

VOLUME: II

CYBERCRIME AND COMPUTER RELATED CRIMES

Part ID: II Offences (ss 4-19)

CHAPTER: 08:06

[Ch0806s4]4. Unauthorised access to a computer or computer system

(1)

Subject to subsections (2) and (3), any person who-

(a) accesses the whole or any part of a computer or computer system, knowing that the access he or she intends to secure is unauthorised; or

(b) causes a computer or computer system to perform any function as a result of unauthorised access to such system,

commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

(2) A

person shall not be liable under subsection (1) where the person-

(a) is a person with a right to control the operation or use of the computer or computer system and exercises such right in good faith;

(b) has the express or implied consent of a person empowered to authorise him or her to have access to the computer or computer system;

(c) has reasonable grounds to believe that he or she had such consent as specified in subparagraph (b);

(d) is acting pursuant to measures that may be taken under Part III of this Act; or

(e) is acting in reliance of any statutory power arising under any enactment or a power conferred under any Act, for the purpose of-

(i) obtaining information, or

(ii) taking possession of any document or other property.

(3) A

person's access to a computer or computer system is unauthorised where the person-

(a) is not himself or herself entitled to access of the kind in question;

(b) does not have consent, from any person who is so entitled, to access of the kind in question; or

(c) exceeds the access he or she is authorised.

(4)

For the purposes of this section, it is immaterial that the unauthorised access is not directed at-

(a) a particular programme or data;

(b) a programme or data of any kind; or

(c) a programme or data held in any particular computer or computer system.

#### [Ch0806s5]5. Unauthorised access to computer service

(1)

Subject to subsection (5), a person commits an offence where such person, knowingly and by any means, without authorisation or exceeding the authorisation he or she is given-

(a) secures access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; or

(b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer or computer system.

(2) A

person who commits an offence under subsection (1) shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(3)

Where, as a result of the commission of an offence under subsection (1), the operation of a computer or computer system is impaired, or data contained in the computer or computer system is suppressed or modified, a person shall on conviction be liable to a fine not exceeding P40,000 or to imprisonment for a term not exceeding two years, or to both.

(4)

For the purposes of this section, it is immaterial that the unauthorised access or interception in subsection (1) is not directed at-

(a) a particular programme or data;

(b) a programme or data of any kind; or

(c) a programme or data held in any particular computer or computer system.

(5) A

person shall not be liable under subsection (1) where he or she-

(a) has the express or implied consent of both the person who sent the data and the intended recipient of such data; or

(b) is acting in reliance of a statutory power arising under any enactment or a power conferred under any Act.

#### [Ch0806s6]6. Access with intent to commit an offence

(1) A

person who, with intent to commit an offence under any other enactment, causes a computer or computer system to perform any function for the purpose of

securing access to-

(a) any programme or data held in a computer or computer system; or

(b) a computer service, commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

(2)

For the purposes of this section it is immaterial that-

(a) the access referred to under subsection (1) is authorised or unauthorised; or

(b) the further offence to which this section applies is committed at the same time as when the access is secured or at any other time.

[Ch0806s7]7. Unauthorised interference with data

(1) A

person who intentionally, without lawful excuse or justification, does any of the following acts-

(a) destroys, deletes, suppresses, alters or modifies data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with-

(i) the lawful use of data, or

(ii) any person in the lawful use of data; or

(d) denies access to data to any person entitled to it, commits an offence and shall on conviction be sentenced to a minimum fine of P10,000 but not exceeding P40,000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

(2)

Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified-

(a) the operation of the computer or computer system;

(b) access to any programme or data held in any computer or computer system; or

(c) the operation of any programme or the reliability of any data,

a person shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(3) A

person shall not be liable under this section where the person-

(a) is acting pursuant to measures that may be taken under Part III of this Act; or

(b) is acting in reliance of any statutory power arising under any enactment or a power conferred under any Act, for the

purpose of-

(i) obtaining information, or

(ii) taking possession of any document or other property.

(4)

An interference is unauthorised-

(a) where the person whose act causes it is not himself or herself entitled to determine whether the interference of the kind in question should be made; or

(b) where the person does not have consent, from any person who is so entitled, to the interference of the kind in question.

(5)

For the purposes of this section, it is immaterial whether an unauthorised interference, or any intended effect of it, is temporary or permanent.

[Ch0806s8]8. Unauthorised interference with a computer or computer system

(1) A

person who intentionally, without lawful excuse or justification-

(a) hinders or interferes with the functioning of a computer or computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer or computer system, commits an offence and shall on conviction be liable to a fine not exceeding P5,000 or to imprisonment for a term not exceeding three months, or to both.

(2)

For the purposes of subsection (1) "hinder", in relation to a computer or computer system, includes-

(a) cutting the electricity supply to a computer or computer system;

(b) causing electromagnetic interference to a computer or computer system;

(c) corrupting a computer or computer system by any means;

(d) inputting, deleting, altering or modifying data; and

(e) impairing, by any means, the connectivity, infrastructure or support of a computer or computer system.

(3) A

person who intentionally, without lawful excuse or justification, commits an act which causes, directly or indirectly-

(a) a denial, including a partial denial, of access to a computer or computer system; or

(b) an impairment of any programme or data stored in a computer or computer system,

commits an offence and shall on conviction be sentenced to a minimum fine

of P10,000 but not exceeding P40,000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

[Ch0806s9]9. Unlawful interception of data

A

person who intentionally and by technical means, without lawful excuse or justification, intercepts-

(a) any non-public transmission to, from or within a computer or computer system; or

(b) electromagnetic emissions that are carrying data, from a computer or computer system,

commits an offence and shall on conviction be sentenced to a minimum fine of P10,000 but not exceeding P40,000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

[Ch0806s10]10. Unlawful possession of devices or data

(1) A

person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(2) A

person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(3) A

person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(4)

For the purposes of subsection (3), "possession of any data or programme" includes-

(a) having possession of a computer or computer system or data storage device that holds or contains the data or programme;

(b) having possession of a document in which the data or programme is recorded; and

(c) having control of the data or programme that is in the possession of another person.

[Ch0806s11]11. Unauthorised disclosure of password

A

person who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system-

(a) for wrongful gain;

(b) for any unlawful purpose;

(c) to overcome security measures for the protection of data; or

(d) with the knowledge that it is likely to cause prejudice to any person,

commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

#### [Ch0806s12]12. Damage to a computer or computer system

(1)

In this section "computer contaminant" includes any programme which-

(a) modifies, destroys, records or transmits any data or programme residing within a computer or computer system;

(b) usurps the normal operation of a computer or computer system; or

(c) destroys, damages, degrades or adversely affects the performance of a computer or computer system or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer or computer system.

(2) A

person who intentionally introduces, or causes to be introduced, a computer contaminant into any computer or computer system which causes, or is capable of causing, damage to such computer or computer system, commits an offence and shall on conviction be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

#### [Ch0806s13]13. Protected computers

(1)

In this section, a "protected computer" means a computer or computer system or programme or data used directly in connection with, or necessary for-

(a) the security, defence or international relations of Botswana;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of the public, including systems related to national emergency organisations.

(2)

Where access to a protected computer is obtained in the course of the commission of an offence under this Act, the person convicted of any such offence shall be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(3)

For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the person referred to in subsection (2) knew that the computer was a protected computer if there was, in respect of the

computer, programme or data-

(a) provision for a warning within the computer, programme or data; or

(b) a warning exhibited to the person to the effect that unauthorised access to the computer, programme or data is prohibited.

[Ch0806s14]14. Cyber extortion

A

person who performs or threatens to perform any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by-

(a) undertaking to cease or desist from such actions; or

(b) undertaking to restore any damage caused as a result of those actions,

commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

[Ch0806s15]15. Cyber fraud

(1) A

person who performs any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

(2) A

person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by-

(a) any input, alteration, deletion or suppression of data; or

(b) any interference with the functioning of a computer or computer system,

commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

[Ch0806s16]16. Electronic traffic in pornographic or obscene material

(1)

In this section-

(a) "publish" includes:

(i) to distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way,

(ii) to have in possession or custody, or under control, for the purpose of doing an act referred to in subparagraph (a), or

(iii) to print, photograph, copy or make in any

other manner (whether of the same or of a different kind of nature) for the purpose of doing any act referred to in subparagraph (a);

(b) "child pornography" includes material that visually or otherwise depicts-

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or

(iii) realistic images representing a child engaged in sexually explicit conduct;

(c) "child" means a person who is under the age of 14 years; and

(d) "sexually explicit conduct" means any conduct, whether real or simulated, which involves-

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic sexual abuse; or

(v) the exhibition of the genitals or pubic area of a child.

(2) A person who-

(a) publishes pornographic or obscene material through a computer or computer system;

(b) produces pornographic or obscene material for the purpose of its publication through a computer or computer system;

(c) possesses pornographic or obscene material in a computer or computer system or on a computer data storage medium;

(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows pornographic or obscene material; or

(e) accesses pornographic or obscene material through a computer or computer system,

commits an offence and shall on conviction be liable to a fine not exceeding P5,000 or to imprisonment for a term not exceeding three months, or to both.

(3) A person who-

(a) publishes child pornography or obscene material relating to children through a computer or computer system;

(b) produces child pornography or obscene material relating to children for the purpose of its publication through a computer or computer system;



(c) possesses child pornography or obscene material relating to children in a computer or computer system or on a computer data storage medium;

(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or

(e) accesses child pornography or obscene material relating to children through a computer or computer system,

commits an offence and shall be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(4) A person who, by means of a computer or computer system, communicates with-

(a) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code; Cap. 08:01

(b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or

(c) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of the offence of defilement or any sexual offence of that person under the Penal Code,

commits an offence and shall be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

(5) Evidence that the person in paragraph (a), (b) or (c) of subsection (4) was represented to the accused as being under the age of 18 years or 16 years, as the case may be, is, in absence of evidence to the contrary, proof that the accused believed that the person was under that age.

(6) It shall not be a defence to a charge under subsection (4) that the accused believed that the person he or she was communicating with was at least 18 or 16 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.

(7) For the purposes of subsection (4), it does not matter that the person in paragraph (a), (b) or (c) is a fictitious person, represented to the accused as a real person.

[Ch0806s17]17. Unlawful disclosure by service provider

A service provider who, without lawful authority, discloses-

(a) that an order under this Act has been made;

(b) any act done under an order; or

(c) any data collected or recorded under an

order,

commits an offence and shall be sentenced to a minimum fine of P10,000 but not exceeding P40,000, or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

[Ch0806s18]18. Attempt

(1) A

person who attempts to commit any of the offences described under this Part, commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

(2)

For the purposes of this section, "attempt" shall have the meaning ascribed to it under section 388 of the Penal Code.

[Ch0806s19]19. Parties to an offence

(1)

Where an offence is committed under this Part, each of the following persons is deemed to have taken part in committing the offence and is deemed to be guilty of the offence, and may be charged with actually committing it-

(a) a person who actually does the act or makes the omission which constitutes the offence;

(b) a person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence;

(c) a person who aids or abets another person in committing the offence; or

(d) a person who counsels or procures any other person to commit the offence.

(2) A

person who counsels or procures any other person to commit an offence may be charged either with committing the offence or with counselling or procuring its commission.

(3) A

conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence.