Gateway bank | For your pocket & your planet

January 2024 Issue #76

gatepost

155635

A Message from the CEO

528090

Happy New Year to all our members.

Thank you to the members who provided valuable feedback in our 2023 Annual Member Survey. We take great pride in our strong member satisfaction scores and place huge value on the insights you provide us on how to continuously improve. I'd also like to thank members who took part in our 2023 Annual General Meeting in November - it is always good to meet members in person.

In this issue of Gatepost, we have some important information about scams and social engineering, as being scam aware is increasingly important. We also share the results of the 2023 AGM and Annual Member Survey.

Lexi

731330

2023 Annual General Meeting

Thank you to the members who attended Gateway's Annual General Meeting on Thursday, 23 November.

We would like to congratulate Peter Binetter and Lianne Bolton on being elected to the Gateway Board.

Annual Member Survey 2023

From satisfaction levels to suggestions for improvement, the annual member survey is a crucial tool in understanding our members' needs. As we delve into some of the key findings, we express our gratitude for your participation in helping us improve our service.

Member Satisfaction

84%

Extremely satisfied or very satisfied

Advocacy

57%

Told us that they have recommended Gateway to someone else

Right the First Time

93%

Told us we got it right the first time

Be #ScamAware. Check for tricks before you click.

In 2022, Australians lost a record $3.1 billion to scams, with an 80% increase in losses compared to the previous year, according to the Australian Competition & Consumer Commission (ACCC).

To help protect yourself, we've listed some common scam techniques that involve social engineering, which is a psychological tactic that cybercriminals use to manipulate people into divulging sensitive information. Unlike traditional cyberattacks, social engineering relies on exploiting human psychology and emotions like fear, curiosity, and trust.

935690

Examples of Social Engineering Attacks:

1. **Phishing Emails:** Scammers send fraudulent emails that appear legitimate, tricking recipients into revealing sensitive information or downloading malicious software. Be cautious of unsolicited emails and always verify the sender before clicking any links or entering any information.

2. **Phone Scams:** Scammers use tactics like spoofing and caller ID manipulation which disguises phone numbers, making them appear as legitimate entities like banks on the caller ID. Be wary of unsolicited calls, even if the caller ID appears trustworthy, and hang up immediately if you feel uncomfortable or suspicious.

3. **Pretexting:** Scammers create false scenarios to gain victims' trust and extract information. They may impersonate bank representatives or create false emergencies. Always be cautious of unsolicited requests for information and always verify the identity of the person making requests.

4. **Baiting:** Attackers offer enticing incentives, like gift cards or free software downloads, in exchange for personal information or access to your device. If it seems too good to be true, it probably is. Always verify the identity of the person or company making the offer.

5. **Impersonation:** Scammers pretend to be someone trusted, like family members, friends, or coworkers, to manipulate victims into providing sensitive information. Be sceptical and verify the identity of anyone requesting information or money.

What to Do If You Suspect You Have Been Scammed:

- Cease Contact: Stop all communication with the scammer and do not provide any further information or money.
- Report the Scam: Report the scam to the appropriate authorities, such as the ACCC's Scamwatch website or your local police.
- Protect Your Accounts: Contact your bank if you shared sensitive information. Change passwords and enable two-factor authentication for your online accounts.
- Consider Credit Monitoring: Enrol in a credit monitoring service to detect unauthorised activity or identity theft attempts.
- Educate Yourself: Learn about common scams and how to protect yourself from them in the future.

At Gateway Bank, we prioritise your privacy and security. If you ever think you've been impacted by a scam, please contact Gateway's member services team immediately on 1300 302 474 (8am - 6pm AEDT, Monday to Friday). For further security updates, visit gatewaybank.com.au/onlinesecurity.

144420

Climate Active Carbon Neutral ORGANISATION

Printed on 100% recycled paper

Spot your Member number to win $50*

If you find your own Gateway Member number printed in its entirety in this edition of gatepost, you are a winner. Call our Customer Service team on 1300 302 474 before 31 March 2024 and your Gateway account will be credited with $50.

Note: Five different Member numbers have been randomly selected and printed in this edition of gatepost.

*Eligibility is limited to current Gateway Members aged 16 years and over.