

Notice to Members: Update on cyber incident

29th July 2025

Earlier in 2025, we wrote to current and former members to notify them of a cyber incident which St. Agnes Credit Union had recently become aware of. As communicated at that time, we identified that the Credit Union had been subject to a personal data breach, in which a third party gained access to an employee's email account and used that access to send phishing emails purporting to be from the Credit Union.

Upon becoming aware of the incident, we took steps to remove the third party from our systems. We also engaged external legal, IT and forensic support to investigate and resolve the incident and to review the affected data and this exercise has concluded. On foot of this assessment, and in accordance with our obligations under data protection law, we contacted a small number of individuals whose personal data had been affected and who we considered to be at a heightened risk as a result of the personal data breach.

In addition to these notifications, we wish to reiterate our previous advice regarding the risk of phishing attacks and confirm that the security of member accounts was not compromised by the incident. Please note that we will never send texts or emails with links requesting you to disclose personal details or share PINs/passwords for online banking. We continue to advise you to remain vigilant and to familiarise yourself with the usual fraud prevention advice, details of which we have set out below. In particular:

- Hang up and do not engage with any unsolicited communications or calls (whether purporting to be from St Agnes Credit Union, any other financial institution, State body or any third party) to avoid falling victim to 'scams'.
- Do not click on suspicious links or open attachments from unsolicited or suspicious communications as these could compromise the security of your mobile phone, email or computer.
- Do not provide any personal or confidential information in response to an unsolicited communication or call. Never provide your account login details (such as PIN or password information) to any third party including via SMS, email or over the phone.
- If you wish to verify whether any particular communication is genuine, you should contact the sender using the details published on their website, as those provided by the sender or caller during a call or from an unsolicited communication may be fake.
- If you receive any unsolicited communication from St. Agnes Credit Union, you can contact us to confirm if it is genuine. Our contact details are available on our website and are also below.
- If you believe that you are a victim of fraud, immediately contact us and report to your local Garda Station.

For further information, the National Cyber Security Centre (NCSC), An Garda Síochána and the Banking and Payments Federation of Ireland have published guidance to educate the public about how to protect yourself from fraud which are available on the Fraud Smart website and on the NCSC website. Links to these guides are available below.

We wish to assure our members that the safety of their information remains our top priority. Please contact a member of staff at 014555670 or email info@stagnescu.ie should you have any questions or concerns.

Guides

[NCSC Quick Guide Phishing](#)

[Fraudsmart TOP 10 TIPS 2023](#)

[Fraudsmart Personal Brochure 2024](#)