

One apple a day  
takes the **virus** away.



Here are **10 good daily practices for a safe management of your emails and Internet browsing** in order to help you avoid unpleasant problems.



**F.C.S. Solutions S.r.l.**

[www.fcssolutions.it](http://www.fcssolutions.it)

# EMAIL MANAGEMENT

1. When you receive an email with attachments or a link in the message body, always check the sender's email address; **if you don't know it, then be careful**; if you already know it, but the text is generic, make sure the sender really meant to send you that particular attachment.
2. If the email has a link to an invoice that is apparently attached, always make sure that the last file extension is NOT .exe (i.e. **invoice132.pdf.exe is definitely a virus!**).
3. If the content of the email takes to some links, before you click, check if the link matches the specification, simply by hovering with the mouse over the link: **often this links shall redirect you to a site other than specified.**
4. To check the authenticity of the message, simply reply to the email you received, asking for confirmation that the email was purposely sent to you; **in case of viruses, most of the messages come back with a non-existent mailbox error.**
5. It seems quite obvious, but **it is impossible that a bank to which you are not customer may ask you direct information, or an electric / gas utility provider may write to your company's email address, if those information concern your private residence.**

6. To make it look like real communication, often part of the address that is before the @ is reported as email recipient's name, i.e.: [john.smith@corporatename.com](mailto:john.smith@corporatename.com) receives an email starting with "Dear john.smith, pls. find here attached our invoice...", which is **the classic suspect email that is NOT to open!**

# WEB SURFING

7. **Avoid using/letting people use personal email through the company's computer**
8. When you enter a site and a pop-up appears, **do NEVER click on the X because sometimes the X itself is a link.** It is better to close the browser with the key combination ALT + F4 or by right-clicking on the icon on the taskbar.
9. **When the digital certificate associated with a website is not verified or expired you should be careful:** it may be a site collecting authentication data.
10. Apply the same precautions as suggested for the email (step 3): if you are required to click on a certain link to be redirected on another site, simply **hover over it with your mouse in order to check the destination of the link**



## FCS MEANS PREVENTION

We help you  
with the good daily practices to  
**work safely**



## FCS MEANS MANAGEMENT

We help you  
build a **computer network** made to  
perfection



## FCS MEANS EMERGENCY SUPPORT

Have you suffered a virus attack?  
We can help you **recover**  
**your precious data**