Australasian Research Management Society

Dear ARMS Board, Convenors of Standing Committees, SIGs and Networks,

In recent weeks, we have received reports from members about the receipt of scam emails, where attempts have been made by the scammer to trick individuals into giving out personal information or request that funds be transferred into fictitious bank accounts. The scammer typically contacts an individual pretending to be from a legitimate business or even a fellow ARMS colleague. Contact may also be made via social media, phone calls or text messages etc. Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is pretending to represent, including their branding and logo.

If you have received an email from someone posing to be an ARMS member – for example, the President, COO or even a general colleague requesting personal information or funds be transferred into an account, this is likely to be a scam and we ask that you report this to our office immediately.

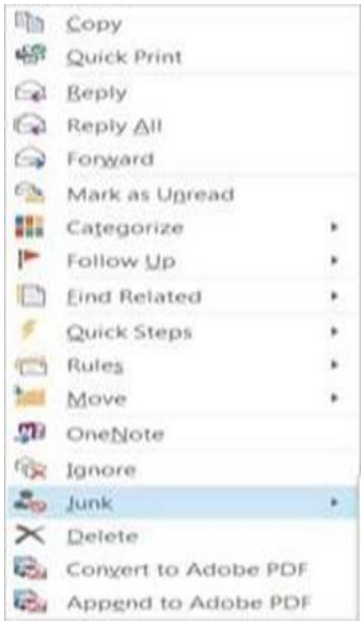
Our office cannot and will not transfer funds into an account or provide personal details without all of the required documentation (invoice, reimbursement request from a relevant and legitimate source). The Executive Office does not give out personal or sensitive information about our members without authority from the individual and complies with our Privacy Policy.

How to protect yourself?

Here are some suggestions to help avoid being scammed:

- ✓ Do not click on any links or open attachments from emails claiming to be from your bank or another trusted organisation and asking you to update or verify your details – just delete the email entirely.
- ✓ Do an internet search using the names or exact wording of the email or message to check for any references to a scam – many scams can be identified this way.
- ✓ Look for the secure symbol. Secure websites can be identified by the use of 'https:' rather than 'http:' at the start of the internet address, or a closed padlock or unbroken key icon at the bottom right corner of your browser window. Legitimate websites that ask you to enter confidential information are generally encrypted to protect your details.
- ✓ Never provide your personal, credit card or online account details if you receive a call claiming to be from your bank or any other organisation. Instead, ask for their name and contact number and make an independent check with the organisation in question before calling back.
- ✓ Report the email to your local IT or to the ARMS Executive Office.
- ✓ Check if the senders email address is different to their contact name. For example: Maria Zollo presidentialprivate.emaill@gmail.com
- ✓ Often there are spelling and grammatical errors contained within the email notification.
- ✓ Report as “junk” in outlook to avoid receiving emails from the source in the future.

Australasian Research Management Society



Please be aware that scammers are everywhere, but urge you take necessary precautions to reduce the incidence of being scammed. Please bring this alert to members of your committee, SIG, Networks etc. and be aware of the signs.

The text from this email will also appear in the next edition of our newsletter – Up In ARMS.

Please do not hesitate to contact our office if you have any further questions – arms.adminofficer@flinders.edu.au