Important Security Information

South West Slopes Credit Union Ltd
The security of the Online Banking is a high priority with South West Slopes Credit Union Ltd. We have loaded this pop-up page because we believe the security issues detailed below to be important. This page uses a cookie to ensure that it is only displayed once, so as not to inconvenience you. We apologies if this is not the case.

Known Threats
There are several methods being used by thieves to target Online Bank accounts. The most common are listed below.

Phishing
You receive an email purporting to be from your bank. Messages are various but will prompt you to follow a link to our internet banking site. In fact if you follow the link it will take you to a "ghost website" that looks like ours. When you log on, your keystrokes will be captured by the thieves and then used to siphon money from your account.

An example of one commonly used message is: "Dear User. We confirm that today the amount of $832.25AUD has been debited from your account. The message includes a link, apparently to our website. Human nature being what it is, there is a great temptation to click on the link to find out where this apparently unauthorised debit has gone. In fact the link either goes to a ghost website or contains a hidden key logger which infests your computer and may be called up when you log on to our legitimate banking site.

Trojan horse
A program that pretends to be something it's not. Like the original Trojan Horse, it contains something hidden inside it a malicious program. These programs can damage your computer or might contain a key logger which can even be turned on to capture your keystrokes next time you log on to the official banking site.

Spyware
This is software that gathers information without you knowing. It can enter your machine as a software virus or as the result of installing a new program.

Virus A malicious software program that invades your computer. There are many viruses. Some cause damage to your computer; others use the infected machine’s internet connection to launch an attack on another computer or computer network.

A particularly serious virus is one that records key strokes and logs your activities; including your Internet banking numbers and passwords, network passwords and credit card numbers entered into online shopping sites. This information is then sent back to thieves who may use it to siphon your account and make purchases on your cards.

To Protect Your Banking Details
South West Slopes Credit Union Ltd urges you to:

- Install a personal firewall
- Run latest anti-virus software
- Delete all unsolicited emails
- Always type in our address when e-banking
- Never follow a link to our website

How to Protect Yourself
To ensure your e-banking is secure, follow our Golden Rules:

- Always log on to e-banking by typing http://www.swscu.com.au or https://online.swscu.com.au
- Always exit your e-banking session when finished, by clicking the Logoff Button in the top right-hand corner of the window.
- Always check there is a padlock symbol on the bottom right corner of the log-on page (where you enter your PIN and Access ID).
- When logged onto CU Online, always check the address field shows our official website, https://online.swscu.com.au.
- Never follow an email link which takes you directly to a log-on screen.
- Never divulge your PIN. South West Slopes Credit Union Ltd will never ask you for your PIN (either in person or by email).
- Ensure your computer is protected by up-to-date anti-virus and personal firewall software.
- Only conduct financial transactions online using computers you know are secure. This means that use of internet cafes should be avoided.
- Never leave your computer unattended while logged on to e-banking.
- Regularly check your account balances and transaction histories and immediately report any discrepancies to SWSCU.
- You should protect the security of your PIN and Access ID at all times. If you believe your details may have become known to another person, you should log on to our e-banking site immediately and change your PIN.
- You should immediately be suspicious of any phone call, email or correspondence which asks you to disclose your banking details. The staff of South West Slopes Credit Union Ltd should never , for example, ask you for your PIN (although in some circumstances we might ask you to verify your membership number).

If you receive a suspect email
Do not open it.

Delete it from your Inbox and then permanently delete it from your Deleted Items folder.

If you have clicked on the link in the email:
Use your virus protection software to scan your computer for viruses and Trojans.*

After scanning your computer, contact the staff at your local South West Slopes Credit Union branch who can, if necessary, reset your Access Code.

Once you are certain your computer is virus-free, we suggest you change your e-banking PIN for peace of mind.

* It is critical that you ensure your computer is free of viruses before logging on to e-banking. If you have any questions about virus protection, please contact your software vendor or your internet provider.

Contact us if you have a concern
if you believe your e-banking details may have been compromised by one of the methods above; please contact the staff at your local branch. Alternatively, you can alert us of any suspicious activity you have witnessed by emailing us here.