Staying Safe Online

Recently within Berkswich we have become aware of an increase in scam calls made to members of the church. It would therefore seem to be opportune to remind everyone of safe practices online.

There was a poster in the church hall that advised us “Don’t be rushed, don’t be hushed” which is good advice. Try not to do anything in a hurry as we all take less care when hurried. And also seek advice from someone you trust if in any doubt, don’t stay silent.

You may receive a telephone call, or an email stating that either your computer has a virus, or that your internet connection has been compromised. This is total bunkum, and the aim of the caller is to get you to login to a specific webpage so that they can download spyware onto your computer. Spyware will record what you do on your computer and send the details to the scammer. What they really want to do is to find out your banking details so that they can steal from you. There is no easy technological way that a caller can associate a computer with a telephone number, and the major internet companies are far too busy to worry about an individual’s computer. So simply hang up the phone, or ignore the email. The caller may well become insistent stating that you have illegal images and data on your computer. This is all part of the process to unsettle you and make you act in a hurried way. So, ignore the threats and hang up. If you are really worried by such a call, feel free to ask one of the tech team at Berkswich Church and we will arrange for your computer to be scanned for viruses.

You may also get an email claiming to be from someone you regularly pay bills to. I have been caught out previously when I received an email supposedly from Virgin, claiming that my direct debit for my broadband had not gone through, and they would cut my connection in 24 hours (being rushed!!!). The email asked me to amend my direct debit details on a form that looked very authentic. Of course, that meant filling in all my details on the fake form. I was very busy at the time and distracted, and it was only when I paused and stopped to think that I averted what could have been a very expensive mistake. Of course, if in doubt, ring the company’s customer help desk and talk directly to them.

Remembering that the principal aim of the scammers is to discover your banking details, so be especially cautious if you receive a call or text claiming to be from your bank. These days banks tend not to phone customers directly, but write to them instead. So, best advice is always to put the phone down, and call the customer help desk from another phone, looking up the right number yourself on your bank card or bank statement. Checking the validity of the call. At no time will anyone ask the PIN number of your card, or your internet banking password and you should never tell anyone these things.

Also, be very careful with the direct transfer of cash through the internet banking services. I tend to transfer a small amount, say £5, and then contact the recipient to ensure that they have received the money. Once the link is established I have some confidence in sending larger amounts. However, it is more prudent to pay people using cheques or by using your bank cards, both of which are covered by insurance.

And obviously, if you get an email asking for help to transfer a large amount of money and promising a percentage, or indeed a surprise email from someone who is away asking for emergency money, then my advice is to ignore it, or at least do some quick checks before committing yourself. The phrase “if it is too good to be true, then it probably is” is a useful reminder.

Finally, some advice and good practice.

1. Make sure that you use an anti-virus program on your computer and that it is updated automatically.
2. Make sure that your internet banking password is unique and not used for other things. I would suggest using a phrase rather than a single word and swapping out letters like “@” for “a”, “3” for “e” and such like.
3. I would suggest that you change all important passwords at least once a year. I have recently received an email which told me my old password, and I was reassured that I no longer used that password.
4. If you are contacted by a scammer regarding your bank account, tell the bank. They may well cancel your visa card and issue a new one, but they will certainly advise you.
5. If you are contacted by phone, email or text by a bank or any other supplier, do not give or confirm any personal info. Instead find their customer services number yourself on your bank card, or invoices, and call them yourself. Ideally from a different phone.
6. Always ask any visitors to show you their ID … and if any doubt ring up the company to check.
7. And again, “don’t be rushed, don’t be hushed” as there are people in the church who can help.

Mark Timothy