regard de la Convention de Budapest

La Convention de Budapest traite avant tout des actes criminels et n'aborde pas expressément les techniques ou technologies employées. En conséquence, elle ne contient pas de dispositions spécifiques relatives à l'usurpation d'identité ou au hameçonnage. Cependant, la pleine application des dispositions de droit matériel de la convention permet aux Etats d'ériger en infraction pénale tout agissement lié à une usurpation d'identité.

La convention fait obligation aux Etats d'ériger en infraction pénale des agissements tels que l'accès illégal à un système informatique, l'interception illégale de données, l'atteinte à l'intégralité des données, l'atteinte à l'intégralité du système, l'abus de dispositifs et la falsification informatique :

Phase	**Article de la convention**	**Exemples**
Phase 1 – Obtention des renseignements personnels	Article 2 – Accès illégal	Lorsqu'un pirate contourne la protection par mot de passe, enregistre les frappes d'un clavier (« keylogging ») ou exploite les failles des logiciels, il est possible d'accéder illégalement à

		l'ordinateur à des fins d'usurpation d'identité ou de hameçonnage. L'accès illégal aux systèmes informatiques figure parmi les infractions les plus communément commises pour obtenir des données sensibles, comme les renseignements personnels.
	Article 3 – Interception illégale	L'usurpation d'identité comporte souvent le recours à des dispositifs de surveillance (« keyloggers ») ou autres types de programmes malveillants pour intercepter illégalement des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique contenant des données sensibles, comme les renseignements personnels.
	Article 4 – Atteinte à l'intégrité des données	L'usurpation d'identité ou le hameçonnage peuvent endommager, effacer, dégrader, altérer ou supprimer des données informatiques. Cela intervient souvent dans le cadre du processus d'obtention d'un accès illégal, moyennant l'installation d'un « keylogger » pour obtenir des données sensibles.
	Article 5 – Atteinte à l'intégrité du système	L'usurpation d'identité ou le hameçonnage peuvent entraver le fonctionnement d'un système informatique pour voler ou faciliter le vol de données à caractère personnel.
	Article 7 – Falsification informatique	L'usurpation d'identité ou le hameçonnage peuvent donner lieu à l'introduction, l'altération, l'effacement ou la suppression de données informatiques, engendrant des données non authentiques qui seront prises en compte ou utilisées à des fins légales comme si elles étaient authentiques. Le hameçonnage est probablement l'illustration la plus courante d'une falsification informatique (page web falsifiée d'un établissement financier par exemple). Cette activité illicite est par conséquent la méthode la plus couramment employée pour obtenir des données sensibles, comme les renseignements personnels.

Phase 2 – Possession et cession des renseignements personnels	Article 6 – Abus de dispositifs	Les données personnelles volées – mots de passe, clés d'accès, cartes de crédit et autres – peuvent être considérées comme la possession d'un « dispositif, y compris un système informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 » de la Convention ou « d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique ».
Phase 3 – Utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions	Article 8 – Fraude informatique	L'utilisation d'une identité frauduleuse pour introduire, altérer, effacer ou supprimer des données informatiques et/ou porter atteinte au fonctionnement d'un système informatique peut servir à exploiter des comptes en banque ou des cartes de crédit, à contracter des prêts et crédits ou commander de biens et services, et peut donc causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique.
Toutes les phases	Article 11 – Tentative et complicité	L'obtention, la possession et la cession de données personnelles peuvent constituer une tentative de commettre plusieurs des infractions spécifiées dans la convention ou de se rendre complice de leur commission.
	Article 13 – Sanctions	L'usurpation d'identité sert à de multiples fins criminelles dont certaines ont une incidence grave sur les personnes et les institutions publiques ou privées. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard de l'usurpation d'identité soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à l'usurpation d'identité « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en

		considération des circonstances aggravantes, par exemple si l'usurpation d'identité porte atteinte à un grand nombre de personnes ou cause un préjudice considérable ou expose une personne à un danger.

4 Déclaration du T-CY

Le T-CY considère que ci-dessus sont illustrées l'étendue et les multiples éléments de pénalisation de l'usurpation d'identité et du hameçonnage ainsi que les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que ces infractions, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

5 Annexe : Extraits de la Convention de Budapest

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a par toute introduction, altération, effacement ou suppression de données informatiques ;
b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.