Information Security Now - 5

John Mitchell

“Never write down, or disclose your password” is one of the most common strictures of the information age and yet one of the UK’s most senior professional body for internal auditing is urging its membership to do just that. I recently received a new membership card from the Institute of Internal Auditors (UK & Ireland) with boxes on the card for my user identification and password and the direction to complete these. The only sop to security was that I should store my card in safe place. The IIA used to offer a Qualification in Computer Auditing (QiCA), which is currently under review. Part of the syllabus covered computer security. Perhaps the IIA’s Membership Development Manager should read it? The whole problem (or is it ‘challenge’?) of computer security is the ease and willingness of trusting people to disclose useful information. The rise of community sharing sites, such as Face Book make it easy for the criminals to obtain that key bit of information required to validate your access credentials. How often do you select your mother’s maiden name as your validator to request a new password? This piece of data is easily available, even if not directly disclosed, from community and genealogy sites. The key to security is originality coupled with watchfulness and a healthy dose of paranoia.

I once needed to top up a phone card whilst working abroad. I called the free number clutching my credit card to initiate the top up only to be met with a request for my password from the so called help desk. When I declined to reveal it I was informed that my card could not be topped up. When I asked why they needed my password I was told so that they could validate me. I pointed out that I was giving them money and perhaps I should have proof that I was talking to a bona fide support person? The stand off was not resolved so they lost a customer. Ease of access and tight security is getting better with the increasing use of challenge/response one time pads. The advantage here is that the phishing of your access credentials means that you are still secure as the criminal lacks that important second factor. The problem is that I now have to carry three of these things with me on my travels and airport security are beginning to wonder whether this may be some plot to take control of the aircraft’s electronics. On balance however, I prefer the one time pad to the need to write down several different and complex passwords.

The phishing situation is not helped by the cavalier attitude of many of the on-line companies that I deal with. A message from one of my share dealing companies informed me that they were transferring my account to another company as a result of a take over. Would I please follow the supplied link to validate myself with the new company? Following the link required me to log-in. At that stage I stopped. The message contained a telephone number for me to call if I had any queries. Well, no one in their right mind is going to call a telephone number contained in a suspicious message so I had to dig out the number from my original sign-up to the service. It was different to the one in the message! I called to be told by an answering machine that all queries were now being dealt with by the new number. Was it a phishing attempt? No, it was the real thing, but I had wasted nearly an hour validating the authenticity of the message.

My ISP's security was compromised recently and my web site was loaded with a few items of badware. The first I knew about it was when a colleague in Australia emailed me with the results of a Google search which stated that my site could harm his computer. I quickly resolved the situation with my ISP (egg on their face), reloaded my web site from my secure copy and then asked for a review of my site. This was commandingly quickly done and Google searchers now no longer receive the warning. A good service from Google in identifying dangerous sites. Way to go boys.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.