MANSFIELD
BUILDING SOCIETY

Online Security

At The Mansfield Building Society we take the security of your information very seriously and detailed below are some helpful hints and tips to help keep your personal information and your online activity secure.

1. Secure Pages

Not all websites are secure and you can always tell whether or not a connection is secure.
Secure website addresses usually begin with the letters https: and your browser will display an icon, usually a closed padlock 🔒 or an unbroken key 🔑

These symbols are good indicators that you are visiting a trusted site but you must be aware that bogus web sites do exist and therefore you should never follow a link in an email to the Society's website. Please ensure that you type our website address www.mansfieldbs.co.uk into your browser manually.

2. Keep your security details safe

Keep your User ID, Password, Memorable Data and Account Numbers safe at all times. Avoid writing your User ID, Password and Memorable Data down. If you write them down because you think you might forget them, make sure it is in a way that will not be readily identifiable by someone else and keep them in separate places. Never disclose your security details to anyone, even if you share a joint account.

The Society may ask for your User ID to help identify you on our system, however we will never ask for your Password and Memorable Data. We strongly recommend that you change your Password and Memorable Data regularly.

2. Phishing Emails

Fraudsters can also target customers using bogus emails which encourage you to follow a link from the email to a spoof site to re-register, sign in, confirm or change your security details. The Society will not contact you in this way to use its online system or ask you to change your online information. If you receive any email asking you to do this please contact us immediately.

3. Trojans

Trojans are destructive programs that contain malicious codes designed to give control of your computer to a hacker. Typically these are installed on your computer through an email that is sent asking you to click on a link to a website which looks like it is under construction. If the site is not genuine, a program may be downloaded onto your PC which can then be used to record your keystrokes the next time you sign on, and send them to the hacker. This has the potential to capture your security details.

4. Log out properly when you have finished using our Online Service

Do not leave your computer unattended when you are accessing your account online. For your security our online system, ClickMansfield, will automatically log you out if you do not use the sys-tem for several minutes.

5. Use secure messaging rather than email

As email is not a secure form of communication, it is safer to use the Secure Messaging Service, accessible from within ClickMansfield, when enquiring about your account.

6. Protecting Your PC

Ensure you have up-to-date Anti-Virus software

The Society strongly recommends that you have up to date Anti-Virus software installed on your PC. The more superior Anti-Virus programs have an Auto Update feature which updates your software to protect you against the latest viruses.

Protecting against Spyware

Spyware is a general term for hidden programs that invade your privacy. They collect information about you and send it over the Internet without your permission. Sometimes it can hijack your computer and display unwanted advertising pop-ups. Spyware can slow down your computer and internet connection and at worse can pass on security details to criminals. The Society therefore suggests that you run an Anti-Spyware program frequently to remove any threats.

Anti-Spyware programs can be downloaded free of charge from the Internet.

Protect yourself using a Firewall

Firewalls are programs that protect your computer against unauthorised traffic to and from your computer and block unwanted internet activity. Like Anti-Virus software, Firewalls can be purchased from most computer stores and can be purchased from the Internet.

Avoid using computers in public places

You should avoid logging on to a secure site using a computer in a public place as you cannot be certain about the computer's security.