Online security considerations and computer protection

I am in a very privileged position because I am trusted by my client's to not only work on and fix their computers, but also potentially to help them with some pretty serious computer disasters with not only their hardware, but also their personal data.

This month I am going to concentrate on two main topics of security: **1. Not falling for scams, fake phone calls and emails. 2. Protecting your online accounts with an up to date mobile phone number.**

So, I shall begin with my first point above, `**Not falling for scams, fake phone calls and emails**`. Recently I have had to deal with some particularly difficult data recovery operations because people have fallen foul of either a fake phone call or a fake email. I will not bore you all with the process, but simply try and help educate those that are most at risk. The basic rule is, nobody or very few genuine organisations are going to phone you up or email you to offer help when you have not requested help!

If, you receive a phone call offering help or advising you of a problem with anything at all, it is best to look their genuine phone number up (not to simply use an unchecked phone number or simply phone them back on the same phone number they just phoned you from) or you could decide to speak to a trusted professional and seek some advice. The same applies with emails; it is highly unlikely that a genuine establishment is going to contact you out of the blue to report a problem to you that you possibly didn't know about. If you, by chance do receive a genuine call or a genuine email and you chose not to either take the phone call or reply directly to the email, then no professional organisation is going to be offended as long as you contact them via a legitimate phone number or email address (I am not suggesting that you simply ignore something, I am suggesting that you are all cautious).

The second point is, ` **Protecting your online accounts with an up to date mobile phone number`.** These days more and more online establishments and organisations are requiring a mobile phone number as an extra layer of security for both you and them. So, it is absolutely essential that if you are using your mobile phone number in this manner, that you make sure that it is kept up to date or that you keep the same mobile phone number if you ever change providers. Because, if you do not keep on top of this security and forget to update websites or organisations with your correct and active mobile number, you are not only going to possibly prevent malicious activities, but you are very likely to block yourselves from carrying out an online task or maybe even a simple payment or transaction.

But, please remember this – if you give remote access to your computer to someone that just contacted you out of the blue, then you really should then expect major trouble with your computer or your online accounts after you allow them access. **Please just stop and think before you simply accept what they are saying to you!**

Ultimately we are all responsible for our own computer and communication devices and our own individual online security. The online security procedures are put their to assist us all, but it can only assist us if we all keep on top of it and understand that more and more criminals are trying to access our lives via whatever means that they can.

Information provided by Mark Dibben of Dibtech Computers in Devizes.
Web: www.dibtech.co.uk. Email: computers@dibtech.co.uk