Spark nz

COVID-19
SCAM FACTSHEET

8 tips to avoid getting scammed during COVID-19

With kiwis using their devices more than ever before and scammers looking for ways to leverage the virus, COVID-19 related scams are starting to pop up.

From emails to cold calls and even text messages, you can help protect yourself from becoming the victim of a scam by following these 8 key tips:

□ **Avoid clicking suspicious links and attachments.**
Don't click on links, download files or open attachments in emails, or links in text messages from sources you don't know or suspicious looking communications from friends who might have been hacked – they may contain malware.

□ **Protect your personal information.**
Be careful where and with whom you share your personal details, including on your social media accounts.

□ **Think critically about any virus-related communications sent to you out of the blue.**
Be wary of emails, texts and cold callers posing as health professionals offering health advice, test results or vaccines, as well as offers for investment opportunities in companies whose products or services will be in high demand due to the virus, and invitations to donate to charities and crowdfunding sites including the fake 'World Health Organisation COVID-19 Response Fund'.

□ **Don't call back numbers you don't recognise.**
Avoid calling back numbers you don't recognise and if you're unsure whether the call is genuine, the best thing to do is hang up.

□ **Make sure your operating system and applications are up to date.**
Turn on 'Auto Updates' on your devices – the latest software updates may contain security updates that will help defend against malware and hacking attempts.

□ **Ensure your anti-virus software is up to date.**
Spark broadband customers can also get 'Spark Security Suite', an anti-virus software for free. Visit https://www.spark.co.nz/help/internet/security/spark-security-suite/ to install.

□ **Choose unique passwords.**
Avoid using the same password for your online banking, email and social media accounts.

□ **Turn on multi-factor authentication where possible.**
Turn on multi-factor authentication for critical accounts including banking, email and social media. You'll often find the option to enable multi-factor or two-factor authentication in the privacy settings of your account.

PLEASE NOTE

You can stay in the know about COVID-19 related scams by regularly checking our scam alerts page at https://www.spark.co.nz/help/scams-safety/current-scams/ and find more advice on how you can avoid getting scammed at https://www.spark.co.nz/help/scams-safety/avoiding-scams/

And always remember, Spark will never contact you out of the blue and request your password, credit card details, access to your personal computer or laptop, nor threaten to disconnect your internet or tell you you've been hacked.