www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 16 April 2013 (draft for discussion) T-CY (2013)8

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #4

Identity theft and phishing in relation to fraud

Proposal prepared by the Bureau
For comments by T-CY members and observers
And for consideration by the 9th Plenary of the T-CY (June 2013)

Comments on this draft Guidance Note should be sent to:

Alexander Seger
Secretary Cybercrime Convention Committee
Head of Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of identity theft and phishing and similar acts[2] in relation to fraud.

The Budapest Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved".[3] This is to ensure that new forms of crime would always be covered by the Convention.

This Guidance Note shows how different Articles of the Convention apply to identity theft in relation to fraud and involving computer systems.

2 Identity theft and phishing

While there is no generally accepted definition nor consistent use of the term, identity theft commonly involves criminal acts of fraudulently (without his or her knowledge or consent) obtaining and using another person's identity information. The term "identity fraud" is sometimes used as a synonym, although it also encompasses the use of a false, not necessarily real, identity.

While personally identifiable information of a real or fictitious person may be misused for a range of illegal acts, the present Guidance Note focuses on identity theft in relation to fraud only.

This may entail the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name.

Related acts may include "phishing", "pharming", "spear phishing", "spoofing" or similar conduct, for example, to obtain password or other access credentials, often through email or fake websites.

Identity theft affects governments, businesses and citizens and causes major damage. It undermines confidence and trust in information technologies.

In many legal systems there is no specific offence of identity theft. Perpetrators of identity theft are normally charged with more serious offences (e.g. financial fraud). Obtaining a false identity normally implies a crime, such as the forgery of documents or the alteration of computer data. A false identity facilitates many crimes, including illegal immigration, trafficking in human beings,

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

[2] Similar acts to phishing are known under various names such as spear phishing, SMiShing, pharming and vishing.

[3] Paragraph 36 of the Explanatory Report

money laundering, drug trafficking, financial fraud against governments and the private sector, but is most generally seen in conjunction with fraud.

Conceptually, ID theft can be separated into three distinct phases:

- Phase 1 – The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from outside (illegal access to computer systems, Trojans, keyloggers, spyware and other malware) or through the use of phishing and or other social engineering techniques.
- Phase 2 – The possession and disposal of identity information, which includes the sale of such information to third parties.
- Phase 3 – The use of the identity information to commit fraud or other crimes, for example by assuming another's identity to exploit bank accounts and credit cards, create new accounts, take out loans and credit, order goods and services or disseminate malware.

In conclusion: identity theft (including phishing and similar conduct) is generally used for the preparation of further criminal acts such as computer related fraud. Even if identity theft is not criminalised as a separate act, law enforcement agencies will be able to prosecute the subsequent offences.

3 T-CY interpretation of the criminalisation of identity theft in relation to fraud under the Budapest Convention

The Budapest Convention is focusing on criminal conduct and not specifically on techniques or technologies used. It does, therefore, not contain specific provisions on identity theft or phishing. However, full implementation of the Convention's substantive law provisions will allow States to criminalise conduct related to identity theft.

The Convention requires countries to criminalise conduct such as the illegal access to a computer system, the illegal interception of data, data interference, system interference, the misuse of devices and computer related fraud:

Phase	**Article of convention**	**Examples**
Phase 1 – Obtaining of identity information	Article 2 – Illegal access	While a criminal is "hacking", circumventing password protection, keylogging or exploiting software loopholes, the computer may be illegally accessed in the acts of ID theft/phishing. Illegal access to computer systems is one of the most common offences committed in order to obtain sensitive information such as identity information.
	Article 3 illegal interception	ID theft often entails the use of keyloggers or other types of malware for the illegal interception of non-public transmissions of computer data to, from or within a computer system containing sensitive information such as identity information.

	Article 4 – Data interference	ID theft/phishing may involve damaging, deleting, deteriorating, altering or suppressing computer data. This is often done during the process of obtaining illegal access by installing a keylogger to obtain sensitive information.
	Article 5 – System interference	ID theft/phishing may involve hindering the functioning of a computer system in order to steal or facilitate the theft of identity information.
	Article 7 – Computer related forgery	ID theft/phishing may involve the inputting, altering, deleting, or suppressing of computer data with the result that inauthentic data is considered or acted upon as if it were authentic. Phishing is possibly the most common representation of computer related forgery (e.g. a forged web page of a financial institution) and as a consequence the most common illegal activity through which sensitive information is collected, such as identity information.
Phase 2 – Possession and disposal of identity information	Article 6 – Misuse of devices	Stolen identity information – including passwords, access credentials, credit cards and others – may be considered "devices, including a computer program, designed and adapted for the purpose of committing any of the offences established in accordance with articles 2 through 5" of the Convention, or "a computer password, access code, or similar data by which the whole of any part of a computer system is capable of being accessed".
Phase 3 – Use of the identity information to commit fraud or other crimes	Article 8 – Computer related fraud	The use of a fraudulent identity by inputting, altering, deleting or suppressing computer data, and, or interfering with the function of a computer system will result in the exploitation of bank accounts or credit cards, in taking out loans and credit, or ordering goods and services, and thus causes one person to lose property and causes another person to obtain an economic benefit.
All Phases	Article 11 – Attempt, aiding and abetting	The obtaining, possession and disposal of identity information may constitute attempt, aiding and abetting of several crimes specified in the Convention.
	Article 13 – Sanctions	Identify theft serves multiple criminal purposes, some of which cause serious damage to individuals and public or private sector institutions.

		A Party may foresee, however, in its domestic law a sanction that is unsuitably lenient for identity theft, and it may not permit the consideration of aggravated circumstances. This may mean that Parties need to consider amendments to their domestic law. Therefore, Parties should ensure, pursuant to Article 13, that criminal offences related to identity theft "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanction. Parties may also consider aggravating circumstances, for example if identity theft affects a significant number of people or causes serious distress or exposes a person to danger. [4]

4 T-CY Statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of criminalisation of identity theft and phishing.

Therefore, the T-CY agrees that the different aspects of such crimes are covered by the Budapest Convention.

_____

[4] See also Article 10 of the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (com (2010) 517 final).

5 Appendix: Extracts of the Budapest Convention

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally,

an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.