Here are some useful tips for social networkers;

- Evaluate the contents of your social networking account(s); how do you feel about complete strangers seeing what you posted?
- Do not post private information, including your mobile phone number, home address, work schedule, social plans, etc. unless you are prepared for anyone to find you/track you down, any time of the day or night.
- Do not post anything that may cause you embarrassment or potentially harm the corporate image of the GSC.
- Utilise the "Privacy" settings on your social network account—you can adjust your privacy settings so as to control who has access to your personal information.

Finally, you can always Google your name to see how your name or identity is being used. If you suspect that you are a victim of identity theft contact the police immediately.

For more on the dangers
of Social Networking see
the Security Awareness Letter issue # 4
from January 2012 available
at the Security Awareness
website via Domus.

See also the "General Principles
for the use of Social Media
by GSC staff" CP 088/11.

For any further questions or comments,
please do not hesitate to contact
the Security Awareness Cell at

security.awareness@consilium.europa.eu

Graphisme et impression: DGA 3 - Services techniques de production - RS 114/2011 - Photos: Fotolia

CONSILIUM

PEACE OF MIND
FOR SOCIAL NETWORKERS

Not among friends!
7 Fatal Blunders
when
Social Networking

GSC SECURITY
AWARENESS

Not everyone online is who they say they are.

REMEMBER

Everything known about you can and may be used against you

You should be aware that social networking sites are monitored by stalkers, criminal networks and security agencies.
While it's impossible to escape every social networking security threat out there, you should be aware of the 7 Fatal Blunders of Social Networking. The GSC Security Awareness Cell has produced this leaflet to help you significantly reduce the risks both to your private life and to the GSC.

1 Mixing personal with professional

This blunder is closely related to the first, but extends beyond the mere disclosure of GSC data. This is the case where someone uses a social network for both business and pleasure, most commonly on Facebook where one's friends include business associates, family members and friends. The problem is that the language and images you share with friends and family may be entirely inappropriate on the professional side. Remember that your actions online may reflect badly not only on your own image but potentially that of others.

2 Sharing work-related information

By sharing too much about the GSC's work on social networks, you may inadvertently reveal sensitive information about the GSC, its staff and its work.

Not only that, there is documented evidence that hackers (criminal and third state intelligence services) controlling legions of botnets are using data possibly acquired from your social network site, could be programmed to attack the GSC's defenses and, upon finding a weakness, exploit it to access data or sensitive information.

3 Engaging in Tweet (or Facebook/LinkedIn/Myspace) rage

For the person who is dissatisfied at work or who may have a disagreement with his/her line manager the urge to "let off steam" via social networks can be irresistible. Call this a blunder of rage.
Before launching into a verbal outburst online, be mindful of what you say and be aware that your audience is probably much larger than you intend it to be. So think twice about clicking 'submit' because the world may be looking at your angry rant for years to come.

4 Believing he/she who dies with the most connections wins

For some social networkers it's all about accumulating as many connections as possible. This may seem harmless enough or, at the worst, just annoying. But when the name of the game is quantity over quality, it's easy to click on a "friend" who may in fact be a scam artist, identity thief or foreign intelligence service. It is always advisable to verify the identity of the person who wants to get in contact with you. Do you know him or her? If not, why is the person trying to connect with you? Check if the profile of the other person is secured. If you can't retrieve a list of that person's connections, you have to ask yourself if it is really worthwhile contacting that person.

5 Password Laziness

Another common blunder is one of laziness. In this case picking passwords for your social networks that you're least likely to forget. In many cases, that means using the same password for LinkedIn and Facebook that you're using for your online bank account or work machine. If someone with malicious intent figures out the password for one social network that person can now go and access everything else. Using the same password on several sites is like trusting the weakest link in a chain
to carry the same weight.

6 Trigger finger (clicking everything, especially on Facebook)

Facebook in particular is notorious as a place where inboxes are stuffed with everything from drink invitations to requests for worthy causes. For some social networkers, clicking on such requests is as natural as breathing. Unfortunately, the bad guys know this and will send you links that appear to be from legitimate friends. Open the link and you're inviting a piece of malware to infect your machine.

7 Endangering yourself and others

All of the above tie into the seventh and perhaps most serious blunder, which is that reckless social networking can literally put someone's life in danger. It could be a relative or co-worker. Or it could be yourself.

Don't let this brochure scare you,
but you need to remain aware,
safe and secure when social networking.