Editorial

John Mitchell

My ISP is anxious to attract new subscribers so it presents these potential income streams with great offers. Cash backs, free wireless routers, discounted period, etc. What do us existing and reliable customers get? Nothing. Moving to a new ISP is pretty straight forward these days and like the interest rate tarts in the financial services sector the urge to move is becoming stronger with each offer that my ISP makes to potential customers. Surely they should start thinking about retaining their existing customer base, especially when one ISP has announced apparently totally free broadband? Okay, there are catches with this offer, but the message is clear. The underlying communication method should be “free” with the profits coming from the provision of value added services.

On the subject of service, I found out that I could now make an appointment with my doctor via the internet. So I registered for the service, very quickly received my access credentials and then tried to do the business only to find that the appointment site was down. So I whizzed off an email to the provided contact address only to receive a response that they could not let me know when the service would be available due to “patient confidentiality” and I should contact my surgery for help! So I blew my top and flame mailed them and received a slightly more reasoned reply that they could not deal with patients because there are too many of us. To which I pointed out that if that was the case why did they provide their contact details on the site? No response, but the service came up the next day and I made my appointment, which is a very useful value added service.

Some of you may have heard reports regarding an experiment conducted last Valentine’s day in London. The experiment carried out within London's business district revealed that employees in some of the City's best known financial services companies don't care about basic security. CDs were handed out to commuters as they entered the City by employees of an IT skills specialist and recipients were told the disks contained a special Valentine's Day promotion. However, the CDs contained nothing more than code which informed the distributor how many of the recipients had tried to open the CD. Among those who were duped were employees of a major retail bank and two global insurers. The CD packaging even contained a clear warning about installing third-party software and acting in breach of company acceptable-use policies - but that didn't deter many individuals who showed little regard for the security of their PC and their company.

Fortunately these CDs contained nothing harmful. No personal or corporate data was transmitted due to the actions of these individuals but the fact remains that

this could have been someone wanting to cause havoc in the City. Effectively the employees, by carrying the CD into the company and putting it into their PC, had by-passed much of their company's security. Employees have to recognize they are the first and easiest route into a company's network and social engineering of this nature requires no technical skill to bypass the company's firewall. Just last year Japanese bank Sumitomo Mitsui in the City allegedly fell victim to a spy ware infection which almost ended with the theft of £220m. That case should have highlighted the threat posed by applications entering the enterprise through unofficial channels and yet it appears few companies have taken note. The key here is 'education'. Regularly keeping all employees abreast of the latest scams is the duty of the company, it's officers and corporate security team.

Which leads me nicely into the phishing problem. I receive so many of these that when I received a message purportedly from the National Lottery I automatically consigned it to the rubbish bin. After all, it was suggesting that I should follow a link and provide my log-on details. So I dumped it, but a week later I realized that I had not received an expected (small) cheque for a recent win and so logged on to find out why. You will have guessed it already. The message from the Lottery people was to inform me that I had won and the reason for not receiving the cheque was that the money had been paid to my bank account! I had forgotten this last part it being so long since I had won anything, but the main point is that here was a legitimate message being rejected by me because I thought it was a phishing spam. A sort of self imposed denial of service being triggered by my own paranoia!

Which brings me neatly to this edition, where you will find a prediction on phishing activity from Vasilis Katos of Portsmouth university, while Bob Ashton, our Oceania correspondent, deals with the problems faced by IT professionals in keeping up-to-date. Mark Smith provides details of some member benefits he has negotiated on your behalf and Alex Brewer, our chairman provides an update on the Group's activities during the previous year. Jean Morgan our Treasurer gives you an insight to our finances, but Colin Thompson who provided the BCS Matters column for so many years has retired and I am in the process of searching out a replacement, so no news this time from our parent body.