PRECAUTIONS RELATING TO ONLINE BANKING

1. Consider which bank is best for you

Some banks offer a small device that can be used to generate a unique code each time you log in. This code is only valid for a very short period of time and is required in addition to your login credentials in order to gain access to your online account. These banks may suit someone who is regularly required to make payments online when away from their office.

Other banks install a digital certificate onto a specific machine and electronic payments can only be effected from that machine. These banks may suit someone who normally carries out their banking in the office and is rarely required to effect a payment when they are absent.

Ensure that your bank offers some form of two factor authentication for online banking.

Discuss with your bank the type of security they have in place and other best practices it can recommend based on its systems. For example, some financial institutions offer specialised software which is designed to protect both the financial institutions themselves and their customers against cyber attacks

Also, familiarise yourself with the protection and processes the bank provides to business accounts in the event of losses.

2. Personalise your settings

If possible implement dual payment authorisation & payment limits. This increases the difficulty for criminals to give effect to the transfer of large sums from the bank account.

Unless your practice regularly makes international payments, turn them off (where possible). The payments can be made in branch if required on an irregular basis.

Some banks offer a facility for customers to set up text or email notifications to alert them to certain activities on their account. For example, if a withdrawal matches or exceeds a specified amount or the account balance dips below a certain point then a message will be sent. Such alerts could give quick notice of suspicious activity on your account.

3. Access your accounts from a secure location

It's always best practice to connect to your bank using computers and networks you know and trust. Consider designating a single computer to use as your business's online account machine. This computer should solely be used for online banking and not for other activities such as e-mail, web browsing, or file sharing.

If you need to access your bank online from remote locations you might want to set up a VPN (Virtual Private Network) so that you can establish an encrypted connection to your home or work network and access your bank from there.

Look for a small padlock icon somewhere on your browser and check the address bar – the URL of the site you are on should begin with 'https'. Both act as confirmation that you are accessing your account over an encrypted connection.

Be cautious if you use open Wi-Fi such as those provided in hotel lobbies, Starbucks etc.

Try to avoid using Internet cafes or a computer that is not your own.

4. Monitor your accounts regularly

It should go without saying that monitoring your bank statement when received is good practice as any unauthorised transactions will be identified on a timely basis. Take advantage of the feature in online banking and check your account on a regular basis. Look at every transaction since you last logged in and, if you spot any anomalies, contact your bank immediately.

5. Always log out when you are done

It is good practice to always log out of your online banking session when you have finished your business. This will lessen the chances of falling prey to session hijacking and cross-site scripting exploits.

You may also want to set up the extra precaution of private browsing on your computer or smart phone, and set your browser to clear its cache at the end of each session.