Capital Credit Union

Online Banking Terms and Conditions

- The terms and conditions that apply to internet banking are in addition to the terms and conditions that apply to your account with Capital Credit Union. Copies of the standard terms and conditions are available on our website, at the Capital Credit Union office in Edinburgh, or by contacting our Member Services Team on 0131 225 9901.
- When you register for internet banking you will set up a password, which will only apply to Internet Banking.
- It is your responsibility to protect your access password to ensure that no one else can access your accounts.
- For security reasons do not write down your access password or keep it with your account information.
- Do not disclose your access password to third parties (including family members). You should change your access password on a regular basis to ensure that it is secure (this can be done through your online account).
- Do not use internet cafes or public access internet terminals to conduct internet banking or use any other internet terminal where you cannot verify that the virus protection is up to date and that firewalls have been installed. Capital Credit Union will not be liable for any unauthorised transactions that result from your login details being compromised from such a source.
- Capital Credit Union will NEVER ask you, via email, or telephone, or any other way to divulge your internet banking Access Password, nor shall we ask anyone to do this on our behalf. If you respond to such an email purporting to be from Capital Credit Union, we will not be liable for any unauthorised transactions. A number of financial services and portal sites offer you the convenience of displaying all your account details on a personalised web page. These sites need your member or account number and access password to your Capital Credit Union accounts so that they can interrogate our system and display your details back to you. Capital Credit Union can take no responsibility for unauthorised transactions that may arise as a result of you disclosing your member or account number and access password to other parties. It is your risk if you give your access password to an account aggregation service.
- Should you become aware of the loss, theft, or possible unauthorised use of your access password you should immediately change your access password for internet banking, and contact Capital Credit Union.
- Capital Credit Union is not liable for any loss or consequential damage if you use internet banking to access your Credit Union accounts or to perform transactions on your Credit Union accounts.
- If you have been reasonably aware of the loss, theft or unauthorised use of your internet banking details or access password and you have not advised Capital Credit Union of this loss, theft or unauthorised use of the said details or access password Capital Credit Union will not be liable for any unauthorised access to your account information or to any transactions processed using internet banking.

- Whilst every effort will made to ensure that the internet banking service is available 24 hours a day, there may be occasions that the service will not be available due to system maintenance, system failure or network problems beyond our control.
- If Capital Credit Union suspects fraudulent activity or unauthorised transactions on your account we will temporarily freeze your internet banking access and/or stop payment on any suspect transaction until we can contact you and receive confirmation that is satisfactory to us that the transaction may proceed.
- By using our online banking service you will not acquire any ownership rights, title or interest in or to the software made available to you. You must not:
- do anything which may damage, interfere with or disrupt the software or the way it is provided; or
- display, alter or use any trademarks without the owner's prior written permission
- The services provided within online banking and the site content, including these terms and conditions are subject to change by us without notification.

Important Information - It is essential you take the time to read this security warning

- Clients can check that they are linked to Capital Credit Union internet banking by:

  Observing the locked padlock symbol located in the bottom right corner of their browser.

  Clicking on the locked padlock symbol to check the certificate.

- To ensure that no one else can access your account information through internet banking, it is important to select a password that is difficult for someone else to guess. For security reasons, do not keep your access password with your account information, or disclose it to anyone else and change it regularly.
- It is important to "log-off" from internet banking if you are leaving your computer unattended for a period of time. This will prevent unauthorised access to your account information. As an added security precaution internet banking will "log-off" automatically after 10 minutes if your internet banking session is inactive.
- Also we require that you do not use AUTO-COMPLETE to save your passwords. This would allow others to access your account after you have used the computer.
- Ensure that you have current anti-virus software and a personal firewall. There is also a government website which features a wide range of information on all types of internet fraud and how to prevent becoming a victim.

- Be very wary of installing software or running programs of unknown origin - particularly if downloaded from the internet as this is the principal source of "malicious" programs that pose a serious risk to your personal information.

Do not accept links or redirections from other websites or media for the purpose of logging onto the Capital Credit Union website, particularly for internet banking, Phishing and Internet Banking

- 'Phishing' is the term used to describe what the wide net cyber-spammers use to generate messages that ask recipients to reveal personal details or they depict an urgent scenario, offer or event to entice the user to click a link. Links may contain dangerous payloads may upload dangerous codes to computers and capture personal details.
- Some banking websites have been ghosted or 'spoofed' in the past to appear as if they are a real site, you should always check for the https in the address which denotes you are at a secure site. If the Capital Credit Union site looks strange or different in any way disconnect and report it to us immediately.
- If you receive an email message from a sender that you do not recognise or with content you do not know - delete it immediately.
- Perpetrators will use immediate alerts or urgent response mechanisms to entice you to reveal your details, always confirm any message reportedly from us BEFORE responding even if the message is headed urgent or stresses that your banking links or cards will be rendered inactive.
- Email spam messaging can contain dangerous payloads in the form of computer viruses that capture your personal banking details. If you suspect that this has happened to you or you suspect that your details may have been compromised you should tell us immediately.

Identity Theft

- Identity theft is fast becoming a major issue for financial institutions and their customers.
- Identity Fraud can take many forms, it can be perpetrated in a number of ways including:

  Take-over of a valid identity of a customer using valid channels such as Internet banking, Telephone banking, bill payments, account opening, lending applications via remote sources and changing customer contact details.

  Theft of a valid identity and attempt to open an account in the customer's name using the stolen and sometimes altered documentation.

- In dealing with possible identity theft issues, Capital Credit Union may have to ask for additional proof of identity for certain types of transactions

and although this process may cause some inconvenience for you, it is an essential action Capital Credit Union must take to protect your funds.

- Some of the requests that may require heightened proof of identity include:

  Almost all non face-to-face requests (phone, email, fax etc)

  Requests to change address (may also require other proof of this change)

  Third party introduced lending and account applications where original documents have not been seen by us

  Requests for issue of debit card or internet/phone banking access (particularly over the phone)

- To minimise your risk of identity theft:

  Never carry your identification documents such as your birth certificate or passport in a wallet, case or handbag unless you need them.

  Ensure you retain any personal records and other financial documents such as statements and receipts in a secure place and shred any documents which are no longer required.