

Security Update: 'Phishing Attacks' hit

It has been brought to our attention that a number of incidents known within the industry as 'Phishing attacks' have taken place worldwide. This security update is intended to recommend best practices for customers when participating in Internet banking, or receiving spurious e-mails purporting to be sent from banks.

Below is a list of precautionary measures that we advise you to take when banking online.

1. Do not respond to e-mails purporting to be from your bank that request you reply with your password or personal details. Always contact your bank on a phone number that you know is genuine to confirm the e-mail is genuine.

2. Wherever possible never disclose personal information or account history information over the Internet such as:

- ~~///~~ ATM PIN – Personal Identification Number
- ~~///~~ Account Passwords (unless you are confident it is the bank and for on-line banking use).
- ~~///~~ Credit Limit (on credit card)
- ~~///~~ Last five previous purchases
- ~~///~~ Passport/Driving Licence details
- ~~///~~ The above points (excluding ATM PIN) may sometimes be used but only once inside the security of your Bank's on-line banking service

3. Shop on-line with reputable companies as you would in the physical world. If you feel suspicious of a site or it does not meet your expectations and you don't feel comfortable providing your account details, then leave this site, check the validity with your bank, and, if still unsure, shop elsewhere.

4. Make sure you are able to contact the retailer in the event of a dispute or query. Make sure there is always a valid address/telephone number.

5. If you are using the Internet in a public place like a library, airport or cyber café, ensure no one is watching you type passwords and do not leave it unattended while logged on with your user name or whilst in a secure site. Always secure the PC before leaving it for any length of time.

6. You should not change secret information such as your on-line banking passwords if you are in a public place like a cyber café.
7. Choose passwords that are unrelated to your birthday or family members. If possible, choose alphanumeric passwords (characters and numbers).
Do not write passwords down or disclose them to anyone else.
8. If you think your password has been compromised, then change it immediately.
9. Consider using Anti-Virus software or installing a personal firewall, which will help prevent unauthorised persons accessing your PC and guard against Viruses.
10. If you suspect any personal details regarding you account have been compromised then contact your member bank immediately.