

General Information

Security and Privacy Considerations

- **Choose your passwords wisely** - don't use one that can be easily guessed and don't use only one or two passwords at many sites just because they are easy to remember. Stay away from real words, use a combination of letters and numbers, and keep passwords at least six characters long. Don't use birth dates, names of children or pets, or simple sequences like XYZ123. Keep a record of your IDs and passwords, but not on your PC. Don't store your password at a site or on your browser to avoid entering it the next time you log on. And periodically change your passwords. You can use our [password generator](#) for ideas.
- **Don't give out personal information** - like password or credit card information through email, chat rooms, etc. Give out the least amount of information necessary to complete any registration. Don't fill in options. Don't store credit card numbers for future convenience. Don't save password for future visits. The rule of thumb: When in doubt, leave it out and see our [Tips for Revealing Personal Information](#).
- **E-mail is insecure** - Don't send information through e-mail that you wouldn't want on the front page of the newspaper. Anyone intent on gaining access to it can read your e-mail. For confidential correspondence, there are plenty of easy-to-use encryption programs available.
- **Don't talk to strangers** - and recognize that you are not safe when you communicate with people you don't know. Spammers and others use harvesting software to grab e-mail addresses even when you think you haven't supplied one. Turn it off instant-messaging software when you aren't using it, and configure it to hide your presence.
- **Make Cookies Work for You** - Don't accept cookies that follow your surfing habits and report on what you view. Useful cookies let Web sites recognize you as you use the site or on a return visit, so rather than disable them completely, consider a cookie-management program. You can delete cookies from your browser by visiting your settings.
- **Watch for Java or .exe files** - Be cautious of sites that want to install java applets or other executables on your computer. Disable auto-running of Visual Basic Scripts - Open them in Notepad instead: Open Windows Explorer, View, Folder Options, File Types, Scroll down to "VBScript Script File" in the "Registered file types" list, Edit Actions, Set Default.
- **Use Anti-Virus Software** - Be sure to install an anti-virus program in real-time mode and update the virus definitions regularly.
- **Stay Current** - Apply security updates of your software, especially Microsoft software.
- **Never open attachments from an unknown source** - and virus scan ones from people you do know before you run them (friends sometimes pass on viruses without meaning too).
- **Protect you E-mail** - Make sure that the program is set to ask for permission before it runs any macros - most modern mail clients help with this by setting it as default.
- **See complete file names** - so you know what they are: Open Windows Explorer, View, Folder Options, View tab, Advanced, Click "Show all files". Uncheck "Hide file extensions for known file types."
- **Turn off printer and file sharing** - It's an open door for any

General Information

knowledgeable hacker to enter through in order to snoop around and perhaps do some mischief. If you must share your files, be sure to password protect your PC with a sound password.

- **Use a Firewall** - If you use cable, DSL or other broadband connection, you should consider a personal firewall - an anti-intrusion program that acts as your PC's Internet gatekeeper - especially if you leave your computer on. DSL and cable users can ask if dynamic addressing is available to avoid static IPs.

Unique solution ID: #1018

Author: Jack Massari

Last update: 2017-02-06 16:55