**Ethical and Security Issues in Information Systems**

Table of Contents

[Information Systems 2](#_Toc63380029)

[Dimensions of Information Systems 2](#_Toc63380030)

[The Evolution of Information Systems 3](#_Toc63380031)

[Risks of Information Systems 4](#_Toc63380032)

[Cyber Crime 4](#_Toc63380033)

[Identity Theft 5](#_Toc63380034)

[Copyright Infringement 5](#_Toc63380035)

[Click Fraud 5](#_Toc63380036)

[Advance Fee Fraud 6](#_Toc63380037)

[Hacking 6](#_Toc63380038)

[Computer Viruses 6](#_Toc63380039)

[Solutions to Information Security Threats 7](#_Toc63380040)

[Information Systems Ethics 9](#_Toc63380041)

## Information Systems

Information systems are combinations of hardware, software and telecommunication networks that allow organizations to collect, create, use and distribute data. Banks, online shops, etc. all have information systems. Information systems exist to aid us in decision making, coordination, control, analysis and visualization.

Consider how a university would allow students to apply. Students would apply with their grades, the university would need to store all of their data and finally a system would sort out the most eligible students and publish a list of those accepted to the university. An information system would deal with how to actually make this process happen. Additionally, it would make the process more efficient compared to manually doing all the work.

### Dimensions of Information Systems

There are three main dimensions of an information system:

* Technology – This includes the hardware, software, data and networking communication involved in an information system.
* People – This includes everyone in the organization, from the front-line help-desk workers to system analysts, programmers and the Chief Information Office (CIO). Even if they are not directly involved with the information system, everyone has a role to play in the organization and the organization would be unable to function properly without them.
* Organizations – This refers to the actual organization that owns the information system and the organizational processes involved. An organizational process is a series of steps undertaken to achieve a desired goal. The example we saw earlier of the application process in a university is an organizational process. Information systems exist to make these processes more efficient and more productive and allow the organizations to have more control over the process.

### The Evolution of Information Systems

|  |  |  |  |
| --- | --- | --- | --- |
| Era | Hardware | Operating System | Applications |
| Mainframe (1970s) | Terminals connected to mainframe computer | Time-sharing (TSO) on MVS | Custom-written MRP software |
| PC (mid-1980s) | IBM PC or compatible. Sometimes connected to mainframe computer via expansion card. | MS-DOS | WordPerfect, Lotus 1-2-3 |
| Client-Server (late 80s to early 90s) | IBM PC “clone” on a Novell Network | Windows for Workgroups | Microsoft Word, Microsoft Excel |
| World Wide Web (mid 90s to early 2000s) | IBM PC “clone” connected to company intranet | Windows XP | Microsoft Office, Internet Explorer |
| Web 2.0 (mid-2000s to present) | Laptop connected to company Wi-Fi | Windows 7 | Microsoft Office, Firefox |
| Post-PC (today and beyond) | Apple iPad | iOS | Mobile-friendly websites, mobile apps |

The table above gives some information about the hardware, operating systems and applications available in different eras of technology.

## Risks of Information Systems

Even though information systems have made many businesses wildly successful, their improper use can create problems for organizations, employees and even the general public.

A few abuses of information systems that we will be looking into are:

* Cyber Crime
* Identity Theft
* Copyright Infringement
* Click Fraud
* Advance Fee Fraud
* Hacking
* Computer Viruses

### Cyber Crime

Cyber crime is a category of crimes where information technology is used to commit the crimes. It can range from annoying people to causing huge financial loss or even murder.

The growth of high-end mobile devices with internet access has led to a significant rise in cybercrimes.

### Identity Theft

Identity theft is one of the cybercrimes. It refers to a criminal impersonating another person or entity. This is usually done by using their personal details.

Personal details can be obtained in many ways. Something as simple as shoulder surfing, where another person takes a peek over your shoulder to see your password or other person details, can allow them to obtain this information. Another method is called phishing, where fake websites, emails or public networks (hotspots) are created and made to look like their legitimate counterparts in the hope that people will be unable to tell the difference and will willingly give up their personal details.

### Copyright Infringement

Copyright infringement in general refers to the unauthorized use of copyrighted material. Simply put, copyright infringement refers to piracy. Websites like The Pirate Bay are used to distribute copyrighted material like music, movies and software.

### Click Fraud

Advertising companies like Google AdSense offer pay per click advertising services. Click fraud is when someone clicks advertises repeatedly so as to drive up advertising costs for the companies using the service and skew their user data. Automated software is used to do this.

### Advance Fee Fraud

This is anything that asks you for money by making a promise that you will get something later on. Nigerian prince email scams basically.

### Hacking

Hacking is when someone by-passes security controls to gain unauthorized access to a system. They can then install programs that allow them to spy on the user or control the system remotely. Other objectives include defacing websites, stealing sensitive information, etc. Essentially most of the other types of crimes we learnt about above can be achieved by hacking into systems.

### Computer Viruses

Viruses are unauthorized programs that can be used to annoy users, steal sensitive data or control the computer and any equipment connected to the computer.

## Solutions to Information Security Threats

The first step falls on the user. We have to protect our devices from unauthorized access. The general username/password combination is old and hackers have gotten really creative about how to obtain this information. Unless someone is extremely careful, this stuff is easy to obtain.

A far better security measure is to use two-factor authentication, where a one-time password (OTP) is sent to a connected device, like a phone, and that password must be entered whenever logging in. There are even physical devices that generate OTPs that are given to you so as to avoid the risk of an SMS or email with an OTP being intercepted. The concept of an OTP falls into the category of something you know, something you have, which refers to the main password (that you know) and the OTP (which comes to your smartphone, a device you physically have on you) respectively.

Beyond this, there are other security measures that can be taken which are a little more complicated.

Anti-viruses can of course be used, which should keep us safe from viruses in most cases. Even Windows Security has gotten really good at this.

A network firewall is also great. Corporations tend to use this rigorously, but the average Joe should also learn about it and use it.

Data encryption can help keep data secure from prying eyes. Some services like [mega.nz](http://mega.nz/) use this. There is also a host of other software we can use to manually encrypt our data.

A physical security key can help protect your actual computer. Your laptop should have a tiny slot on the side where you have to put in a small plastic device that works as a key. Only with that key can you unlock the device.

Finally, we have biometric authentication. This involves scanning your fingerprint, your eye or your face. Smartphones have begun using this increasingly. This is a new concept that goes into something you know, something you have and something you are (your fingerprint being the part you are). However, it is a bit risky because, if that data gets stolen, you can’t exactly replace your fingerprint.

## Information Systems Ethics

The British Computer Society (BCS) Code of Conduct covers the following four key principles for IT professionals:

* “You make IT for everyone”, referring to the fact that work in the IT field must be done in public interest, not self-interest.
* “Show what you know, learn what you don’t”, which basically means don’t be a egotistical show-off. Don’t pretend to know things you don’t.
* “Respect the organization or individual you work for”, which we covered much earlier.
* “Keep IT real. Keep IT professional. Pass IT on”, which is less meaningful and more cool sounding.

Other codes of conduct include:

* The ACM Code of Ethics and Profession Conduct, which can be found [here](https://www.acm.org/code-of-ethics).
* The IEEE Code of Ethics, which can be found [here](https://www.ieee.org/about/corporate/governance/p7-8.html).