Guidelines on giving out details to third parties

Social Engineering is the art of exploiting human behaviour to elicit sufficient information to be able to launch an attack on information security resources.

This may take the form of ringing up an institution and asking a variety of questions of a variety of people. Each individual is not aware that they give out enough information to be of use to a miscreant, but the total information gleaned from the variety of sources is sufficient.

For example, Kevin Mitnick, a convicted hacker, admitted that the majority of information he gleaned to assist in his hacking was through social engineering techniques.

Social engineering also covers situations where a person may wear a yellow protective jacket and be assumed non-suspicious when lifting a manhole cover in the street. Or someone takes up floor tiles in a large office and just says they are from the "IT department" fixing the cable, or a plumber looking for the source of a leak. They may be actually breaking a cable, installing extra equipment to intercept traffic or even be a terrorist leaving a bomb under the floor.

There follow a few suggestions for how to handle enquiries, in particular, from external sources:

1 Be cynical.

2 Try to identify who calls you. They often mumble their name. Ask for it if you don't catch it the first time and ask where they are calling from if they are external.

3 Don't believe everything they say - try to verify what you can.

4 Be aware they may try to pressure you by implying your boss has said they can get information from you - don't assume they are being truthful. This may be intentional or accidental.

5 Consider others' privacy - they may not wish to be hassled by cold calls from salespeople. If asked, e.g. "who deals with information security at UCL?", suggest they look at the UCL website rather than giving out an individual's name, email address or anything else they might not want to pass on.

6 Try to determine the nature of the call - if they are calling concerning a security breach, tell them to contact the Computer Security Team in the usual way (cert@ucl.ac.uk) - that's what they are here for. If they say it's about what they can provide, we are not interested. If they push (and they often do), offer to take their details and pass them on. If asked if you know who is in charge of an area or who might be interested in something particular, offer to take the caller's details and pass them on. A genuine caller would be grateful, someone who is trying to elicit information may choose not to give their details.

7 The bad guys often play on the differences in responses that may happen if they appear to be already known to you. They may say they have spoken to someone before, maybe don't remember their name, but know what they do. This all sounds very plausible, but treat them with caution. Do not take everything they say at face value. Similarly, if you receive a phone call or email that implies someone has already met you, don't assume that is the case - try to remember or ask them to provide some evidence. If you register

for a major seminar/exhibition and do not go, you may find you receive messages or calls that assume you went and play on the fact. You may receive such contact simply following a major event in your sphere of work on the assumption that you must have attended.

8 What may appear to be an innocent question when asked in isolation may be put together with answers to other innocent questions asked of others in the organisation and, in total, give out entire details of sensitive systems or internal procedures which can then be exploited.

9 Sometimes the third party is someone you know - maybe even in UCL. They may ask you to do something or give them something. This is a different type of social engineering. In such a case they may be trying to exploit their position to find something out without going through formal channels. For example, a request for someone else's password or access to their files in their absence. There is UCL policy governing such requests (see the UCL policy on monitoring) and forms are available to ensure proper authentication of such access to stay within the law.

There is a lot of useful information at the following:

http://www.getsafeonline.org/