

## Scam - Fraudulent requests for Quotes

This message is for the attention of existing and potential suppliers to the University of Auckland

We want to alert you to a fraud scam that is targeting existing and potential suppliers of goods to the University of Auckland, as well as other Universities and businesses in New Zealand. Please take the necessary precautions so that you are not a victim of this scam.

While the University of Auckland cannot prevent this fraudulent activity we are supplying the Police with details to investigate the matter as we become aware of specific instances.

The fraud scam involves requests for product quotations and may lead to subsequent purchase orders that purport to originate from the University of Auckland but are in fact fraudulent.

The scam operates in the following way: the supplier will receive an email requesting a quotation for goods. The email address being used for this is "auckandc [at] auckand.co.nz" purporting to originate from the University Purchasing Office. Once the quotation has been provided, a purchase order is emailed to the supplier that bears little resemblance to an authentic University purchase order. The purchase order typically instructs delivery to an address not affiliated with the University. After shipping the item/s, the supplier never receives payment and is unable to retrieve the shipped products.

### Indicators of fraud:

- Incorrect domain name used to send emails and purchase orders. A valid Auckland University email address will always end in ....@auckland.ac.nz. Hovering over the email address may reveal the originator's email address if different from that displayed.
- The delivery address is not a University address. Fraudulent addresses will typically be a domestic residence or a self-storage facility.
- Poorly written email with grammatical errors.
- Use of a false or unknown contact from the University. If requests for quotations or purchase orders are received from a new Auckland University contact that raises your suspicion then please email [stc@auckland.ac.nz](mailto:stc@auckland.ac.nz) to verify the validity of the request. Do not contact the name/number used on the email/purchase order.
- Phone numbers not associated with the University.
- Unusually large quantities are requested.
- Rush to ship priority/overnight

### What to do if you suspect fraudulent activity:

- Email [stc@auckland.ac.nz](mailto:stc@auckland.ac.nz) to verify the validity of the request, (Please ensure you include any emails and documents you have received that relate to the enquiry).
- The Shared Transaction Centre (STC) Office will respond to your email asap to confirm the validity of the request.
- Please do not attempt to call any phone numbers contained within the fraudulent emails that purport to be University of Auckland numbers as they will attract a service charge.

### What the University is doing:

Liaising with affected suppliers that may be subject to this type of fraudulent activity to provide the validity of RFQ request received.

Reporting actual cases identified to the Police.

Requesting that domain names used for fraudulent activity are closed.