Towards a computer security induction manual for non-IT citizens

Louise Kriel¹,², M Loock¹, E Kritzinger¹ & E Smith¹
Unisa, School of Computing¹
Defence, Peace, Safety & Security, Council for Scientific and Industrial Research²

Abstract
In a technical and research environment the risks associated with the conduct of non-technical employees can be managed by implementing guidelines concerning the correct use of company computers and network access. This article will therefore consider good computer practice for new and non-technical employees. It will further give information relating to the underlying computer security risks associated with common office practices, and offer a quick reference guide for employees.

The reader is provided with a brief summary of many of the more common forms of computer intrusion and the threats posed by malicious software, as well as the various ways in which network access is gained. Actions that can lead to increased risk are also discussed. Since technology advances result in a rapidly changing environment, with new intrusion methods regularly being devised, the aim is not to provide a comprehensive overview, but rather to sensitize employees to good computer ethics and make them more aware of the inherent risks associated with certain actions.

Keywords
information, computer security, non-technical, password, phishing, malware, network, software

1 Introduction
In any environment in which there is information that can be utilized and exploited by other parties, security and the protection of information are important. This holds especially true in a technical and research environment. One of the biggest potential
threats to information security is the people who operate the computers. The potential risk is exacerbated by the ignorance and the conduct of non-technical employees. Computer risks are not limited to a corporate environment, but also apply to any computer or digital interface used by any person. It is therefore necessary to educate computer users about the potential risks associated with specific actions performed on computers. This article will examine computer risks identified within the corporate environment; these, however, are also applicable to all citizens using computer technology.

2 Problem statement and objective

In a technology-dependent environment, information is of paramount importance, and many employees are linked to different networks. This makes the management of security more difficult, since the potential access points increase exponentially. When employees are not appropriately trained to understand information security risks, they may endanger the rest of the network. The need for a quick reference manual and induction booklet for non-information technology (IT) employees in an IT environment was identified.

This article serves as research input for a manual of this kind. To manage the risks associated with negligence or lack of technological knowledge, we will identify and discuss some common risks to computer technology to be included in a guidance manual of this nature, which would also contain guidelines on how to minimize these risks. The concept of computer security in general will be briefly discussed in the next section.

3 Computer security

Although the term “computer security” is used frequently, a standalone computer is often less vulnerable than a computer connected to a network. As the use of computer networks, especially the internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources.

The interpretation of an aspect in a given organizational environment is dictated by the needs, customs and laws of a particular organization (Bishop, 2003). Computer security depends on confidentiality, integrity and availability, represented by the acronym CIA.

- **Confidentiality** means that information cannot be accessed by unauthorized parties, and can be considered secret or private. A secure computer system must not allow
information to be disclosed to anyone who is not authorized to access it (Lehtinen, Russell & Gangemi, 2006). The repercussions of a breach in confidentiality can range from the embarrassing to the disastrous.

- **Integrity** refers to the trustworthiness of information resources and the protection of information against unauthorized changes. Hacking compromises the integrity of databases and other resources.

- **Availability** refers to the ability to use information or resources desired. The deliberate arrangement of denial of access to data, called “denial of service attacks”, is sometimes the topic of national news.

Of importance for computer security are access control and non-repudiation. Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access. Non-repudiation implies that a person who sends a message cannot deny having sent it and, conversely, that a person who has received a message cannot deny having received it. This is essential in business transactions, as it provides the necessary proof should dispute resolution become necessary (Hang, Li & Lee, 2004).

In addition to these technical aspects, the conceptual reach of computer security is broad and multifaceted. Computer security draws from disciplines such as ethics and risk analysis, and is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and identity and anonymity in cyberspace (Kinkus, 2002). The next sections will discuss topics deemed important for non-IT employees working with computer technology.

### 4 Information security

As opposed to computer security management, in the context of which confidentiality, integrity and availability are the most important concerns, internet users often regard privacy as the most important aspect of computer security (Harris Interactive & Westin, 2000; Meinert, Peterson, Criswell & Crossland, 2006).

Although users may feel that they have nothing to hide when they are registering on an internet site or service, privacy on the internet is about protecting one's personal information, even if the information does not seem sensitive. Many people prefer to have
control over what information is collected about them, how it is used, who may use it, and what it is used for (Meinert et al., 2006; Harris Interactive, 2002).

More companies store business and individual information on computers than ever before. Much of the information stored is highly confidential and not for public viewing. Many businesses are based solely on information stored in computers. The personal details of staff, client lists, salaries, bank account details, and marketing and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate, and to protect this information, information security systems must be implemented.

Breaches of information security can be divided into five categories:

1. Interception of messages;
2. Theft of stored data;
3. Information sabotage (ie alteration or destruction of data belonging to another party);
4. Spoofing (ie using stolen information to pose as somebody else);
5. Denial of service (ie deliberate shutdown of cash machines, electric-supply grids, air-traffic control networks, and so on).

Individual computer experts ("hackers"), intelligence agencies, criminals, rival businesses, disgruntled employees and other parties may all seek to breach information security, and thus gain access to information.

Effective information security systems incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners alone are not sufficient to protect information; a set of procedures and systems is necessary to effectively deter access to information (Crystal, 2010).

5 Data storage and backup
Backup tools for enterprise data storage systems include data replication, snapshots, data backup and recovery reporting, backup testing and other backup software. Backing up online is becoming one of the more favored options.
6 Computer ethics

Ethics, in the classical sense, refers to the rules and standards governing the conduct of an individual in relation to others. As technology and computers became more and more a part of our everyday lives, it must be understood not only that the problems that have in the past plagued business and conduct will continue to be a problem, but also that a new medium may in fact give rise to increasingly difficult questions of judgment. Therefore, since the introduction of the world wide web (WWW), the definition of ethics has had to evolve, and a new type of ethics, known as computer ethics, has emerged.

According to Moor (1985), computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology. Computer ethics has become necessary for the following four reasons:

- The growth of the WWW has resulted in a number of new legal considerations.
- New questions are being asked to which older laws do not hold the answers.
- Traditional laws are outdated/anachronistic in this world.
- A more coherent body of law is needed to govern the internet and computers.

Three of the more pressing concerns in computer ethics today are questions of copyright, privacy, and censorship (Oracle Think Quest, 1999).

7 Office information discipline

There are two prerequisites for the success of overall information security discipline:

i. The people who are expected to maintain and monitor information security in the company need to know what is expected and demanded of them.

ii. The employees of a company may be viewed as the first line of defense when it comes to the early detection of problems. Consequently, employees at all levels of the company must be made aware of the pivotal role played by security and specifically information security within a company. They need certainty on what their responsibility for information security within the company is, and what will happen if they do not perform their security duties (Etsebeth, 2006).

Therefore, the purpose of office discipline and usage policies is to help ensure an information infrastructure that supports the mission of the company. Computers and
networks are powerful enabling technologies for accessing and distributing information and developed knowledge. As such, they are strategic technologies for the current and future needs of the company. As these technologies leverage each individual's ability to access and copy information from remote sources, users must be mindful of the rights of others to privacy, intellectual property and other rights. The usage policy codifies what is considered appropriate usage of computers and networks in terms of the rights of others. With the privilege of using the information resources of a company comes the specific responsibility outlined a policy of this nature.

8 Hardware security

According to a study released in 2000 by the Federal Bureau of Investigation and the Computer Security Institute, over 70% of all attacks on sensitive data and resources reported by organizations occurred from within the organization itself. Implementing an internal security policy appears to be just as important as an external strategy. All computers have a BIOS that controls system resources on the hardware level. BIOS passwords prevent malicious users from booting the system, deterring the user from quickly accessing or stealing information stored on the hard drive.

If a computer is stolen (the usual victims of theft are frequent travelers who carry laptops and other mobile devices) and disassembled, the computer’s BIOS password does not prevent the attacker from removing the hard drive. If this is installed in another computer without BIOS restriction, the hard drive can be read. It is therefore recommended that workstations have locks to restrict access to internal hardware. Hardware such as lockable steel cables can be attached to computer and laptop chassis to prevent theft, and key locks on the chassis itself may prevent internal access (Red Hat, 2002).

9 Security attacks

9.1 Social engineering

In computer security, social engineering is a term that denotes a non-technical type of intrusion that relies heavily on human interaction, and often involves tricking other people so as to evade normal security procedures. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an
organization or its computer systems (Perrin, 2010). There is general consensus that social engineering is a hacker’s clever manipulation of the natural human tendency to trust.

The hacker’s goal is to obtain information that will allow him or her to gain unauthorized access to a valued system and the information that resides on it (Goodchild, 2010). For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem: social engineers often rely on the natural helpfulness of people in addition to their weaknesses.

An appeal to vanity, an appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person or researcher, and may even offer credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and make use of the information gained from the first source to add to his or her credibility.

Social engineering also relies on people's inability to keep up with a culture that depends heavily on information technology. Social engineers capitalize on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Frequently, social engineers will search dumpsters for valuable information (see section 9.6 below), memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed. Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system. Prevention includes educating people about the value of information, training them to protect it, and increasing their awareness of how social engineers operate.
A specific pattern is often identifiable in social engineering. This consists of the four phases of information gathering, relationship development, exploitation, and execution (Allen, 2006), illustrated in figure 1.

![Figure 1. The four phases of social engineering]

9.1.1 Phishing
Phishing is a social engineering technique by means of which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity (Kumaraguru, Rhee, Acquisti, Cranor & Hong, 2007). It is an e-mail fraud method in which the perpetrator sends out apparently legitimate e-mail in an attempt to gather personal and financial information from recipients. Phishing attacks use e-mail or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send e-mail from what appears to be a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as
• natural disasters (eg Hurricane Katrina)
• epidemics and health scares (eg H1N1)
• economic concerns (eg revenue scams)
• major political elections
• holidays

9.1.2 How to avoid becoming a victim
A number of precautions can be taken to avoid becoming a victim of this form of social engineering.

• Be suspicious of unsolicited phone calls, visits or e-mail messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

• Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

• Do not reveal personal or financial information in e-mail, and do not respond to e-mail solicitations for this information. This includes following links sent in e-mail.

• Do not send sensitive information over the internet before checking a website's security.

• Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (eg .com vs .net).

• If you are unsure whether an e-mail request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.

• Install and maintain anti-virus software, firewalls and e-mail filters to reduce some of this traffic.

• Take advantage of any anti-phishing features offered by your e-mail provider and web browser (McDowell, 2004; Broersma, 2006).
The guidelines given above also offer protection against smishing, another form of social engineering, which is discussed in the section below.

9.1.3 Smishing
Smishing (short for “SMS phishing”) is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his or her cellular (cell) phone or other mobile device.

A cell phone user may, for instance, receive an SMS message saying something like this: “You have been selected to participate in the Vodamail weekly lotto draw. Participation is R3.50 per week. If you do not wish to participate or receive further invitations to participate, please decline. Please visit: www.vodacon.co.za.” While some might recognize this as a scam, many unsuspecting users would not. Fearful of incurring unwanted cell phone costs, they visit the web site supplied in the message. Once they arrive at the URL, they may unknowingly download a program that is in fact a Trojan horse that turns control of the computer over to the hacker. The computer can then be used to launch denial of service attacks, install keylogging software, steal personal account information, and carry out other malicious activities.

9.2 Password security
Passwords are the primary way that the system verifies that the user logging in is who he or she claims to be. This is why password security is enormously important for the protection of the user, the workstation and the network. The single most important thing a user can do to protect his or her account is create a strong password, in that way making it less susceptible to a password cracking attack.

9.2.1 Guidelines for creating strong passwords
When creating a password, it is a good idea to follow the guidelines given below (Natarajan, 2008; Bradley, 2010):

- Make the password at least eight characters long – The longer the password, the better.
- Mix upper and lower case letters.
• **Mix letters and numbers** – Adding numbers to passwords, especially in the middle (not just at the beginning or the end) can enhance password strength.

• **Include non-alphanumeric characters** – Special characters such as &, $, and > can greatly improve the strength of a password.

• **Pick a password you can remember** – The best password in the world serves no purpose if you cannot remember it. Use acronyms or other mnemonic devices to aid in memorizing passwords.

• **Do not use only words or only numbers.**

• **Do not use recognizable words** – Words such as proper names, dictionary words or even terms from television shows or novels should be avoided, even if they are bookended with numbers.

• **Do not use words in foreign languages** – Password cracking programs often check against word lists that encompass dictionaries of many languages.

• **Do not use hacker terminology** – Hacker terminology, also called l337 (LEET) speak, is included in many word lists.

• **Do not use personal information** – Personal information should never be used as a part of your password. If the victim is known to the attacker, it is easier to guess the password from personal information such as the victim's name, family names, pet’s name, dates of birth and phone numbers.

• **Do not invert recognizable words** — Good password checkers always reverse common words, so inverting a bad password does not make it any more secure.

• **Do not write down passwords** – Never store passwords on paper; it is much safer to memorize them.

• **Do not use the same password for all machines** – It is important to create separate passwords for each machine. This way the risk to other machines and systems is limited.

With all these rules, it may seem difficult to create a password meeting all of the criteria for a good password while avoiding the traits of a bad one. Fortunately, there are some simple steps one can take to generate a memorable, secure password.

**9.2.2 Methods for creating strong passwords**

There are many methods for creating secure passwords. One of the more popular methods involves acronyms. For example:
• Think of a phrase, such as: "Over the hills and far away, to grandmother’s house we go".

• Turn the phrase into an acronym (including punctuation): othafa, tgmhwg.

• Complexity can be enhanced by substituting numbers and symbols for letters in the acronym, for example, substitute 7 for t and the @ for a: o7h@f@,7gmhwg.

• Add more complexity by capitalizing at least one letter, such as the h: o7H@f@,7gmHwg.

The disadvantage of this method is that there is little logic to assist with remembering the final password and people will be inclined to write it down, creating a different vulnerability.

9.2.3 Password aging

Password aging is another technique used by system administrators to defend against bad passwords within an organization. Password aging means that after a set length of time, usually 90 days, the user will be prompted to come up with a new password. The theory behind this is that if a user is forced to change his or her password periodically, a cracked password is useful to an intruder for only a limited period. The disadvantage of password aging, however, is that users are more likely to write their passwords down (Fedora Documentation Project, 2009).

9.3 Information security incidents

An information security incident is an event which may compromise the confidentiality, existence, accuracy or availability of stored information. The computer user is responsible for complying with the regulations and for reporting security breaches.

Examples of security incidents include:

- someone has accessed a user’s account using his or her username and password;
- files are missing from a user’s home directory or files have been changed without his or her knowledge;
- a virus infection that was not detected and cleaned automatically.

If a user becomes aware of any security incident that affects him or her or his or her colleagues, this must be reported immediately. The incident should then be logged and
passed to the information protection and security manager for evaluation and possible further action.

### 9.4 Defining threats

In order to be alert to the different ways in which a computer can be compromised, it is helpful to have an understanding of the different potential threats, how they are grouped and their basic function, as summarized below:

i. **Malware** – Programming or files developed for the purpose of doing harm (malicious code).

ii. **Virus** – Malicious computer code sent to another computer.

iii. **Trojan** – A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and do its chosen form of damage, such as ruining the file allocation table on the hard disk.

iv. **Adware** – A software application in which advertising banners are displayed while the program is running.

v. **Spyware** – A nefarious form of data collection technology that gathers private and personal information about a user or organization without his, her or its knowledge or consent. It usually lives on the internet in the form of a virus and installs malicious code on a computer without the user’s knowledge when he or she clicks on a link in an e-mail or web browser pop-up window.

vi. **Worm** – Self-replicating malicious code that does not alter files, but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

vii. **Data miner** – In a malware context, a program that tracks and processes data about the user's browsing behavior for marketing purposes.

viii. **Executable** – A type of file containing a program that will start it running; viruses are often sent in executable files that will run when the user opens the file.

ix. **Key logger** – A type of spyware program that records the user's keystrokes invisibly and either transmits them to the attacker on an ongoing basis or saves them to a secret file in the user's computer, to be sent at a later time.
The various forms of malware are used to achieve various nefarious aims. It is therefore important for any computer user to be alert to the threat they pose. Identity theft, discussed below, is an example of where information harvested by means of one or more of the above can be used to achieve this aim.

9.5 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. The victim of identity theft (the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Both organizations and individuals who are duped or defrauded by the identity thief can suffer adverse consequences and losses, and both can be considered victims.

Identity theft is often the result of phishing, smishing and dumpster diving, and guidelines against these will help prevent identity theft.

9.6 Dumpster diving

Dumpster diving refers to people going through rubbish bins in the hope of finding paper records reflecting valuable information, such as customer names or future product plans. This problem is growing with the increased use of USB flash drives and portable music players (Valli & Jones, 2005). Every user who throws away (or loses) a flash drive could be unintentionally leaking critical information to a competitor. Any of the tens of millions of desktop and notebook computers disposed of each year in landfills, junkyards and yard sales could be a rich trove of corporate data left on a hard drive by lazy users or IT departments (Muller, 2010; Scheier, 2007; Pensten, 2010). Studies in Australia (Valli, 2004) and the United Kingdom (Jones, Mee, Meyler & Gooch, 2005) indicate that a broad cross-section of organizations are failing to adequately protect or erase confidential data stored on hard disk drives before subsequent disposal.

Dumpster diving is a way of gathering a lot of information quickly (Freier, Karlton & Kocher, 1996). IT managers must ensure that sensitive data is not disposed of in a retrievable manner in the rubbish or anywhere else. Tools ranging from low-cost or free disk-wiping software to low-cost encryption and more-expensive "disintegration"
machines for disk drives are available for any IT manager with the will and awareness to use them.

Handheld computing and communications devices such as BlackBerries and PDAs can, via e-mail, funnel sensitive data out of the organization or let viruses or other malware in. The easiest and least expensive technology for protecting digital information is encryption. Modern encryption software is inexpensive and easy to use and is capable of protecting virtually any organization against the theft of data on devices after they have been disposed of or if they are lost or stolen (Scheier, 2007).

10 Conclusion
Kocher (2006) makes the observation that the most important way of ensuring that information is protected is by making sure that the staff appointed can be trusted and that they are educated properly. According to his research, 40% of security breaches are attributable to current or former employees rather than outside hackers, and if malicious employees have access to sensitive data, no technical solution will provide absolute protection. The solution to the problem posed is therefore clearly two-fold: appoint the right people, and train them in order to equip them to deal with any threat to computer safety. An induction manual, of which this article forms the basis, provides the second part of the solution and will be developed expressly to provide non-IT citizens with the basic information that will enable them to manage their IT risk profile.

REFERENCES


