GUIDELINES FOR PREVENTING IDENTITY THEFT

INFORMATION COMMISSIONER

The purpose of the document:	The Guidelines provide a complete outline of the identity theft subject matter; they discuss the meaning of identity theft, different types of identity theft, legal regulation in the Slovene legislation, the ways identity thieves gather personal data and, among other things, the practical measures to prevent identity theft.
Target publics:	Individuals.
Status:	Public.
Version:	1.0
Dated:	1 April 2010
Author:	Information Commissioner RS.
Key words:	Guidelines, identity theft, phishing, pharming, social engineering, virus, worm, spyware, adware, copying of personal identity documents, password, Penal code, complaint, civil action.

Translation and design of the e-brochure was kindly supported by the European Commission as part of their ICT-Policy Support Programme under Project No. 225044.

CONTENTS

ABOUT GUIDELINES

The purpose of the Information Commissioner's guidelines is to provide common practical instructions and procedures for data controllers and individuals in a clear and appropriate manner. It seeks to address the most common questions from the area of personal data protection that different data controllers are faced with. With the help of such answers and guidelines, companies and data controllers should accordingly be able to comply with the statutory provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 – official consolidated text; hereinafter: ZVOP-1).

The legal basis for the Information Commissioner (hereinafter: the Commissioner) to issue the guidelines is provided by Article 49 of the ZVOP-1 which stipulates that the Commissioner shall give non-binding opinions, explanations and positions regarding personal data protection, and, further to this, publish these on its website or in other suitable formats, as well as prepare and offer instructions and recommendations regarding personal data protection in individual areas.

See also:

- Commissioner's opinions: http://www.ip-rs.si/index.php?id=383
- Commissioner's brochures: http://www.ip-rs.si/index.php?id=388
- The Commissioner's Guidelines are published on the website: http://www.ip-rs.si/index.php?id=491

INTRODUCTION

People own many things. These things can be bought, inherited or bestowed; they may carry a monetary or sentimental value. We may lose things, bestow them, they may be seized or even stolen from us. But one of our most cherished personal things that can be stolen from us is our personal identity. Due to the ever-increasing virtual activities that we partake in, identity theft is becoming an urgent problem.

The fastest developing type of criminal activity in the last decade is known to be identity theft. Using someone else's name, address, unique personal identification number (e.g. SSN) or – even better – a bank account number or credit card number a criminal can swiftly perform a financial transaction, hire a loan, buy merchandise for larger amounts of money, take a mortgage on the victim's house, buy property or gain certain rights (e.g. the right to enter premises). Identity thieves may obtain information about a bank account number in numerous different ways; research shows that as many as 46 % of such thefts occur as a result of a forgotten credit card or some similar way of obtaining bank account information. Thieves can, for example, sift through garbage and obtain data from discarded bills. They can brake into a mail box or redirect mail to their address with a demand for a "temporary change" of the victim's address so that they can obtain the data needed for their bad intentions.

The Information Commissioner has dealt with a case where a person forged another person's signature and demanded an itemised telephone bill on his behalf from a telephone operator. The perpetrator later broke into the victim's mail box and thus obtained a list of telephone numbers often contacted by the victim. It continued with harassment of the victim's family members, friends and acquaintances over the phone. However, the police failed to catch the offender. The Commissioner imposed a fine upon the operator for negligent identity authentication of the person requesting an itemised bill – the forged signature on the fax evidently differed from other (genuine) signatures of the customer (victim).

Since 1990, there have been already 33.4 million victims of identity theft in the United States, where this branch of criminal activity was born. It is estimated that this number grows by 50 % each year; however, the result of the police efforts to catch the "bad guys" is scarce. Nearly 88 % of the victims had no contact with the identity thief whatsoever. A modern criminal acts swiftly, accomplishes his goal within a week or two, and disapeares. On the other hand, the victim discovers the scam only after some time, when, for example, he starts receiving immense bills at his address. It takes months, if not years before the victim manages to prove his or her innocence and gets rid of the consequences of the fraud. Experts estimate that the average costs of administrative, judicial, security or detective services for clearing one's good name are valued at approximately 740 USD.

The purpose of the present Guidelines is to clarify what identity theft really is, what different types of identity theft we know, how it is regulated in the Slovene legislation, in what ways identity thieves gather personal data and what practical measures we should take to prevent identity theft.

WHAT IS IDENTITY THEFT?

The term identity theft is defined as obtaining personal data or identity of another person in order to gain benefits or to incriminate another person.

Identity theft is explicitly incriminated in the new Slovenian Penal Code and is defined as a criminal offence, where the perpetrator gains vital personal data, such as a number from a personal document combined with unique identifiers (the most common of which, in the Slovenian legal system are the "Unique Citizen Identification Number" and Tax number), with the intention of acquiring personal (and not only financial) benefits. The harmful consequences of this criminal offence are therefore not limited to acquired proceeds, but may also include other benefits (such as, for example, entering certain premises).

The consequences of identity theft can be unforseeable for the victim, because he can even become liable for acts he did not commit. Therefore, many countries, including Slovenia, adopted a legislation that classifies identity theft as a criminal offence.

Identity theft is a special type of severe and irreversible infringement of informational privacy or personal data protection. By its intensity, the effects of identity theft can be compared to the consequences of violent criminal offences against life and limb or property. Identity theft does not only bare the effects on a person's property (such as emptying his or her bank account, selling of securities etc.) but it also infringes on the victim's personality, since there are even reported cases of people being deprived of their liberty on suspicion of a criminal act which they did not commit (particularly often in cases of theft of biometric personal data, e.g. fingerprints).

The Federal Trade Commission (FTC) in the USA publishes an overview of the most frequent complaints, in its annual reports on consumers' complaints. Identity theft holds the leading position for several years in a row (last year has been the seventh consecutive year).

A perpetrator can make use of many different methods of obtaining personal data so that he can start posing as someone else and enter in different legal relationships (e.g. employment, acquiring professional qualifications, obtain personal identity documents etc.). The scope of identity theft is therefore not limited to the abuse of personal data, since it always includes the purpose of gaining certain benefits. Consequently, the protection of victims' rights is not limited only to data protection, but needs to focus on other rights as well, originating from broader aspects of the right to privacy (i.e. protection of the privacy of correspondence and other means of communication as defined in Article 37 of the Constitution of RS). Identity thieves can also encroach upon the victim's right to personal dignity by damaging his or her honour and reputation, and causing constant emotional distress, mainly due to the fact that theft of certain personal data can be irredeemable (e.g. the theft of biometric personal data, unique identifier and alike).

There are different methods of identity theft, which we divide according to:

- *the person, performing the attack (the intrusion can be either authorized or unauthorized);*
- *whether the data has been stolen from a database or during the information flow through a network (a direct attack on data storage or a medium for transmitting data; another possibility for theft of data is also when documents are being scanned from an analogue to a digital format);*
- *the motive (financial identity theft, criminal identity theft, assuming identity in daily life);*
- *the selected method (technical and non-technical methods).*

THE WAYS IDENTITY THIEVES OBTAIN PERSONAL DATA FROM THE INTERNET

One can assume another person's identity illegally using different methods that mainly depend on the general level of personal data protection in a society or a specific legal order. Preparatory activities for this kind of criminal offences can include different types of both criminal and non-criminal activities; for example stealing a wallet containing personal documents, intercepting electronic messages, scanning and cloning RFID enabled cards, using computer viruses (i.e. with *phishing* and *pharming* attacks), using fraud to gain information or even searching for discarded papers containing personal data (an activity known as *dumpster diving*), etc.

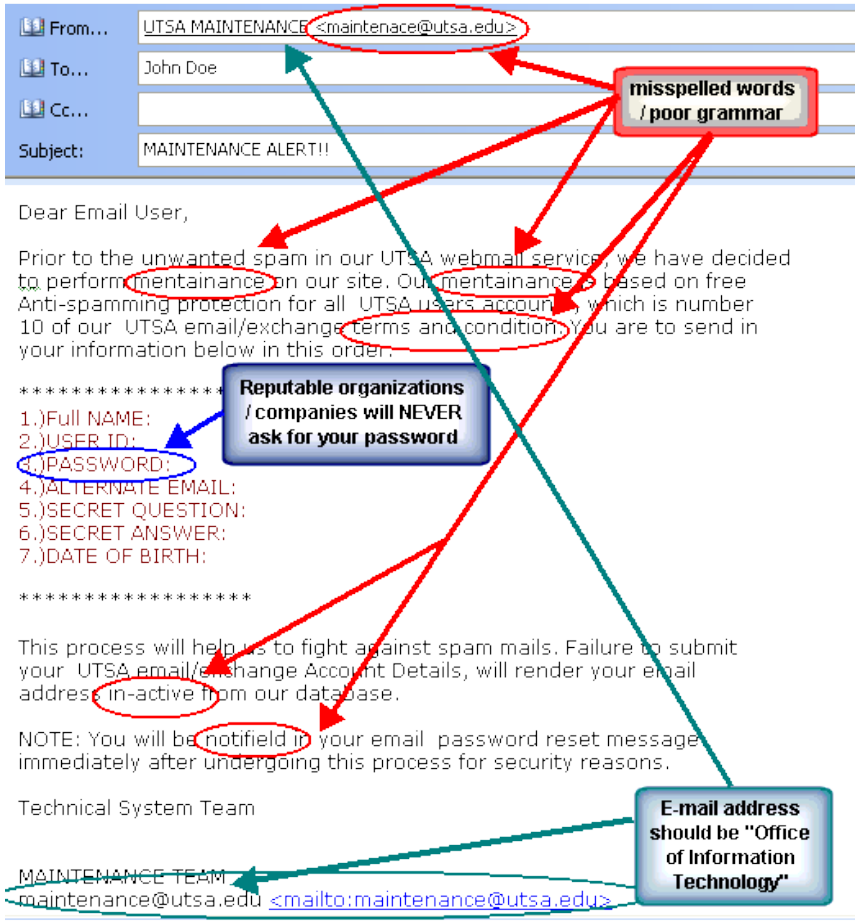
Abuse of personal data and identity theft are tightly connected with the development of information-communication technologies; we therefore continue with the explanation of some of the most frequently used methods of obtaining personal data from the internet network.

PHISHING

The term *phishing* originates from the English words "password" and "fishing". It means an illegal deception of users, by which a scammer tricks a user with false internet pages and e-mails, to obtain their personal data, such as credit card numbers, usernames and passwords, digital certificates and other personal data. Different techniques, pertaining to the domain of social ingeneering, are also used. Fraudsters usually set up a false web page, very much like the real one, and with the help of a false electronic message they try to lure people into visiting that false web page or they try to obtain personal data directly through your answer to the e-mail message.

A commonly used "trick" is sending an e-mail that appears almost exactly like a genuine message from a bank. The sender would usually warn an individual about a trouble with the user's bank account and ask that person to respond by sending an account number or username and password. In case the user had complied (to such a message), he would become a victim of an internet scam.

Example of typical, poorly-constructed phishing e-mail message:



Source: www.utsa.edu

PHARMING

Pharming is a neologism that derives from the English words "farming" and "pharmacy" and alludes to the technique of genetic engineering, whereas in the world of internet, we could speak of engineering the web sites. Pharming attacks can be very harmful for the users, mainly due to the fact, that they are so difficult to recognize. The main difference between *phishing* and *pharming* attacks is that the latter is more technical, whereas a phishing attack employes more of the social engeneering techniques. A pharming attack is usually a direct attack on the DNS servers or an attack on a specific data file located on a user's computer (with the so called *host file* that contains data on URLs and domains). By entering the proper URL address of the web page, the user is convinced he visited the real (genuine) web page; the truth however, is that one of the described methods of attacks has redirected him on a false page without the change in the URL address in the browser. Due to the false belief that the page is real, the user feels confident enough to enter personal data into online forms.

SOCIAL ENGINEERING

Social engineering is a selection of techniques that helps the attacker convince a user or a system administrator to disclose authentification data, which would help him log into a system unauthorised. Social engineering bases on the so called cognitive deviations and takes advantage of certain reactions of people in certain situations (for example, under pressure). Social engineers can be very successful in obtaining important personal data by using skills aimed at assuming other people's identities. Probably the most notorious hacker, Kevin Mittnick, was famous precisely for his ability to lure personal data out of people. Social networks (such as Facebook and alike) represent very useful tools for social engineers, especially because people publish their personal data on their own initiative, and such personal data then helps the attacker to get to know his victim better and to predict the way the victim reacts.

VIRUSES AND WORMS

Viruses are representatives of malitius code and "live" inside files, such as, Word and Excel files and others. When we open an infected file the virus spreads and infects other files on the computer as well.

Worms are self-replicating programs as well, but contrary to viruses, they are a bit more intelligent, mainly because they can search for appropriate targets to infect automatically. Both, worms and viruses, carry with them a payload that enables them to take control over an infected computer, erase the files and steal the personal data.

Just a brief glance through this field reveals that each week around 500 new viruses and worms break out. The number of these two malicious codes increases by 400 % each year and their authors/criminals get more creative as the time passes.

As viruses and worms frequently reside in unsolicited electronic messages (spam mail), due diligence is warranted when opening such messages.

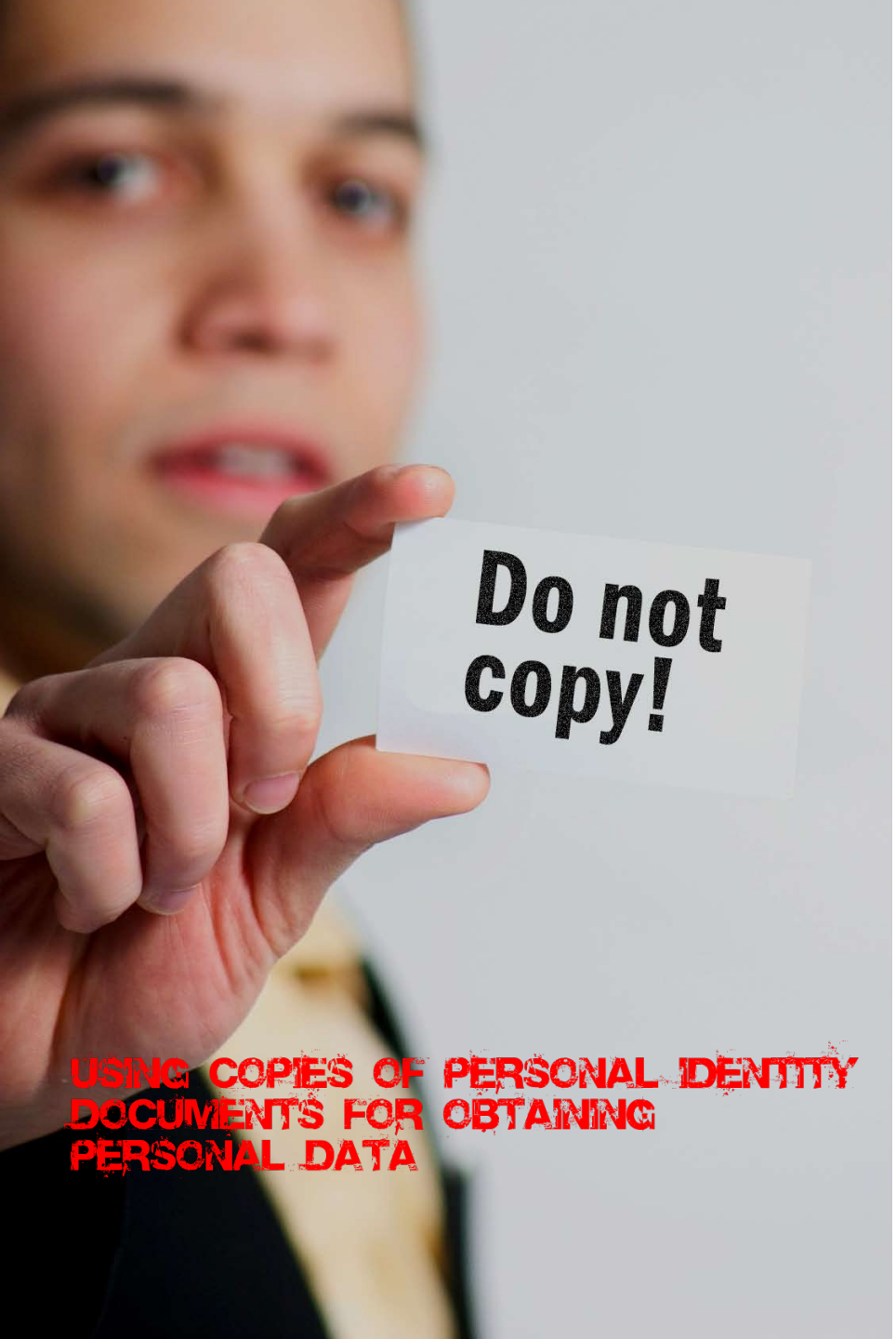
SPYWARE, ADWARE AND TROJAN HORSES

Spyware is another category of malicious codes. Such programs enter the computer whilst the user surfs the Internet, and they take advantage of security weaknesses of Internet browsers (Mozilla, Internet Explorer, Opera etc.). Some of such representatives can crawl into computers in the form of free software programs, screen savers, toolbars and file sharing P2P programs. Spyware can even change the dial-up number used by modems to connect the user to the Internet. Spyware can also be used to record passwords and other confidential data, which is then sent to the criminals. One of the most popular tricks of such spyware programs is also redirecting browsers to unwanted web addresses, which enables the attackers to perform a series of criminal acts.

Adware, on the other hand, is a category of malicious code that collects a user's data and their internet habits. Such representatives of malicious codes report their findings to different agencies, which then use the data to flood the users with different advertisements and unsolicited e-mails.

Spyware and adware differ from their cousins' viruses and worms because such software is not able to spread from one computer to other computer systems.

Another category of harmful programs are the Trojan horses that can smuggle into a computer, disguised as a legitimate program. When the user installs a legitimate program, a Trojan horse is secretly installed as well and it enables the attacker to take control of the computer.



USING COPIES OF PERSONAL IDENTITY DOCUMENTS FOR OBTAINING PERSONAL DATA

One's identity can be illegally obtained (stolen) by accessing personal identity documents. In 2008, two acts were amended in Slovenia, pursuing the goal of personal data protection and taking preventive measures against identity theft. These acts were the Identity Card Act (ICA) and the Passports Act (PA). Before, copying of personal documents was neither expressly allowed nor expressly forbidden. Many companies, as well as public sector bodies, did in fact photocopy personal documents, using their own interpretations of the law and their obligations. Information Commissioner's experiences from inspections showed that such an unclear legislation resulted in large number of personal data files containing photocopies of personal documents that were, much too often inadequately secured, and possibly abused for other purposes. A photocopy of an identity card or a passport holds relatively high trust among the people and that could make it possible for someone who appropriates such a photocopy to take over the identity of another person with relative ease and use it to purchase a product, for example, via distance selling (e.g. by fax machine).

Copying of identity cards or passports

Copying of personal documents is regulated by the Identity Card Act and the Passports Act, which permit copying **only in cases explicitly provided by the law.** Regulation of copying with executive acts of the Government or even with internal acts of the data controller is therefore null and void, be it the private or the public sector that tries to regulate it in this way.

The law stipulates that personal documents may be copied (besides by the owner) by the notary and by financial corporations providing financial services, if they need a copy for proving the identity of a citizen in an existing proceeding. Copying is also permitted on the basis of an owner's **written consent**.

The Commissioner is urging the data controllers, to interpret the statutory provision that allows for copying of personal documents for proving the identity of citizens in existing proceedings, restrictively. The data controllers must not overlook the general principle, that copying is allowed only on the basis of the statute – even a personal consent for copying must be explicitly provided by the statute. Moreover, the data controllers must respect the principle of proportionality, established by the Personal Data Protection Act (ZVOP-1). This principle, enacted in Article 3 of the ZVOP-1, states that personal data that is being processed must

be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed.

The mark on the copies and the prohibition of storing the copies in electronic form

The before mentioned statutes explicitly demand that the data controllers who intend to copy personal documents mark the copy adequately with the warning of prohibition of the use for other purposes. The statutes do not require any mandatory form of such a mark; therefore the decision about the form is left to the data controllers. Nevertheless, the Commissioner recommends that the controllers include at least the following information:

- that the document is a copy;
- the name/title of the data controller;
- the purpose of photocopying;
- the legal basis for photocopying (e.g. personal consent).

A stamp or a watermark has to be placed on the photocopy of an identity card or a passport, where the copy or an image of the document is seen, and not on the white margin around it or on the blank side of the paper, since it would be possible to cut out the stamp and photocopy the document without the data of the controller.

The law also prohibits copying and storing of copies of documents in an electronic form. It is therefore forbidden to copy personal documents using scanners and other similar devices that record the copy in an electronic form and save it on an electronic medium.

The law allows for the owner of an identity card to mark the copy of a document with his signature. It is recommended that the photocopy is signed in such a way that the signature is written over the copy of the picture and not in the blank space on the edges of the copy.

The issuing of a certificate

Both statutes lay down the obligations of the data controllers to certify that a copy of a personal document has been made. Mandatory components of such a certificate are:

- the purpose for the use of a copy;
- the duration for the intended use of a copy.

PRACTICAL PREVENTIVE MEASURES FOR PROTECTION AGAINST IDENTITY THEFT

We continue by offering 9 useful tips for protection against identity theft. Abuse of personal data can be prevented by taking adequate security measures.

Credit cards

Monitor the traffic of your credit cards. Review your bills before you pay them. Remove the bills that you do not need at the time from your wallet and spare yourself the additional concern if you lose the wallet or if it is stolen.

Tax number and Unique Citizen Identification Number

Reveal your Tax number and Unique Citizen Identification Number only when it is truly necessary. Many people and companies demand these two identifiers even when they do not need both. These two identification numbers are the most commonly abused data by the criminals.

The best way to destroy documents

Paper shredders and other devices, serving to destroy documents, are not intended for the limited use of large corporations, spies and similar entities. If you do not intend to use a shredder, provide for another way of destroying the important documents, expired credit cards, bills, bank account statements, medical reports etc., because most of them contain some personal data.

Signing documents

Be cautious when signing documents. Sign with your full name. The information on each bill must match the information on the documents. Draw a line on blank passages of the page and never sign blank pages.

Online shopping

Remember a small checkbox that you must check before a purchase, confirming that you agree with the business policy and storage of your personal data? READ IT! Do not make purchases from web pages that do not publish such terms and conditions. Pay attention to the use of safe connection and encryption.

The bank

If you think that there is something wrong with your bank account, pick up the phone and call the helpdesk at your bank. Check your bank statements regularly and pay attention to inconsistencies. If you receive an e-mail from a bank or an online store which you have not done business with, it is best to delete the message without opening it. Many "phishing" messages contain viruses and spyware programs.

The mail

Deliver sensitive mail personally to the post office and do not throw it in the mail box. When you are away for a longer period of time, arrange with your neighbour or a friend that they empty your mail box; it is better that way than to let your mail hanging outside the mail box.

In the office

Be informed about the data storage policy of your employer. Find out where and how they keep your personal data and how they handle sensitive data.

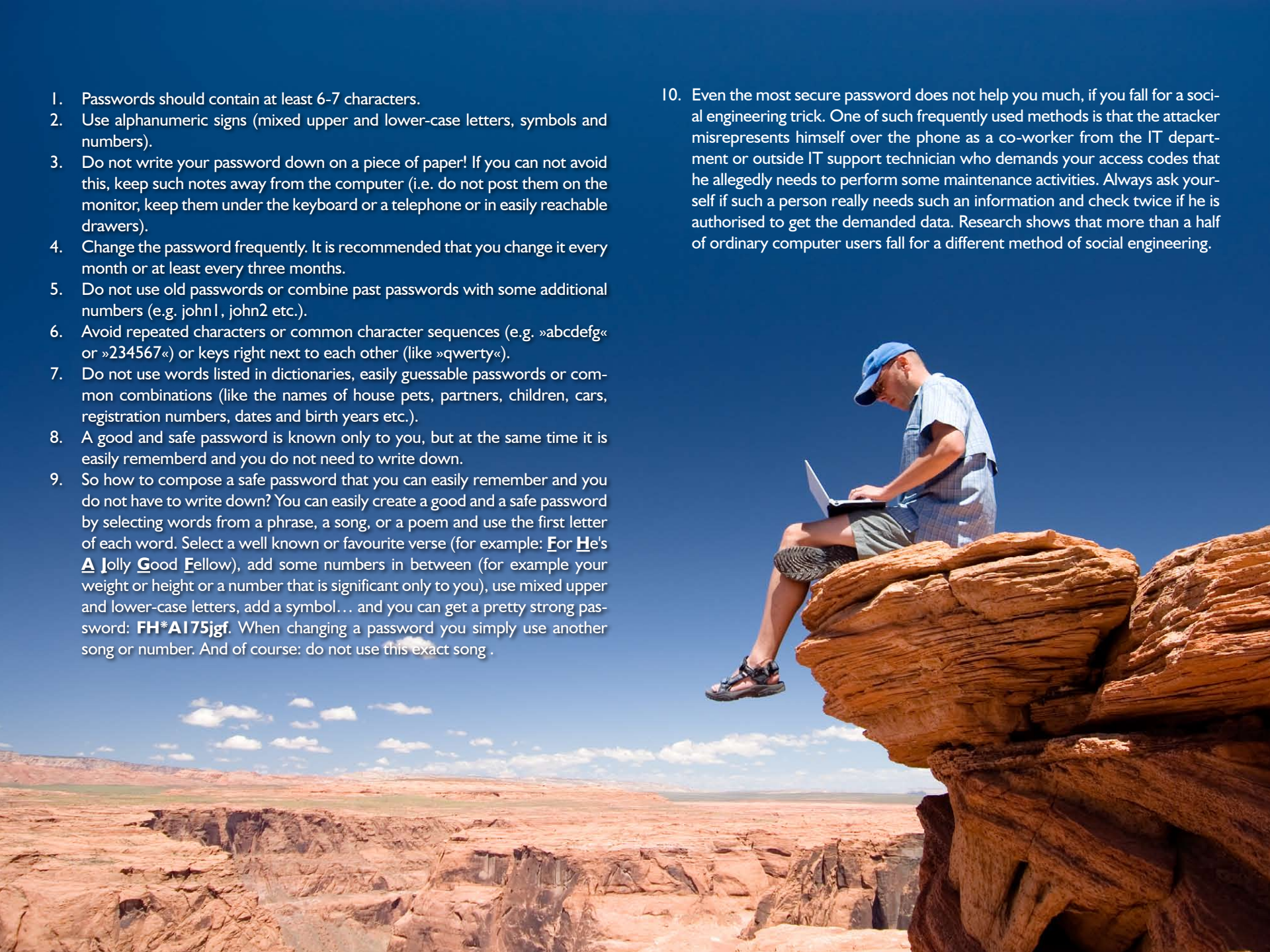
Passwords

First and by far the most important rule of computer passwords and PIN codes is that a password has to be "strong". That means that:

- it should not be the same as the user name,
- it should not be a word from the dictionary,
- it should not be made up of frequently used words,
- it should not be made up of a name, surname or any other easily guessable information pertaining to the user (e.g. birthdays, partner's name, children's name etc.),
- it should include a combination of letters and numbers,
- it should be as long as possible,
- it should be easy to remember but hard to guess.

It goes without saying that we should not carry our passwords written on a piece of paper with us.

1. Passwords should contain at least 6-7 characters.
2. Use alphanumeric signs (mixed upper and lower-case letters, symbols and numbers).
3. Do not write your password down on a piece of paper! If you can not avoid this, keep such notes away from the computer (i.e. do not post them on the monitor, keep them under the keyboard or a telephone or in easily reachable drawers).
4. Change the password frequently. It is recommended that you change it every month or at least every three months.
5. Do not use old passwords or combine past passwords with some additional numbers (e.g. john1, john2 etc.).
6. Avoid repeated characters or common character sequences (e.g. »abcdefg« or »234567«) or keys right next to each other (like »qwerty«).
7. Do not use words listed in dictionaries, easily guessable passwords or common combinations (like the names of house pets, partners, children, cars, registration numbers, dates and birth years etc.).
8. A good and safe password is known only to you, but at the same time it is easily rememberd and you do not need to write down.
9. So how to compose a safe password that you can easily remember and you do not have to write down? You can easily create a good and a safe password by selecting words from a phrase, a song, or a poem and use the first letter of each word. Select a well known or favourite verse (for example: **F**or **H**e's **A** **J**olly **G**ood **F**ellow), add some numbers in between (for example your weight or height or a number that is significant only to you), use mixed upper and lower-case letters, add a symbol… and you can get a pretty strong password: **FH*A175jgf**. When changing a password you simply use another song or number. And of course: do not use this exact song .
10. Even the most secure password does not help you much, if you fall for a social engineering trick. One of such frequently used methods is that the attacker misrepresents himself over the phone as a co-worker from the IT department or outside IT support technician who demands your access codes that he allegedly needs to perform some maintenance activities. Always ask yourself if such a person really needs such an information and check twice if he is authorised to get the demanded data. Research shows that more than a half of ordinary computer users fall for a different method of social engineering.



Beware of fraudsters

Do not transmit information over the phone or e-mail, especially if the other person contacted you on his own. Fraudsters often pretend to be employees of banks, public servants or some other profile that usually gets in contact with you. Make sure that you communicate with the actual person and not a fraudster who is trying to trick you.

Software

Use antivirus software that is frequently updated and set it to automatically check e-mails. Also use a personal firewall and anti-spyware programs.

IS IDENTITY THEFT HAPPENING IN SLOVENIA AS WELL?

There is no reason to believe that Slovenia is in any way immune to identity theft. After all, once in a while we hear a clear case of identity theft on the news, although the headlines might be disguised as something in the line of »Caught stealing telephone impulses« or something similar. The Information Commissioner dealt with some classic cases of identity theft in his praxis.

The Information Commissioner dealt with a case when an unknown female person came into a store that offered phased payments of bought merchandise, charged monthly on the telephone bill and assume another lady's identity by showing a forged passport, buying in her name and carrying home several plasma TV's. The woman, whose identity was stolen, was perplexed when she received a monthly bill worth several thousand Euros of debt for goods she never bought. She had to prove she was not the same person that bought and took the plasma TV's.

A special type of identity theft that drew the attention of a mobile network operator to the importance of identity checks was a case where unknown persons paid a homeless man some small change to conclude a subscription contract with one of the authorised shops for concluding subscription contracts. In the battle for new subscriptions, the network operator concluded the contract without a fuss but they were shocked when they found out that strangers had made a couple of thousand Euros worth of calls abroad that they had never paid for.

The Commissioner also warns about an identity theft that recently got a BBC reporter that visited Slovenia into trouble. A few years ago his passport was stolen and a new one was issued. Due to the fact that his stolen passport was used for committing a criminal offence abroad and that the data in the internationally exchanged police files was not updated, he was detained for two days in Ljubljana before he managed to prove they had the wrong person. This real-life case clearly shows how serious and lasting the consequences of disregarding the principle of accuracy and keeping personal data in up-to-date data files can be. These two principles are some of the basic principles of data protection that the public sector bodies should be well aware of. Inpresent times we often hear the argument »I have nothing to hide; here is my personal data – keep it« and even European studies show that the individuals lack awareness of the meaning of encroachments of privacy under the pretext of improving security. However, if we do not respect all the criteria or principles of data protection then those who »have nothing to hide« will »suffer« as well. It is possible to perform identity theft with a wide variety of personal documents and personal data, therefore we must be really careful about how we treat them and look after them.

THE ABUSE OF PERSONAL DATA AS A CRIMINAL OFFENCE

Article 143 of the new Slovenian Penal Code (Official Gazette of the Republic of Slovenia, No. 55/08) incriminates the abuse of personal data; it states:

(1) Whoever uses personal data, which may be kept only on the basis of the statute, contrary to the purposes for which personal data was gathered or without personal consent of the individual, to whom the personal data relates, shall be punished by a fine or by imprisonment of not more than one year.

(2) Whoever breaks or enters without an authorisation into a filing system kept on a computer in order to acquire personal data for himself or a third person, shall be subject to the same penalty.

(3) Whoever publishes on the Internet or enables others to publish personal data

of victims of criminal offences, data of victims of violations of rights or freedoms, data of protected witnesses, that is available in judicial records of the court proceedings, in which, by the decision of the Court or the provision of the law, the hearing was closed for the public; identification of the victims or protected witnesses was forbidden; personal notes about them that could identity them or make them identifiable concerning court proceedings were sealed, shall be sentenced to imprisonment of not more than three years.

(4) Whoever assumes the identity of another person and abuses his rights by false representation, acquires an unlawful property benefit or affects his human dignity, shall be sentenced to imprisonment of between three months and three years.

(5) In the event of the offence, under the previous paragraphs of the present article, being committed by an official, through the abuse of office or of official authority, such an official shall be sentenced to imprisonment of not more than five years.

(6) The prosecution of the offence under the third paragraph shall be initiated upon a complaint.

THE SECURITY OF PERSONAL DATA AS REGULATED IN THE PERSONAL DATA PROTECTION ACT ZVOP-1

Article 38 of the Slovene Constitution guarantees protection of personal data and prohibits the use of personal data contrary to the purpose for which it was collected. The collection, processing, designated use, supervision, and protection of the confidentiality of personal data is provided by law and everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data. That means that the Constitution allows only such processing of personal that is provided and clearly defined by law in advance.

ZVOP-1, as a basic and systemic law in the field of data protection, provides in the Article 6, Item 1 that personal data is any data relating to an individual, irrespective of the form in which it is expressed, whereas the individual is an identified or identifiable natural person to whom personal data relates. According to the Article 6, Item 3, processing of personal data means any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system or which are intended for inclusion in a filing system, such as in particular collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or connecting, blocking, anonymising, erasure or destruction.

Article 24 of ZVOP-1 stipulates that security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:

1. by protecting premises, equipment and systems software, including input-output units;
2. by protecting software applications used to process personal data;
3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient. The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed. Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

The duty to secure personal data is provided by Article 25. Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of this Act. Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data.

The Commissioner prepared a brochure with practical information on how to secure personal data; the brochure is available on the web page: http://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/brosura.pdf (only available in Slovene).

REPORTING VIOLATIONS

Even though you are informed about the described misdemeanours and criminal offences regarding personal data, there is still a chance that you become a victim of identity theft. Remember the following: Even though you take good care for the safety of your computer and you have the proper tools installed, thieves can steal your personal data from databases of a company, government, insurance company, or even easier – from your wallet or handbag.

In such cases report the violation immediately:

- Every theft must be reported immediately to the police, bank and/or insurance company. If you find out that someone opened a bank account in your name, demand the closing of the account and the proper steps from the prosecuting authorities.
- If someone else uses your credit card, immediately report this to the issuer (Visa, Maestro, MasterCard, Diners, American Express etc.). When you notify one of the listed issuers, they will immediately warn all the others. Such warnings prevent the thieves from opening a bogus account in your name in the future.
- Turn to the Information Commissioner, who will take appropriate measures against the company from which the personal data was stolen. As a matter of law, the protection of personal data files is guaranteed by the Personal Data Protection Act.

The procedure under the Personal Data Protection Act

Each individual can lodge a complaint with the Information Commissioner if he thinks that someone (private law or public law legal entity) is violating the Personal Data Protection Act. After receiving such a complaint, the Information Commissioner takes appropriate inspection measures ex officio in accordance with the Inspection Act.

An individual who discovers that his rights, established by the Personal Data Protection Act, were violated can also seek judicial protection while the violation is still pending. If the violation already ceased, the individual has the right to bring an action before the court to have the infringement established in case no other remedy exists regarding the violation. The action is decided upon by the competent court under the rules of the Administrative Dispute Act unless the Personal Data Protection Act stipulates otherwise. The procedure is urgent and preferential which means that the court has to initiate and close as soon as possible. The hearing in such proceedings is usually closed for public. If the individual suffered damages he can demand compensation from the responsible person in accordance with the law.

The Personal Data Protection Act assumes many penal provisions that prescribe fines (penalty payment) for violations of particular provisions of the law which at least indirectly protects individuals against violations and abuses of their personal data. Rights of the individuals are directly or indirectly protected with the statutory provisions on inspection supervision over the implementation of the provisions of the Personal Data Protection Act. Numerous provisions that prohibit such invasions of a persons's privacy are also encompassed in the Penal Code.

The Information Commissioner files a crime report when he suspects a criminal offence of abuse of personal data was committed, provided that he estimates that all the elements of the criminal offence were fulfilled; in other cases he conducts misdemeanour proceedings on the basis of established violations.

Criminal proceedings

Abuse of personal data, incriminated in Article 143, Paragraph 4 of the Penal Code (identity theft) is a criminal offence prosecuted ex officio. In accordance with the Articles 146 and 147 of the Criminal Procedure Act any person may report the abuse of personal data, established by the Article 143, Paragraph 4 of the Penal Code, in writing or orally to the competent public prosecutor or to the police.

USEFUL LINKS

More information about all of the important aspects of identity theft is available at the following links:

1. Wikipedia: http://en.wikipedia.org/wiki/Identity_theft
2. Moj mikro: http://www.mojmikro.si/preziveti/varnost/varnost_za_telebane_kraja_identitete
3. Federal Trade Commission: http://www.ftc.gov/bcp/edu/microsites/idtheft/
4. Identity Theft – Prevention and Survival: http://www.identitytheft.org/
5. Identity Theft UK: http://www.identity-theft.org.uk/

CONCLUSION

Modern technologies brought an overwhelming simplicity of personal data processing, especially the ones in electronic form, to our everyday lives. However, with such technological advancement came the dangers of faster and easier abuses of personal data which can be, when combined correctly, easily used for identity thefts. Some researches show that terrorist attacks are not at the first place among the people in the USA - identity theft attacks are. Despite a relatively rigorous legislation on personal data protection even citizens of the European Union are no longer immune to personal data abuse. Nevertheless, even the strictest law cannot replace the most important aspect of personal data protection - the awareness of each individual about the importance of his own personal data. If we do not provide for an adequate security of personal data on our own, we can soon become targets of identity thieves.