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.

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. Absolutely do not let them on your computer nor give them any financial information no matter which company they claim to be from. 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.

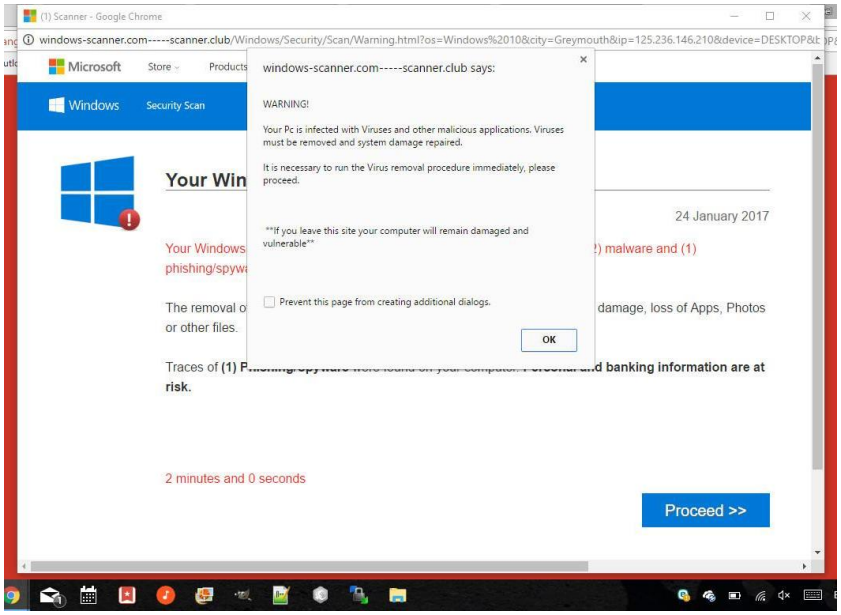

Figure 1: Fake Warning Ad Example

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 claim to be from somewhere like Microsoft or Spark. If you keep them on the line, they will show you something harmless on your computer and claim it is dangerous. It is impossible for someone to diagnose a problem with your computer without first accessing it in person or remotely with your permission. Hang up on them immediately. Do not let them access your computer. Do not give them any financial information under any circumstances. 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 bad idea.

Attempts to Get Critical Login Details aka “Phishing”
Phishing scams usually happen via email but can take the form of a phone call too. The scam claims that your account and/or contact details need to be “verified” for some obscure reason or has some other problem. They provide you with a link so you can log in and solve the issue. 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 such as Facebook or your bank. The address of the website may be carefully picked to look official but is slightly different. There is an example below (Figure 2).

Figure 2: Facebook Phishing Example. Note the Incorrect Address.

65 Mackay Street, Greymouth. Phone: 027 285 1859. Email: joel@gotech.co.nz
Follow Us on Facebook at facebook.com/gotechwc for Free Tips and Tech News

If you enter your login details, you will get a message claiming the verification has been successful, but what you have actually done is hand over 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 its 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. This is a big weakness in the security of email, but it is necessary for certain things to work. If what an email is asking you to do seems suspicious then assume the worst and ask for help before acting.qqqqqqqq

Email and Social Networking Hoaxes
Many harmless but 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 you are doing is annoying your friends, potentially spreading fear needlessly, and cluttering up people's Facebook walls or email inboxes with junk. If you want to be sure, do a quick Google search with as 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 is easier than ever to check on facts for just about anything.

Sick Child Hoaxes
This practice which has manifested on Facebook 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 scheme. Searching Google will turn up no information to support that such a fundraising scheme has ever happened. 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.

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 that 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. 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), or trick you into downloading viruses. Once a page has gained enough likes from a giveaway scam, it is often changed completely and then before you know it, you have ads for questionable things appearing in your Facebook newsfeed 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. First, does the amount of product being given away make sense? Second, is the promotion being discussed on the business' real Facebook page or website? To confirm if a Facebook page is real, check the post history by clicking onto their page and scrolling down. If there are only a few posts, then it is probably a fake. In the case of a website hosted promotion, check the address bar of the page discussing the promotion. 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 these questions is no, do not sign up for the giveaway.

65 Mackay Street, Greymouth. Phone: 027 285 1859. Email: joel@gotech.co.nz
Follow Us on Facebook at facebook.com/gotechwc for Free Tips and Tech News

Facebook Apps
Facebook offers an uncountable number of applications you can install on your profile. These apps range from games to 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 dishonest 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. 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 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 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. 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. You can do this by going to the privacy settings page on your computer or your mobile device’s web browser.

https://www.facebook.com/settings?tab=privacy

65 Mackay Street, Greymouth. Phone: 027 285 1859. Email: joel@gotech.co.nz

Duplicate Profiles
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 target's photo and then set up a new Facebook profile under their target's name. They may then add known friends of their target and start attempting to scam them or may simply try to ruin the target'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. You can protect yourself against being made a target yourself by editing the privacy setting of your friends list to be only you. You can do this by going to the privacy settings page on your computer or your mobile device's web browser.

https://www.facebook.com/settings?tab=privacy

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/Hoax-Slayer-69502133435/
https://www.facebook.com/Facecrooks

65 Mackay Street, Greymouth. Phone: 027 285 1859. Email: joel@gotech.co.nz