

TOP 10 TIPS TO KEEP YOU PROTECTED ONLINE

NORMAN®

1 NEVER INVITE STRANGERS HOME – be conscious of shared folders/resources. Check your PC configuration before you go online. Turn off your PC when it is not in use.

2 USE PROFESSIONAL CLEANERS – install antispysware and antiadware products on your PC. Update your antivirus software regularly; let it scan your incoming mail before emails are allowed into your computer.

3 UPDATE YOUR OPERATING SYSTEM CONTINUOUSLY – make sure that all important security updates are downloaded and installed as quickly as possible after they are available from the software provider.

4 BE CRITICAL TO THE "POSTAL SERVICE" – delete the email if:

- The sender is unknown.
- The subject field does not make sense.
- The mail contains a link, and you are not sure where it will direct you on the Internet.

- The email contains a suspicious attachment.
- The email seems to be from a software vendor with an attached program that claims to be a security update. Software vendors never send security updates as mass-distributed emails!
- Email is in your spam folder. You should never reply to spam messages, which often contain malicious software.

5 GET A TRUSTWORTHY DOORMAN – your computer has many 'entrances' for different tasks. Open ports could allow unlimited access to your computer's resources. The main purpose of a personal firewall is to protect you against unwanted 'visitors'.

6 LOCK UP "FILING CABINETS" WITH THE SENSITIVE INFORMATION – store your confidential data securely. The best solution is to use encryption tools, which handle folders as well as individual files.

7 DO NOT LET ANYBODY IN – configure your web browser to ask if you allow 'active content'. Be selective with regard to which websites you grant access to your PC and programs you download from the web and peer-to-peer systems.

8 TAKE ADVICE FROM EXPERIENCED IT PERSONNEL – if you use a portable computer in your daily work, familiarize yourself with your employer's rules and regulations on IT security. Consulting your company's IT personnel may help you to avoid many problems in the future.

9 DISCLOSE AS LITTLE AS POSSIBLE ABOUT YOURSELF – never reveal information of a personal nature, unless it is absolutely necessary. It might be a good idea to use separate email addresses for different purposes.

10 BACK UP RELEVANT INFORMATION – data can be erased by an accident or malware activity. Back your valuable files that you have invested time and effort to create. Software and other system files can be reinstalled.

