

SMS One Time Password

Even if your usual Access Code has been compromised, a fraudster doesn't have the One Time Password and cannot complete the LogOn. The SMS also alerts you that the attempt has been made!

How does it work?

Normally when you log on to Internet Banking, you use your Log On ID and Access Code.

If a fraudster manages to compromise your PC with a virus, or if someone else learns your codes, they may be able to log onto your Internet Banking as if they were you.

With One Time Passwords (OTP's) you need a second password to log on. The OTP is randomly generated and only valid for one log on. This password is sent to you by SMS at the time you are logging on.

A fraudster will not be able to transfer any funds from your account because they don't have your mobile phone to receive the SMS code.

SMS OTP also acts as an alert for you when an unauthorised log on is attempted - saving your money and giving you peace of mind!

If you receive such an alert contact us by calling your branch or emailing info@gmccu.com.au

Security
as easy as
1-2-3...

To register:

1. Log on as usual

Log On to Internet Banking by using your usual Log On ID and Access Code.

2. Request

Choose 'Security Options' from the 'Other' menu.

Select 'Request' and choose your mobile number.

3. If your mobile is not listed

If your mobile is not listed, you will need to contact your branch to let them know your mobile phone number.

▶ protect your account from fraud

▶ easy to use

▶ no charge

Please Sign On...

An SMS One Time Password has been sent to your mobile number.

Enter One Time Password:

Sign On

Logout

If you do not receive an SMS One Time Password, Logout and try again.

Call Customer Service if you continue to have problems.



To Use:

1. Log on as usual

Begin to Log On to Internet Banking by using your usual Log On ID and Access Code.

2. Receive SMS

A One Time Password will be sent to your registered mobile phone number in a SMS message.

Your computer screen will ask you to input the OTP.

3. Do your banking

Your Internet Banking will only open if the correct One Time Password has been input.

Security Tips

The GMCU recommends that you take these steps to safeguard your accounts;

Cards

- Keep your card in a safe place,
- Sign your card as soon as you receive it,
- Never lend your card to anybody,
- Immediately report the loss, theft or unauthorised use of your card to the GMCU or to the Hotline on 1800 224 004,
- Keep a record of the card number and the card hotline telephone number with your usual list of emergency telephone numbers.

Secret Codes (PIN / Password)

- We recommend against recording your code anywhere. If you do, you must;
 - never write your PIN on your card; and
 - store your code, member number, card and logon details in separate places.
- never tell anybody your code,
- Never select an obvious code such as a dictionary word, name, familiar date (eg birthdate), car registration number or any other character combination that could be associated with you,
- Use care to prevent anyone seeing your code being entered at an Electronic Funds Transfer (EFT) terminal, ATM or PC,
- If you believe that another person knows your code, change it immediately or report the matter to us.

Internet Banking

- You have a responsibility to exercise reasonable care to prevent unauthorised access to the computer you use for GMCU Internet Banking,
- Check your last log-in details every time you log into the GMCU Internet Banking and notify us immediately if the last log-in details are incorrect,
- Keep your PC healthy with updated virus protection and firewall security.

General Security

- Examine your statement immediately upon receiving it and report any transactions which you have not authorised,
- Investigate your transactions if you notice an irregular balance during Telephone / ATM or Internet usage.
- Immediately notify us of any change to your address.

Further Information

Any additional information you require in relation to financial services can be obtained by contacting GMCU.

Registered Office 91-95 Fryers St,
Shepparton, Vic, 3630

Mail Address PO Box 860,
Shepparton, Vic, 3632

Phone 5821 9033
Facsimile 5822 1267
Email info@gmku.com.au

Web site www.gmku.com.au

Branches

| Location | Telephone | |
|---------------------------------|-----------|------------------|
| 91-95 Fryers Street, Shepparton | 5821 9033 | rediATM |
| 30-32 Bridge Street, Benalla | 5762 3380 | rediATM |
| 2 / 130 Hare St, Echuca | 5482 5333 | rediATM * |
| 36 Binney Street, Euroa | 5795 1771 | |
| 85a Sydney Street, Kilmore | 5781 1221 | rediATM |
| 145 Allan Street, Kyabram | 5852 2211 | rediATM |
| 112c McLennan St, Mooroopna | 5825 1999 | rediATM |
| 102 Melville Street, Numurkah | 5862 2894 | rediATM |
| 72 Station Street, Seymour | 5792 1075 | rediATM |
| 33 Cowslip Street, Violet Town | 5798 1761 | rediATM |

Agency
1 / 46 Downey St, Alexandra 5772 1915

* Echuca rediATM located at
Beechworth Bakery
513 High Street



v(1.1) Information in this brochure is current at 26 September 2009. Goulburn Murray Credit Union Cooperative Ltd ABN 87 087 651 509 AFSL 241364. Terms and Conditions available on request. Fees and Charges may apply. Your needs and financial circumstances have not been taken into account - you should consider the Product Disclosure Statement which is available from your branch before acquiring a product.

Internet Banking Security



Goulburn Murray Credit Union

A DIFFERENT KIND OF BANKING