Avoiding Scams

This tutorial is designed to help you spot common tech related scams before they get you into trouble. If you are ever in doubt, ask us for help. Talk is free at Go Tech.

Never Completely Trust Anybody Who Cold Contacts You
If anybody cold contacts you via any means and asks to remotely access your device, ***CEASE COMMUNICATION IMMEDIATELY!*** Have no doubt that you are dealing with a criminal and letting them access your device ***will result in disaster!*** No matter what they say, do not let anyone who cold contacts you remotely access your devices – ***EVER!***

Similarly, never give out any login information, verification codes, or financial information like bank account numbers or credit card details to anybody who cold contacts you – even if it's someone you seemingly know. Their account may be compromised. Legitimate organisations will give you ways of paying them that you can verify are legitimate, such as an email with a link to a domain that you can check with a Google search is theirs.

Learn About Domain Names and Their Importance
Many online scams involve directing victims to fake websites such as the IRD or their bank. This is what is referred to as phishing. Such fake websites are easy to create and can easily fool people. Such sites are usually easily spotted by checking the domain name.

The domain name is the name.ext part at the end of the first part of website address. Here are some examples. I have highlighted the domain name in bold and italic.

- **Inland Revenue Contact Page:** https://www.***ird.govt.nz***/contactus
- **Kiwibank Internet Banking:** https://www.ib.***kiwibank.co.nz***/login
- **My Spark Login:** https://signin.***spark.co.nz***/

Below is an example of a fake Facebook login page.

Figure 1: Facebook Phishing Example. Note the Incorrect Address.

They are trying to make it look legitimate by including www.facebook.com in the domain name but it is in the wrong place. The true domain name is infoknown.com, not

facebook.com. If you follow a link from a message and see a domain name that does not appear to match the real domain, leave immediately.

Another trick scammers deploy is to have the caption of a link have a legitimate domain name in it, but the actual link (which is hidden from your immediate view) will go to a fake domain name. Always check the domain name when you get there. Do not rely on what you can see in the message.

To check where a link is going on a computer, moving your mouse pointer over the link will usually show a pop-up tool tip with the link. On a smartphone or tablet, you can usually check the destination by tapping and holding on the link which should show a popup with the destination.

The only real exception to this is that some businesses and organisations will use external websites for handling their newsletters. There is no need for caution here though because you should know you subscribed to that newsletter and the links will be safe.

Reset or Login Code Fraud

Most websites that have some kind of login give you the ability to reset your forgotten password, or to confirm a login on a new device if you have two-factor authentication on. Scammers have taken to triggering these, contacting would-be victims, and asking for the code under false pretences. Never, ever give this code to anybody under any circumstances – even if it's someone you know. Their account may be compromised.

Voucher Payment Scams

Anybody who claims to be from an official organisation like the IRD who requests payment via some form of voucher is a guaranteed scammer. Cease contact immediately.

Incorrect Domains in Email Addresses

Domain names are also part of an email address. Checking this is useful in spotting a potential scam. For example, an email from Bank of New Zealand would come from something like info@bnz.co.nz, not bnzconz@gmail.com. Unfortunately, due to the number of different email apps and websites, it is impossible for me to give specific instructions. Some apps will show you easily, others you may need to poke around a bit. If you are on a computer, right clicking on the sender's name might give the option to show the email address fully if it is not immediately visible. On mobile apps, tapping and holding on the sender's name while viewing the message may bring up something informative. The sending address can easily be faked however, so the address looking seemingly correct should not be the only thing you use to check for a potential scam. Always check the destination links as described above.

Fake Websites in Search Results

Scammers will often create fake websites and list them on Google, paying for ads to push them up higher in search results by paying for ads. So even here you should always look at the domain name and make sure it makes sense before giving up your financial and personal information or downloading apps.

Language Analysis

Genuine messages from business and organisations, while having the odd error, are usually professionally written and coherent, with consistent font styles and colours. By contrast, scam messages often have quite clear spelling and grammar errors, and may lack their usual colours and fonts. The grammar errors often come about because the original message was written in another language and then translated. If you get a message from a business or organisation you deal with that has a lot of uncharacteristic errors, then it is best ignored and deleted, and not acted upon.

Scams can also come from friends and family whose accounts have been compromised. If you get a message from someone and it doesn't "sound" like them, then ignore or delete the message, and warn them their account may have been compromised.

Exercise Caution with Internet Banner Ads

Banner ads claiming things such like "Your Computer May Be Infected, Click Here!" or "Your Registry May Have Errors!" are scams (Figure 1). Ignore such messages. Do not install the apps. Do not call them if there is a number. Simply close the ad or restart your computer if the ad will not go away. If it keeps coming back no matter what website you are on, take it to your local computer technician for a virus check.

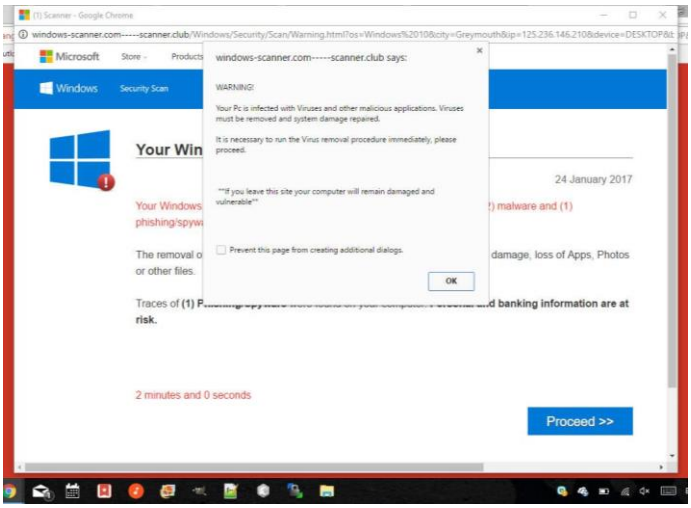

Figure 2: Fake Warning Ad Example

Fake Security Software Renewals

This scam tries to fool people into renewing subscriptions for security software, often software the user may not have. You should be familiar with the name of your security software and its renewal date. If you know you do not have the software mentioned, delete the warning. Even if you do, check the domain name is accurate.

Facebook and Other Social Media Scams

Social media is fertile ground for scammers. Go Tech has a dedicated tutorial for these scams available where you found this one.

Ignore Messages Claiming to Have Evidence of Wrongdoing by You
These are a complete bluff. The evidence they claim to have does not exist, guaranteed. Ignore and delete any of these messages. Do not act upon them.

Exercise Caution with Message Attachments
Attachments to social media messages, texts and emails can harbour malware, notably and most dangerously ransomware that can encrypt your files and demand money for their decryption. So extreme caution is necessary here. If you get an unexpected attachment from a friend or family member, read the message and think about it. Does the message make sense? Does it sound like something they would say? Is the sending address theirs? Then the attachment is probably safe. If the message doesn't read like something they would write, or is non-specific and vague, then it should be viewed with caution. Also be aware of alarmist messages that claim they have found something questionable or strange about you personally. Message them back and ask what it is and why they are sending it.

If it is from a business you know for you sure you do not deal with, delete it immediately and do not open the attachment. Fake messages from courier and freight companies are a common ploy to get people to open dangerous attachments. But such companies always send you information either in the email itself, or in a link to their website. Never in an attachment. If it is a business you do deal with, apply the same language analysis logic from above. Is it professional and sensible, without obvious errors? Is it something you are expecting, such as an invoice? Then it is probably fine. If you are even a little unsure, contact them and ask them what it is. Better safe than sorry.

More About Ransomware
If you are unfortunate enough to be the victim of a ransomware attack, power off your device completely immediately. You do not want a well-intentioned automatic backup system replacing good copies of your files with encrypted ones. Do not pay the ransom. There is absolutely no guarantee you will regain access to your files. It may be a complete bluff and your files might be untouched. Take the device to a professional immediately.

Dropshipping
Dropshipping is not necessarily a scam. This is when someone sets up a website advertising products from other sites such as Amazon with a markup. They then process the order and send it to you. This is arguably no different to what any other retailer does. You could argue that the dropshipper is doing the person selling the product a favour, as getting noticed on large sites such as Amazon and AliExpress can be challenging. Keep it in mind the next time you are browsing more obscure websites looking for something to buy. Look for similar products on AliExpress and Amazon, and you may find you can get it for a better price.

