Title | Reporting cybercrimes
--- | ---
Last updated | April 2013
Applies to | All members
Source | Criminal law, especially Chapter 13 of Electronic Communications and Transactions Act 25 of 2002
Note | This advisory is intended to provide guidance on lodging criminal complaints with SAPS and attempting to ensure that these are properly taken up and investigated. ISPA obviously cannot vouch for SAPS’ acts and failures to act.

Introduction

ISPA is receiving a growing number of queries from members and consumers on the correct process to follow when reporting a cybercrime. This Advisory is intended to provide simple advice on lodging a criminal complaint where you or your client is the victim of a cybercrime.

Section 86 of the Electronic Communications and Transactions Act 25 of 2002 ("the ECT Act") sets out criminal provisions relating to unlawful access to or interference with data. Crimes of this nature are often encountered by ISPA members, both directly and indirectly through their clients. Members providing voice services and their subscribers are also frequently the target of various kinds of fraud.

Suggested process

There is no set process: the advice below is based on ISPA’s consultation with senior SAPS personnel.

1. Draft as short and as simple an affidavit as possible which sets out why you believe a criminal act has taken place (you may want to obtain legal assistance to do this). The affidavit should:
   
   1.1. Set out the identity and contact details of the complainant;
   
   1.2. If available, set out the identity and contact details of the alleged perpetrator;
   
   1.3. Set out the facts which led to the complaint being lodged and refer to or incorporate any available evidence such as IP addresses and log files;
   
   1.4. Set out the sections of the criminal law or ECT Act which have been breached. The full text of Chapter 13 of the ECT Act which deals with cybercrime is contained in Annexure A to this Advisory.
   
   1.5. Make a clear statement that you wish the matter to be investigated further and to be kept informed of process.

ISPA Management Committee:
2. Lodge this affidavit with your local police station. Be patient and polite at all times. Due to their workload and priorities the desk officer may not want to receive your complaint: be firmly insistent and ask to escalate the matter internally.

3. Ensure that you obtain a reference or CAS number. This is critical in allowing you to follow the matter up.

4. According to internal SAPS procedure, your complaint should be referred to a duty detective within 24 hours. If possible obtain the name and contact details of this detective, either when lodging the complaint or when following up at a later time.

5. Request that the complaint be escalated to the SAPS cybercrime division as soon as possible. Typically the duty detective should recognise that he or she is not able to investigate the matter and refer it to the cybercrime division.

6. You will need to accept that it is up to you to follow-up and create pressure for the matter to be handled professionally – it is not going to be sufficient to go through the motions of lodging a complaint without actively pursuing the matter.

7. If, despite your best efforts, you are not able to obtain the kind of progress you are looking for, you may choose to consult with a lawyer or send mail to regulatory@ispa.org.za and we will see if we can help with escalation.

Conclusion

ISPA is aware that this process can be difficult given the differing priorities of SAPS and the lack of specific training on cybercrime issues. Nevertheless, the more complaints that are lodged and pursued, the easier the process should become.

Over the past few years there have been an increasing number of convictions in South African courts for cybercrimes and that there are some extremely competent SAPS personnel involved in detecting and prosecuting cybercrimes. There is also a process under way to increase the penalties which may be imposed.

Members are encouraged to provide feedback to regulatory@ispa.org.za on their experiences in reporting cybercrimes so that this advice can be improved over time. ISPA will also engage further with SAPS to try and streamline the process.

Version history

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Version</th>
<th>Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.0</td>
<td></td>
</tr>
</tbody>
</table>

The Internet Service Providers’ Association
queries@ispa.org.za | +27 11 314 7751 | http://www.ispa.org.za | PO Box 3423, Parklands, 2121
Annexure A – Chapter 13 of the Electronic Communications and Transactions Act 25 of 2002

CHAPTER XIII

CYBER CRIME

Definition

85. In this Chapter, unless the context indicates otherwise—
"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Unauthorised access to, interception of or interference with data

86. (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.
(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.
(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.
(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Computer-related extortion, fraud and forgery

87. (1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.
(2) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

 Attempt, and aiding and abetting

88. (1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.
(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

Penalties

89. (1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.
(2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.