



65 Mackay Street Greymouth
Phone: 03 768 9937 Mobile: 027 285 1859
Email: joel@gotech.co.nz

Avoiding Scams

Go Tech is here to assist you with all of your computer needs. However, there are some things that might happen to you that will do damage that we cannot undo. Some are relatively harmless, but others can have very serious consequences. Read this tutorial, follow the recommendations, and your chances of being a victim are significantly reduced. You are strongly encouraged to make copies of this tutorial and pass it onto whoever you like, as long as it remains unmodified with the copyright notice and contact details intact.

Poor Password Choice

Not a scam per se but something to be mindful of. When using Internet services that require you to use a username and password (or your email address and password), do not pick an overly simplistic password. It does not happen often but hackers can and do attempt to break into accounts with "brute force" tactics – trying a random series of simplistic passwords. So if your password is just your pets' name, for example, you are making yourself vulnerable. The simple act of adding a couple of numbers on the end of a password (the last two digits of your phone number are a good choice) can be the difference between a weak password and a strong one. A couple of letters relating to the service makes it even more secure while still being easy to remember. You might have a base password of "mypass91", and make your Facebook password "mypassfb91", for example.

Exercise Caution with Internet Banner Ads

No doubt you have seen banner ads claiming things such like "Your Computer May Be Infected, Click Here!" or "Your Registry May Have Errors!". Ignore all of these. They prey on your fears to attempt to get you to download their programs which do fake scans, return a stack of errors that do not exist, then ask you for money to fix them for you. Often these programs are harder to get rid of than the viruses they claim to clean. Even if you do somehow end up with one of these systems on your computer, never give them your credit card details. Instead bring your computer to someone like us so the offending software can be removed.

Hoax Technician Phone Calls

Sometimes you may get people call you and claim there is a problem with your computer. To add weight to their claims, they take you through a series of steps to show you a file or series of files that are in reality completely harmless but they claim are actually dangerous. They then get your credit card details in return for fixing this non-existent problem. No one is going to be able to tell your computer has a problem and will not contact you in this manner. Reporting them to your telecommunications company is useless as they are overseas and usually using Internet phone services to call you, making tracing them all but impossible. Hang up on them immediately. If they continue to call you, I would advise keeping a whistle or some other device capable of making a great deal of unpleasant noise close to the phone. They should realise soon enough that bothering you is a really bad idea.

Attempts to Get Critical Login Details aka "Phishing"

A typical phishing scam is an attempt to trick you into giving up login details to an Internet service, such as your email account or online banking. It usually happens via email but could take the form of a phone call too. The email claims that your account and/or contact details need to be "verified" for some obscure reason, and then they provide you with a link to do just that. Following the link will take you to a website that prompts you for your username and password. Most of the time, it is deliberately made up to look like the website of the service in question (eg: your bank's website), but some scammers are too lazy to do even that. The address of the website may be carefully picked to look official too but in reality is slightly different, eg: kiwi-bank.co.nz instead of kiwibank.co.nz. It is not uncommon to receive such mails from services you have not signed up to. This is because a scammer has gotten your email address somehow and is taking a

"shotgun style" approach to getting their scam to work. If even just a few people on their list of potential victims uses the service, and just one falls for it, then their work will have paid off.

If you enter your login details, you will get some kind of a message claiming the verification has been successful, but in reality what you have done is handed your login details to the scammer who can now use them to break into your account. This can have very serious consequences, especially in the case of online banking.

The only time an Internet service will ask you to verify your account is when you first sign up. It is standard practice to email you a verification link to click so that they know the email address you entered when signing up is valid. If you receive anything else after you have signed up asking for you to verify your account, contact details or anything like that it is almost assuredly a phishing scam. Do **not** under any circumstances do what it says. Delete it. Contact the service and check it's validity if you feel you must but do not act on it straight away without thinking.

Important: when trying to assess whether a message like the one above (or any other suspicious email) is a hoax or not, do not give too much weight to the address the message was supposedly sent from. This is because it means nothing. It can be set to anything and has nothing to do with any authentication process. I could configure an email account on your computer that makes it look like you are the president of the USA. This is actually a big weakness in the security of email, but it is necessary for certain things to work. So if what an email is asking you to do seems suspicious then assume the worst and ask for help before acting.

Email and Social Networking Hoaxes

Many harmless but ultimately pointless and annoying hoaxes are passed around via email or social networking site posts (such as Facebook). Many of these have been doing the rounds for years in one form or another. They are usually warnings about health or computer security issues and viruses. The overwhelming majority of these are complete nonsense or at best, a distorted retelling of the truth. The basic rule is, if there is a statement along the lines of "share this with your friends to warn them!", do the exact opposite. You might think "better safe than sorry" but in reality all you are doing is annoying your friends who know not to believe these kinds of things, cluttering up people's Facebook walls or email inboxes with junk, and giving some idiot a cheap laugh at your expense. If you want to be really sure, do a quick Google search with a snippet of text from the warning and then add hoax, eg: "do not add john smith as a friend on facebook hoax". Almost invariably you will quickly locate a page debunking the message. Google makes it easier than ever to check on facts for just about anything. Thirty seconds of your time will save a lot of embarrassment later when angry friends point out the truth.

Sick Child Hoaxes

While similar to the above, I wanted to give specific mention to this vile practice which has manifested on Facebook in recent years. It involves stealing a picture of a sick child from somewhere, then posting it claiming that Facebook or some other organisation will donate money to the child's care for every like and/or share. The photo is accompanied by little or no supporting information, no link to any kind of official press release, and sometimes not even the child's name. It is all designed to prey on people's empathy and get very bored losers a cheap laugh, or to generate likes for someone's page. No organisation will ever agree to such a ridiculous and callous fundraising scheme for a child. To donate money based purely on likes or shares of a photo would be the very definition of heartless. Searching Google will turn up no information to support that such a fundraising scheme has ever happened.

You might again say "Better safe than sorry, what harm could it do?". The answer to that question is "a lot". These scams have caused a great deal of grief to the parents and loved ones of the children depicted, especially since in some cases the child in question has died. Ask yourself how you would feel if a picture of your child was being used in such a manner. Do not fall for this scam. Instead report the photo to Facebook. You can do this by moving your mouse over the photo, clicking "Options" at the bottom, then "Report / remove tag" and finally the "Spam or scam" option.

Giveaway Scams

This is a type of scam that can occur in both email and social networking, primarily Facebook. If it is an email asking you to forward the message onto friends to win or enter, delete it immediately. Tracking the number of times a given email has been forwarded is completely impossible. On Facebook, the message claims that by sharing or liking a picture, you will win or get the chance to win a certain item. The aim may

be just for a cheap laugh, but it may be designed to harvest your contact details for spamming purposes, get you to do surveys (the scam maker gets paid by the people running the surveys for the people they rope in), or trick you into downloading viruses. In the case of giveaway scams on Facebook pages where you have to like the page to be in to win, the scammer cultivates as many likes as they can with their fake giveaway, then sells it to a spammer. The spammer then completely changes the page and before you know it, you have ads appearing in your Facebook sidebar for no immediately obvious reason.

Matters have been complicated by legitimate businesses adopting similar practices on their Facebook pages for genuine promotions. Telling the difference between legitimate ones and scams is usually quite simple, however. Ask yourself, first of all, does the amount of product being given away make sense? Second, is the giveaway being discussed on the business' real Facebook page or website? In the case of the later, check the address bar of the page discussing the giveaway. If it does not match the business' real website, be very suspicious. Just because it has the company's logo and colours does not make it theirs. Anyone can copy that material and upload it somewhere.

If the answer to either of those questions is no, then do not sign up for the giveaway. All of the hoax giveaways are on random pages not connected with any legitimate business, and are usually for some utterly preposterous amount of product. Examples I have seen over the last year or so include 100s of iPhones, iPads, and Vouchers for well known businesses like Dick Smith and Woolworths with a grand total value of multiple thousands. No well known company needs that level of expensive promotion, and no little known company can afford it. The enormous cost of the items, not to mention the amount of additional money and man hours wasted contacting each winner over Facebook or email, getting their address, packaging up the item, and delivery fees would not even come close to justifying the number of new customers the promotion might gain the business.

An example of a recent real giveaway came from the Music Planet series of music equipment chain stores. It was a single guitar pedal which probably cost them less than \$100 to buy from their supplier. People were requested to like their page and share the photo to be in to win. The additional business gained in return for giving away a single, relatively low cost item and it being hosted on their official Facebook page makes it an ideal example of a real, logical giveaway.

Facebook Apps

Facebook offers an uncountable number of applications you can install on your profile. These apps range from games to silly photo morphing tools. The important thing that you need to realise is that the Application interface is completely open. Anyone can create an app, and Facebook does not check up on them or verify them in any way. This means there are a lot of apps that might look useful or interesting on the surface but do nasty things in the background. As soon as you install the application, it has full access to your profile including any contact information you have posted such as your email address and phone number. A dishonest app developer could do a lot of damage with this information. They can also try to trick you into installing viruses or spyware, or redirect you to malicious websites and survey scams like those described above. They can also post spam to your friend's Facebook walls which might contain anything from advertising to pornographic images. They could sell your email address to spammers, or submit your mobile phone number to an expensive text messaging service where you get charged per text sent.

Only install well known and respected apps such as games like Farmville. Even if a friend has posted about it, it does not mean it is safe to use. If you are unsure, a quick Google search of the name of the application along with the word hoax (eg: my top friends facebook app hoax) can sometimes yield useful information. But the best policy is better safe than sorry. If even slightly in doubt, do not touch it.

There are certain apps you should never install under any circumstances. They either claim to accomplish things that are simply not possible, or are applications unnecessarily.

- Apps that claim to tell you who has been viewing your profile.
- Apps that claim to tell you how many times your profile has been viewed.
- Apps that claim to be able to tell who has deleted you from their friends list.
- Apps that claim to be able to determine who have commented on your Facebook content the most.
- Apps that claim to add a dislike button to compliment the default like button.
- Apps that look like a video at first, but before playing try to get you to install an application. Videos can be played within Facebook without a specific app.

- Applications proclaiming to show something bold and shocking, like “OMG this girl killed herself after her father posted this on her wall!!”
- What I call “Random number generator apps”. They take a basic graphic, generate a random number, and post the result. The precise topic varies, like “How many kids will you have?” or “How many beers can you drink?” but the underlying functionality is the same. There is no skill involved in creating such apps, and no gain from doing so unless someone is trying to get access to the contact information on your profile.

Unknown Facebook Friend Invites

Do not blindly accept every friend invite you get. If you do not know them, send them a message. It may be someone you knew a long time ago and forgot about, or a friend of one of your friends. If they really are some random person, then the invite is definitely best ignored. Remember when you are adding someone, you are giving them access to your life and how to contact you. As with rogue app developers, they could do a lot of damage with that information.

This rule is especially important for parents with young kids who use Facebook to enforce. Predators do use social networking to exploit children. The chances of your child being targeted are low, but it is better to be safe than sorry. Once a young female cousin of mine experienced a rather disturbing but fortunately relatively harmless incident where a random person she allowed on her friends list tagged her in a nude photo of a man, embarrassing her in front of friends and family as we all ended up seeing the picture.

You should use the privacy settings built into Facebook to ensure your own and your children's profiles are locked down as much as possible, so only approved friends see pictures and posts. Currently, these settings are found by going to the menu in the top right corner once you log into Facebook. It is a triangle pointing down. Clicking it reveals a menu. From there select “Privacy Settings”, and make sure the Friends option under “Control Your Default Privacy” is set. You are advised to learn about the other settings available to you in the privacy section so you can set them to your liking.

Duplicate Profiles

Over the last year, another type of scam that has become common is creating duplicate profiles. The person who starts it may be a scammer, or someone who has a problem with the person they are impersonating. They download the victim's photo and then set up a new Facebook profile under their victim's name. They may then add known friends of their victim and start attempting to scam them, or may simply try to ruin the victim's reputation by posting offensive things and sending offensive messages. If you get a friend invite from someone you already had on your list, first check that their other profile is still there. If it is gone, then they are likely simply creating a new profile for some reason. If it is still there, message them and ask them if the second profile was created by them.

Facebook Groups and Pages

On Facebook you can join groups and “like” pages. For example, liking a page about your favourite band will keep you up to date with the latest news about them, and joining a group about photography will let you see posts from other like minded people. Much like adding a friend or installing an app, you are possibly giving access to your information to an unscrupulous person so exercise caution. As with apps, there are certain pages and groups that are almost certainly hoaxes and should never be joined.

- Claims that Facebook is going to charge money for membership. There have been dozens of these, and none of them ever offer evidence for their claims. Facebook makes more than enough money from advertising and is smart enough to know introducing fees would kill their user base and deprive them of advertising revenue.
- If they say you must invite your friends to like the page or join the group before they will show you whatever it is they have to show you. This is almost a sure fire sign someone is trying to “harvest” as many profiles as possible for malicious reasons.

Useful Facebook Groups

If you are on Facebook, joining these two groups will get updates about the latest scams and hoaxes posted directly to your wall.

<https://www.facebook.com/pages/Hoax-Slayer/69502133435>

<https://www.facebook.com/Facecrooks>

Conclusion

This information will help your computer be more of a help than a hindrance. If in doubt, ask for help or search for it on Google. You should also "like" the Go Tech page on Facebook where we post free tips on occasion.

<https://www.facebook.com/gotechwc>