zhero

delivering better IT faster

10 August 2023

URGENT SECURITY WARNING
INCREASE IN FRAUDULENT CYBER ATTACKS

We have noticed a concerning rise in cyber fraud incidents. To safeguard you and your business from falling victim to these malicious attacks, we recommend taking some essential precautions. By implementing these measures, you can bolster your defences and minimise the risk of cyber fraud impacting you or your business.

What to do when you get a call from the bank?
Call them back on a verified number as might be someone pretends to be a from your bank to gain access to your money and personal information. It's not just calls, they also use texts, emails and even instant messaging platforms. Do not allow them to login or install any remote access software on your system either. Always verify and do not share your passwords.
Reminder banks will never:

- Call you about fraud that's happening live
- Change your password to something specific
- Ask you for your MFA code
- To move money out of any other account for safe keeping
- Coordinate live fraud operations with any other bank in real time

My supplier has changed their banking details. What now?
Always call your supplier back on a verified number if you receive a letter or an email asking you to update your records accordingly with the consequence that future payments will be made to their account. We highly recommend that you have two steps checks internally on any payments and bank account details change requests.

How to identify fraudulent requests?

- **Email address anomalies;** email might vary by a single character-changing an "l" to a "i" for example. It might be the same address but end in something other than ".com
- **Fake parties copied into the email;** someone to try to demonstrate authenticity and add authority to their request. Inspect email addresses of copied parties just as carefully as the sender's email.
- **Different tone;** check vocabulary, spelling, grammar, or sentence construction may be red flags. Also check for if they use the correct vernacular.
- **Urgency;** these requests are usually urgent-they need to have their bank account information changed immediately

zhero

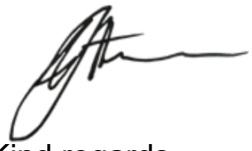
delivering better IT faster

- **Erroneous invoice numbers;** may be from older payments, guessed at from past invoice numbering patterns, or even made up.

In light of the alarming surge in cyber fraud incidents, it is imperative that you remain vigilant and proactive in safeguarding yourselves and your businesses. By heeding the precautions outlined in this notice, you are fortifying your defenses against the malicious onslaught of cyber attacks. Whether it's a call from your bank or a request for supplier bank details change, always exercise caution.

Remember, authentic banks will never ask for sensitive information like passwords, MFA codes, or urge immediate money transfers. Stay alert for indicators of fraudulent requests, such as email address anomalies, suspicious parties copied into emails, unusual tone or urgency, and erroneous invoice numbers.

By adhering to these guidelines, you can effectively stop fraudulent attempts and secure your digital assets.



Kind regards,
Izak Oosthuizen
Founder and MD, Bestselling Author