Do not put unneeded effort into a project - There is a place for perfectionism, but for most activities, there comes a stage when there is not much to be gained from putting extra effort into it. Save perfectionism for the tasks that need it.

Deal with it for once and for all - We often start a task, think about it, and then lay it aside. This gets repeated over and over. Either deal with the task right away or decide when to deal with it.

Set start and stop times - When arranging start times, also arrange stop times. This will call for some estimating, but your estimates will improve with practice. This will allow you and others to better schedule activities. Also, challenge the theory, "Work expands to fill the allotted time." See if you can shave some time off your deadlines to make it more efficient.

Plan your activities - Schedule a regular time to plan your activities. If time management is important to you, then allow the time to plan it wisely.

No doubts, that the observance of these rules will enable you to operate time more effectively. And it, in its turn, is the keystone to successful realization of any activity or project.

Lytvynenko G. I., *ELA*

INTERNET SECURITY AND PRIVACY

Pelepei R.L., *IN-41*

Most of the security problems encountered on the Internet are due to human mistakes.

The first level of security "leaks" usually occurs during the development of the website. If a website developer doesn't correctly plan or proof test his scripts, an eventual hacker could extract confidential information from the website itself. This is usually done by exploiting particular errors or by inserting some particular code snippets into an input field or website url.

The usual way to fix this problem is to make better planning when coding your website and to further test your scripts, especially those dealing with private data.

Another kind of security problem are problems due to users neglecting their own private information. A good example of this kind of neglecting is when someone gives away his or her email address on a public forum. Some "crawler bots" (small programs coded to collect email addresses) could find the address and add it to a mass-mail list, sending spam to the user. This may not be a dangerous "security" problem but the same can also happen with user names and passwords. Most of the big hacking cases occur simply because an important user of a particular network gave away his private information.

The main way to fix this problem is to be very careful to who and how you display confidential data. The best way being - simply not to display them.

Another big security problem is the download of virus-infected files. Most of the virus will usually not affect your computer; still, some of them might contain damageable programs for your computer or even allow a distant user to take control of your computer. These programs are called a "Trojan Horse". While some people may believe the opposite, it is impossible for someone to download potentially damaging files to your computer without your content, as long as you don't let your computer filter your downloads. At the same time, it is barely impossible to simply "get a virus" by surfing on the Internet. Virus mostly come with downloaded files that you usually consented to download or in attached email files that you opened without previously checking it.

That being said, the trick here is again to be extremely careful when you download a file. Peer-to-peer networks are also good virus hives and it is preferable to stay away from them.

The last and probably most uncommon internet security problem is hacking itself. True hacking usually means that the hacker had no or few information on his target and does most of the breakthrough with his own knowledge. Common users are usually not the target of hackers; hackers will usually try to get through security barrier of big organization's Internet servers or try to hack Website Servers. They usually get to do so by using some software engineering flaws that have yet to be fixed (most of Windows XP auto patching aims to fix these flaws for example).

At large, there is no particular way to help in this case, unless you're the developer of that software. Simply report the case to the developer and wait for a security fix or a new version with better security.

Hopefully, some companies actively work at the elimination of all these problems. For example, Norton provides users with a whole array of security tools (e.g.: Norton Antivirus) that do make a difference when it comes to clean up (virus-wise) your computer. Microsoft is also developing software called "Microsoft Antispyware" that aims to help the users keep their privacy, eliminating history data and Spywares.

What you need to keep in mind is that most of the security problems on the Internet are due to the users' misunderstanding of the media or human mistakes. You need to be extremely careful when transferring files or displaying private information and pay close attention to new kinds of virus or security leaks. It's best to also keep in mind that the Internet is not the only network, local or wireless networks are as much vulnerable as is the Net.

Lytvynenko G. I., *ELA*