**Internet & Computer Offenses**

**INTRODUCTION**

Constantly evolving technology has made our business and social practices more efficient and personal. While communicating with friends and family and accessing information easily makes life more enjoyable, this freedom also makes Internet users more vulnerable to cybercriminals. Iraqi Constitution, Iraqi Civil Code 1951, and Iraqi Penal Code No. 111 of 1969 address the dangers associated with the expansion of the Internet and society's dependence upon it. Cybercriminals exploit the Internet through fraud, unsolicited bulk emails (SPAM), phishing scams, child exploitation, etc.

**FRAUD**

The ease and convenience of shopping online have led an increasing number of consumers to purchase goods and services on the Internet. In the process, customers transmit personal information. such as bank account number/s or debit card/s information, through cyberspace. While some of these websites are safe and serve their purpose well, others either do not have the proper security measures or present a fraudulent front with the sole purpose of gaining personal information.

**PHISHING**

Phishing involves sending unsolicited emails in an attempt to capture personal information such as debit card information, bank account numbers, passwords, and other information. A typical phishing email might appear as if it is sent from a company you deal with and may say that you must update your account information by clicking on a link in the email. The email will look authentic and have a visible email address claiming to be from a financial institution or other legitimate company, as well as graphics that resemble the company’s website. The information you input does not go to the purported company but will be routed to an identity thief.

**CHILD EXPLOITATION**

The same advances in technology that allow our children to expand their realm of knowledge are also leaving them vulnerable to exploitation and harm by computer sex offenders. Internet content filters can protect children while they use the Internet.

Signs your child may be at risk include:

* Child has a computer with Internet access in his or her room;
* Child has a webcam on your computer;
* Child spends large amounts of time online, especially at night;
* Pornography or obscene material is discovered on the child’s computer;
* You notice a child may receive phone calls from adults;
* Child receives mail, gifts, or packages from someone you don’t know;
* Child turns the monitor off or quickly changes the screen on the monitor when you come into the room;
* Child becomes withdrawn from family; and
* Child uses an online account belonging to someone else; check your Internet history files or ask your child.

**UNSOLICITED BULK E-MAIL**

Unsolicited bulk e-mail, sometimes referred to as “UBE” or “SPAM,” is an email that is sent for the purpose of selling goods, services, or properties. Commercial UBE advertisements are most often used for multi-level marketing schemes, get-rich-quick schemes, work-at-home schemes, or questionable products or pornography.

Tips to prevent SPAM include:

* If you have doubts about the authenticity of the sender and/or the content, do not respond.
* Get a free email account specifically for newsgroups and registering on websites.
* Do not post your actual email address on your website; spammers have programs that can scan web pages for an email address.
* Use mail filters. They are not always completely accurate, but they can decrease the number of junk emails you receive.

**Harassment through e-mails or phone texts**

Sending threatening, unsolicited, obnoxious, or sexually explicit messages to others by email or texts is a form of harassment. Never send anyone an email or text message containing things you wouldn't say in person.

What is considered humorous to some people, others may consider offensive or even frightening. Email or phone text messages that amount to harassment violate ethical usage of your computer account, and in some extreme cases may even provoke victims to press criminal charges.

**Dissemination of obscene material on the Internet**

A person is guilty of disseminating obscene matter if s/he distributes, exhibits, or offers to distribute or exhibit any obscene matter.

Cyber Defamation refers to any false statement that causes damage to a person’s reputation. Libel is a false statement in written form that destroys a person’s reputation. This could be a blog comment, an article published on the media, a post published on social networks, or an online review.

The law protects opinion statements against defamation lawsuits. But sometimes, things can be tricky when people use “opinions and free speech” as obvious means to defame others.

**Hacking**

Hacking is the use of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.

Some hackers hack for personal monetary gains, such as stealing credit card or debit card information or transferring money from bank accounts to their own. They also indulge in extortion based on information received while hacking a particular network of computer systems.

**Identity Theft**

Identity theft is a form of fraud in which someone pretends to be someone else by assuming that person’s identity, typically in order to access resources or obtain credit and other benefits in that person’s name.

Whoever, fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person is known as identity theft.

**Cyber-stalking**

It is the use of the internet, e-mail, or other electronic communications devices to stalk another person. Stalking involves harassing or threatening behavior that an individual engages in repeatedly.