

Credit unions say - don't take the Phishing bait!

Have you ever received an email which claims to be from your credit union or other financial institution, claiming that they have had a security breach, a system failure, a website upgrade all requiring you to "verify" your personal details?

Be aware – these emails are scams! Phishing scams - e-mails that try and trick consumers into revealing their banking details - are increasing every day. Thousands are sent each month to Australian consumers. These scams can look impressive: they are professional, can have links to 'real' websites, and may seek clarification of your details because of alleged 'security breaches'. Often, phishing scams will try and install viruses and other tricks to give them access to your private accounts and details.

Slam the spam! Never open an unsolicited e-mail from your financial institution. Use our tips to help fight off phishing fraudsters!

Credit unions will never approach members asking for their private details in an unsolicited e-mail or other message. Phishing scams often have features like:

- Addressed to "*Dear customer*", rather than to you by name
- Written with a sense of urgency, often saying that your account will be closed down unless you respond or that security breaches require you to re-enter PIN details.
- Directing you to click on a link which looks like a link to your financial institution.

Credit Union Top Ten Tips to Fight Phishing

1. **Never open an email if you don't know who it's from.**
2. **Delete unsolicited emails without opening them.**
3. **Never click on a link in an email claiming to be from your credit union.**
4. **Never click on a link to your account or institution – always type in the "url" address yourself to get to your online account access points.**
5. **Turn off your broadband after use. Criminals use open bandwidths to exploit vulnerabilities in programs and to upload key-loggers.**
6. **Keep firewall and security programs on home computers up-to-date.**
7. **Don't use public computers to do online banking.**
8. **If you have used a public computer for online banking, delete the history in the browser immediately and empty the trash can straight away – don't leave your banking details for someone else to find.**
9. **If you're out and need to access your account, call your credit union and ask them to check your balance or transfer money for you.**
10. **If you have any questions (or believe you may have already fallen victim to a phishing scam) contact your credit union for advice.**

Credit unions, through the Credit Union Industry Association, are partnering with the Australasian Consumer Fraud Taskforce in a month-long campaign to raise consumer awareness. For more tips and information, access our online resources at www.cu.net.au.