

Your guide to **SAFE** social networking

IT Hackers now earn substantial sums of money by creating new-style viruses which attack your organisation through social networking channels. Take a moment to read through our tips to help keep your business safe from harmful IT viruses.



12 TIPS TO HELP KEEP YOUR NETWORK SAFE

- 1 Never!!** Send user names, passwords, or account details in reply to an email not even to your boss or IT Manager, or to someone posing as your bank - **it will be fraudulent.**
 - 2** Don't tell anyone your user name and password, treat it like your pin number - **keep it safe.**
 - 3** Attachments in emails have the potential to carry spyware and viruses, even Excel spreadsheets. If you don't know what they are or recognise who it's from **don't open it.**
 - 4** E-cards don't always bring glad tidings. If you don't know why you have it, or who it's from **delete it.**
 - 5** Some web links emailed to you could be for somewhere else entirely. See the example right. Hold your mouse over the address, don't click on it, if it displays another address don't click through to it - **it's a scam!**
- A screenshot showing a mouseover tooltip for a web link. The tooltip displays the actual IP address: http://192.168.255.205/wood/index.htm. Below the tooltip is the text "Example of a masked Web address".
- 6** If you are on a secure website, check the address in the address bar is an https address.
 - 7** Keep your computer up to date. Antivirus, programs, and MS updates.
 - 8** Friend or Foe? Be choosy about who you accept as a "friend" on a social network. Identity thieves may create fake profiles in order to glean information from you. This is known as **social engineering.**
 - 9** The more you reveal in profiles and posts, the more vulnerable you are to scams, spam, and identity theft. Only post information that you're comfortable sharing with **complete strangers!**
 - 10** Make your passwords difficult, never choose '**password!**' (Replacing letters with numbers helps. Ideally it should be a combinations of letters numbers and special Characters *!?,_ etc such as *pa55w0rd01*)
 - 11** Whose looking over your shoulder? **Change your password regularly.**
 - 12** E-corresponding means you can never be 100% sure who you are talking to. If an email looks odd be suspicious, delete it, or ring the sender and ask **was this you?**