

## Data Security Problems:

How to protect the confidential information against any competitors and tricksters reliably?



**NOTICE: You DO Have the Right to Reprint or Resell this Report!**  
You Also MAY Give Away,  
Sell or Share the Content Herein

[As long as you don't change anything, misrepresent the report, use SPAM or generally do something ya know you're not supposed to do!]

**ALL RIGHTS RESERVED.** No part of this report may be reproduced or transmitted in any form whatsoever, electronic, or mechanical, including photocopying, recording, or by any informational storage or retrieval system without express written, dated and signed permission from the author.

**DISCLAIMER AND/OR LEGAL NOTICES:**

The information presented herein represents the view of the author as of the date of publication. Because of the rate with which conditions change, the author reserves the right to alter and update his opinion based on the new conditions. The report is for informational purposes only. While every attempt has been made to verify the information provided in this report, neither the author nor his affiliates/partners assume any responsibility for errors, inaccuracies or omissions. Any slights of people or organizations are unintentional. If advice concerning legal or related matters is needed, the services of a fully qualified professional should be sought. This report is not intended for use as a source of legal or accounting advice. You should be aware of any laws which govern business transactions or other business practices in your country and state. Any reference to any person or business whether living or dead is purely coincidental.

### About The Author



Evgeny Korovin is founder of Actual Software Lab – company which developed any security tools for protection your computer and information on it.

This e-book helps you to make your PC faster and more protected and will grant you the full control over your data.

Actual Software Lab Website

<http://www.actsoftlab.com>

Actual Software Lab Emails

[support@actsoftlab.com](mailto:support@actsoftlab.com)  
[sales@actsoftlab.com](mailto:sales@actsoftlab.com)

## Contents

Setting & Using Passwords	4
System Patches and Updates	5
“Malware”	5
A 7-Step Program to Avoid a “Malware Infection”	8
“Phishing”	8
Data Encryption	9

## Setting and Using Passwords

The general rule in choosing passwords is, the longer and more complex the better. What is meant by “complex” is simply that the password should contain not only alphanumeric characters (A-Z, a-z, 0-9) but “special characters” (e.g. &, \$, @, #) as well. With the continuing growth in the speed and power of personal computers available to people around the world - including hackers - passwords that are shorter and/or lack complexity are becoming easier prey to the sophisticated password-cracking software and tools that are widely available to hackers and computer thieves. And make no mistake about it, having one or more of your passwords stolen or compromised is a form of identity theft that permits someone else to impersonate you and gain access to your private data.

When setting up accounts on the web, some providers (including financial institutions) will unfortunately limit the length of the password you choose to less than eight characters, although in some instances they provide additional security measures that compensate for this to some degree. In general, though, eight characters are typically recommended as the bare minimum. Most Internet systems will not only allow passwords of eight or more characters, they will require them along with enforcing complexity. In some instances, you can choose a password that is up to 255 characters in length! (That might be a little hard to remember, though.)

Another important consideration in selecting a password is not to base it on words (including proper nouns and names) that are likely to appear in the many password cracking “dictionaries” that are available. These dictionaries often include not only most common English words (as well as from other languages) but references from popular culture, sports, entertainment and other sources. They will also test for simple character substitutions. So, for example, if you choose “*EricCartman*” as your password, it’s a good bet to be quickly cracked even if it is more than eight characters long. And, changing it to “*3r1cC4rtm4n*” won’t make it much stronger.

Some modern computer operating systems (including Windows XP/Vista) offer the opportunity to use “passphrases” for access to user accounts. These are pretty much the same things as passwords, except they can be much longer and can include spaces, punctuation and other characters that many systems do not permit in passwords. A passphrase stretching to twenty characters or more is exponentially more difficult to crack than an eight-character password, even if the passphrase does not feature complexity. “Oh my God, they killed Kenny!”, in this case, would be a much more secure way to access your account than “*3r1cC4rtm4n*”. While it takes a few more seconds to type in a passphrase, the greatly enhanced security makes for a pretty good tradeoff, especially when you consider that passphrases tend to be more easily remembered than complex passwords.

Of course, even the strongest password or passphrase is useless if you give it away or make it easy for someone to guess or find out what it is. The more people who know you’re a South Park fan, the more likely it is that one of them may

guess one of the examples above as your password/passphrase (and in fact, don't use these - they're just examples). Try to avoid writing passwords and passphrases down if possible, and if you do, don't post or display them where snoops can see them or are likely to look (like on the underside of your keyboard). It is true that we are all acquiring more and more usernames and passwords to keep track of, and remembering them all is simply not an option anymore. Password "vault" programs are available that allow you to record them (and other sensitive bits of information) in a master encrypted file that you can protect with a single strong password for opening and retrieval. These programs are commercially available at minimal expense, and Macintosh OS X comes with such a program ("Keychain") as part of the operating system.

## System Patches and Updates

No matter which of the major operating systems your computer runs, there's an army of hackers good, bad and in-between ("white hats", "black hats" and "grey hats") around the world that continuously probes for weaknesses and vulnerabilities. Although Microsoft, Apple and others have made significant strides in writing more secure software over the last few years, the fact is that the software is so complex that new "holes" are discovered on an almost daily basis. For this reason it is vitally important that you download and install system patches, service packs and updates (especially those that are security-related) for both your operating system (Windows, Mac OS X, Linux, etc.) and your application software (Word, Excel, iTunes, etc.) on a regular basis. At the very least, check for these updates and patches weekly at the sites provided by your operating system's vendor. Microsoft ([www.windowsupdate.com](http://www.windowsupdate.com)) and Apple ([www.apple.com/support/downloads](http://www.apple.com/support/downloads)) make this very easy for you to do and even permit you to automate the process. Many linux distributions such as Red Hat, Suse and Debian also have ways to automatically update and patch systems running their software. "Unpatched" systems have historically been the prime breeding ground for many of the most severe computer "malware" outbreaks of the last decade (*see next section*), even though in some cases such as the "Code Red" virus of 2001, patches that would have prevented infection had been available for more than a year before the outbreak.

## "Malware"

The variety of modern software we use for our work, jobs, hobbies, or just to goof off and play games is astounding. Unfortunately, there's a dark side in the form of malicious software, a.k.a "malware" - programs that are designed to spy on you, destroy your data, steal your personal information, use your computer to infect others or take over and turn your computer into an Internet zombie ("bot").

Some do all of these. It used to be possible to classify malware into distinct classes such as viruses, worms, spyware, “back doors” and “Trojans”, but modern malware often combines the features of each class to the extent that putting it in a single category is impossible. If that weren’t bad enough, many malware programs now install “keystroke loggers” and other forms of spyware that are capable of secretly recording what you type, the programs and files you open, the mouse clicks you make and other actions that give a remote intruder an “over-the-shoulder” view of your computing activity. It’s important to know also that spyware can be acquired from sources that are not normally thought of as malware. Clicking on links in commercial websites, for example, can sometimes lead to download and installation of software (such as DoubleClick) that tracks and reports your online buying patterns. Many “free” peer-to-peer filesharing programs install a variety of spyware for similar purposes, and they even tell you they’re doing it - if you take the time to actually read the licensing agreement before clicking “Agree” to install. Free “toolbars” and “accelerators” are also a prime source of spyware. Besides putting your computer and your personal data at great risk of compromise, spyware also tends to collect like engine sludge, slowing things down to crawl.

Over the last decade, however, the primary source of malware has been, and continues to be infected e-mail attachments. It’s simply a bad idea to click on and open an e-mail attachment unless you’re absolutely sure you know who sent it to you, why they sent it to you and what the attachment contains. Even if it’s your mother sending you a “cute” cartoon or animation she downloaded off a website, it may carry a virus or other destructive payload. And even worse, your mom’s computer is undoubtedly already infected.

To combat malware there are three essential tools you need to have and use religiously. First, make sure your computer is running anti-virus software, and that you are updating it regularly (meaning, daily). Most major anti-virus programs allow you to update virus “signature” files automatically, so as long as your computer is turned on the anti-virus software will have access to the most current virus definitions to check for. Most users using **Symantec Anti-Virus (SAV)**. Be aware, though, that anti-virus software is not “bullet proof”. Sometimes new viruses emerge and spread before the anti-virus vendors can analyze and develop an “antidote” for immediate distribution. And of course, if you get out of the habit of updating regularly, it’s almost like not having anti-virus software at all.

The second major tool to defend against malware is a **personal firewall**. This is a program that acts as a sort of “gatekeeper”, deciding what network traffic may pass into and out of your computer. Both Windows (XP/Vista) and Mac OS X come with built-in firewall applications that are very good, though not quite as capable as inexpensive commercial programs such as **Zone Alarm** or **BlackIce Defender**. Although the default settings on most personal firewalls will permit the sort of normal activity (e-mail, web browsing, etc.) that most users engage in, it may become necessary to tinker with the firewall settings to, for example, allow a new program you’ve installed to communicate across the network as intended. For this

it may be helpful to you to acquire a basic understanding of computer “ports” and protocols, but your Local Support Provider (LSP) or Information Technology Advisor (ITA) can also be a valuable source of help in managing your personal firewall. As with anti-virus software, though, a firewall is not 100% effective, but the more effort you put into monitoring and maintaining it, the more valuable it will be to you.

The third major defense consists of one or more **spyware removal tools**. Because spyware is engineered and behaves differently than viruses and other malware, anti-virus software is generally ineffective against it. Not all spyware removal tools are equally effective against all kinds of spyware (and there are many), so most computing security experts recommend installation of more than one (but not more than three) such tools. As part of their Windows Update service, Microsoft does provide a free spyware removal tool.

While these tools give you essential protection against malware, the best defense in the end is your own common sense and judgment. Here are a few rules of thumb:

**It's OK to be a little paranoid** - there really are people out there trying to get you, there really are dangerous websites, and there really is no “free lunch”. “Free” software almost always comes with some sort of hidden cost, and unless you have the knowledge and resources to thoroughly test such programs, downloading and installing them increases your vulnerability exponentially.

**Read those EULAs** - the End User Licensing Agreement, or the “contract” you're required to agree to before the software will finish the installation process. They can be lengthy, and most people frankly don't have the patience to scroll down through them and read what they actually say before clicking on the box that usually says something like “I Agree”. Particularly in the case of peer-to-peer filesharing programs, close inspection of the EULA often reveals that you are granting them permission to place spyware, advertising and pretty much anything else they want on your computer. You wouldn't sign a contract to buy a house without reading it, especially if it granted the seller the right to come in and raid your fridge any time he wanted - why would you agree to a similar deal for your computer, your “Little House on the Internet”?

**They're watching you** - you're not just a “little fish” in the big Internet sea that the bad guys can't see or don't care about. Whether it's your Internet-connected computer running on DSL or cable modem, you're being scanned on a regular basis, i.e., many times daily, by “Internet burglars” who are performing the network equivalent of “casing the joint” - checking the locks, seeing if there are doors or Windows left open (pun intended) and looking inside to see what looks good. And make no mistake, most of us have valuable information on our systems such as Social Security Numbers, banking information, sensitive work data and more. And, for some of these “burglars” the goal is to break in simply to show that they can.

An unattended computer is a sitting duck - an intruder, or even someone in your office with a grudge against you may take the opportunity to install malware from a CD or USB “thumb drive” while you’ve left your computer unattended and without a password-protected screen saver. Keystroke loggers can also be physically attached devices (usually in-line with the keyboard cable), so it’s a good idea to occasionally inspect your computer, front and back, for devices you don’t recognize or recall installing.

#### A 7-Step Program to Avoid a “Malware Infection”:

1. Download and install operating system patches regularly;
2. Never open e-mail attachments unless you’re absolutely sure you know what’s in them;
3. Visit only trusted websites as much as possible, and be alert to where links are taking you;
4. Do not install peer-to-peer filesharing software unless you really need it;
5. Choose, use and protect your passwords wisely;
6. Install and use anti-virus software and a personal firewall;
7. If you must leave your computer unattended, lock it with a password-protected screensaver.

#### “Phishing”

A sort of e-mail/web “hybrid” scam, “phishing” is an Internet fraud that has become all too commonplace in the last few years. The “bait” arrives as a message in your inbox and appears to have been sent by a financial institution, online retailer or other business with whom a large number of Internet users are likely to have accounts or other dealings with. Among the favorites of long standing are eBay, PayPal, Amazon.com and Visa, as well as a variety of national and regional banks. In order to appear as authentic as possible, the message almost always contains corporate logos and graphics (usually pirated or forged) along with contact information that may or may not be accurate, counting on the fact that most people won’t actually check. The body of the message will allude to some “urgent problem” regarding your account that must be dealt with immediately: billing dispute, fraud claim, unpaid invoice, account info update and many other alleged critical matters. The message will instruct you to click on a link that will open a web browser window to a site, also apparently genuine, where you will be asked to login with your account name/number and password along with other personal information. The site is, of course, as phony as the e-mail message, and the payoff for the “phishers” is that they’ve collected information about you that they can sell or use themselves to commit identity theft and other crimes.

Legitimate businesses should never ask you to transmit sensitive or confidential personal information relating to your account via e-mail, especially if they are initiating the contact.

In the last year there has been a pronounced rise of very sophisticated and refined “phishing” attacks (sometimes called “pharming”) in which the message is “seeded” with personal information about you, personally, that they have been able to obtain, such as your name and job title. This makes it appear to be more than a “generic” phishing attack, and the scam in many of these is not to get you to go to a phony website, but instead to get you to open an infected attachment which will install some form of malware on your system.

If you receive an e-mail message that appears to be phishing-related but have some reason to believe it may be legitimate and require follow-up on your part, DO NOT OPEN ANY ATTACHMENTS, AND DO NOT REPLY DIRECTLY TO OR VISIT ANY WEBSITES SHOWN IN THE MESSAGE. Use a search engine like Google or Yahoo! to locate the firm’s official website and published contact information. Most of these businesses have extensive experience as targets of “phishers” and will often have specific information and instructions for you available on their website (eBay and PayPal are good examples of this). Another good source of help can be found at [www.antiphishing.org](http://www.antiphishing.org).

## Data Encryption

In years past, data flowed back and forth across the Internet in “clear text”, without any thought given to encryption. Likewise, thought was rarely given to the dangers of sensitive information residing on digital media, which for many years referred mostly to hard drives and floppy disks. The advent of laptops, PDAs, “smartphones” (including Blackberry, Treo and iPhone) and other portable devices has provided great mobility to millions of users, and the emergence of new media such as USB “thumb” drives and Compact Flash cards has enabled more and larger data files to be carried around for interchangeable use. With this higher mobility, of course, comes a higher risk of loss or theft of the devices and their data. Even if the only computer you use is an “immobile” desktop (which can still be stolen), it is becoming more and more critical to ensure that confidential data is securely encrypted regardless of the media on which it resides. Both Windows (Encrypting File System on XP and Vista) and Mac OS X (File Vault) provide the means to encrypt data files on your hard drive, but that encryption is typically lost when the file is copied to another medium. Commercial products such as **ASL Crypto Manager** offer encryption that is “portable”, and more of these types of products are becoming available as time goes on. The market in encryption products for PDA’s and other handheld devices is still in its infancy, but look for new offerings in this area to become available as well. Whatever form your custody of confidential information takes, be it personal or business, it is becoming more and more vital to

encrypt it for its protection - and your own.

**ASL Crypto Manager** is a commercial product that is available at reasonable cost at [www.actsoftlab.com](http://www.actsoftlab.com). This program is based on high-speed stream algorithm of encryption. The **ASL Crypto Manager** program is intended for quick encrypting of any user's files. The program allows to cipher any taken file and to pass it safely to the other person, using the common ways (portable data medium, e-mail message, local area network, etc.). Prior to the encrypting of any file, a key word is being set up; without knowing the password, it's impossible to decipher the file by means of any program or any other way. The program also allows to carry out enciphering of multiple files (enciphering of several files at one pass) with identical or different passwords. It is equally important to encrypt data as it travels across the network as well, especially when it comes to wireless networks.

More information about **ASL Crypto Manager** you may find on ASL website:  
<http://www.actsoftlab.com>