chill it
COOL UNDER PRESSURE

SUPPORT DEVELOPMENT CLOUD CONSULTING

July 2017

Protecting your Business | High Alert!

Dear Clients,

We are seeing a lot of fake emails being sent to accounts departments requesting bogus payments. It is relatively easy to piece together staff at a company with profiles and positions on websites and LinkedIn. We are seeing fake emails from people impersonating management, MD's, CEOs, and emailing accounts requesting a quick transfer, typically for an invoice which is attached to that email and looks legitimate.

Chill IT highly advises to *always* confirm unusual transaction requests with a follow up call to Management/Directors to validate such requests.

We are seeing three different types of cases:

Case 1:
A domain is registered that is very similar to your own.
A recent example; a scammer registered a domain with an I instead of an L.
www.allphones.com VS www.alIphones.com
The second domain having a capital "- i -" instead of a lowercase "- l -" and on cursory glance it was not picked up. A fake email was sent from the CEO to accounts requesting a transfer – the accounts department was suspicious and checked with us – we were able to identify it was a fake domain (rather than the real CEO's account being hacked).

Case 2:
People can try and imitate (spoof) your email address.
People can construct and send an email so it looks like it comes from obama@whitehouse.gov.
The more sophisticated systems will check and see if it was sent from an authorised "@whitehouse.gov" server – and if not – will not accept the email.

Case 3:
The scammer can modify the from address, at first it may look authentic - eg John Smith <john.smith@yourcompany.com> - however when you click reply, the recipient address can change to John Smith <john.smith@differentcompany.com> - Be very careful to ensure the reply address is the correct address.

If you have any questions or concerns please call us on 1300 726 679 or email support@chillit.com.au and we will help!