Online shopping accounts, cloud accounts and online security considerations.

Many of us use online accounts and various types of cloud services with purchasing ability – this includes anything with your: bank details, card payment details, links to PayPal and any other form of remote payment method. If this is applicable to you, then this is worth reading – this article is only a guide.

Your online accounts are a target for potential fraudsters and hackers; these fraudsters are not necessarily after your stored data or even your email; although these are not exempt. But, the fraudsters are after your money and any bank payment details that are stored in any of your online accounts.

If you are one of the many people who use very easy passwords and even use the same password on multiple sites – then this article is even more important to you.

Obviously accounts such as: online banking, EBay, PayPal, Amazon and any shopping sites are the first ones that we think about with regards to money and hopefully security; but we must also consider other accounts such as Google and any online account where banking details are stored. Many online cloud services and shopping sites are linked to your banks either via cards or other payment methods and once a security issue is discovered by the potential fraudster, your money is at risk!

All of the main sites such as Amazon, EBay, Google and PayPal have extra layers of security in them that are available for you to activate, but unlike most banks, they are not activated in your accounts as standard and rely upon the individual user to activate them.

What am I talking about – well, I am referring to links within these online accounts that enable your mobile phone to be added in as an extra layer of security – this works when you make a purchase or login and your respective account sends a text message to your registered mobile phone number to either allow access or to allow for a purchase. Obviously it is absolutely essential that you know your own mobile phone number, understand how to read and use text messaging on your mobile phone and always have your mobile phone number updated on all relevant sites.

If you do not use this extra layer of online security and if: your password is either weak, used on multiple sites or compromised and a potential fraudster gains access to anyone of your online cloud, shopping sites or any site where your payment methods are stored, then they can then access your money and purchase either items or online services.

The thing to remember is, even if you have additional protection in your online bank accounts, because services such as PayPal and Google Pay contain your banking and card details, then sometimes once these accounts are fraudulently accessed your bank doesn't always question the transaction unless it triggers the bank to send you a text message. If the security trigger with your bank doesn't happen then your payment will go through until you spot the transaction and contact your bank – then, your bank will decide what should be done in consultation with you. More than likely your card/s are then cancelled and replaced.

Your next actions and considerations are: how did this happen, is my online security good enough, are my passwords strong enough and hard to guess, where did the security breach take place and how can I protect myself and my money better now and in the future?

Ultimately we are responsible for our own individual security and we all need to be more aware of what can go wrong before it goes wrong and implement better security measures.

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