Some Scams

John Allen – Feb 2020

Facebook scam case

Question: A member clicked on a link in Facebook that said "Is this you?" claiming she is in a video.

Answer:

- As a general rule, don't click on links in Facebook
- If you are tempted, first check it out, for example do a Google search for:
  facebook scam "is this you"
- If you just clicked on the link, and did not enter your Facebook username/password on the fake page, then you should be OK
- If you made the mistake of entering your Facebook usename/password on the fake login page, you should immediately change your Facebook password before the scammers have a chance to get in. You could also consider setting up Two-factor authentication for Facebook so you won't lose access to your account if you fall for another phishing scam in the future.
  If you also use your Facebook login on any other websites, for example https://www.airbnb.com.au/login , your accounts on those websites can now be accessed by the scammer unless you changed your Facebook password in time. ***It is much safer not to use your Facebook (or Google) accounts to login to other web sites, always use a proper username and password.***
- If the scammers have already taken control of your Facebook account, you will need to go through Facebook's account recovery process to regain access, and warn your friends by email.
- Be on the lookout for unusual activity on the device in case malware was installed

SMS suspected scam

Question: A member received this text message from an unknown mobile number:

"If have you been in, or transited through, mainland China on org………"

The member didn't open it to view the full message as it looked like a scam to get people to phone the number

Answer:

No scams like this found in Google search, could be a new scam or legitimate.

If you are you registered with DFAT's SmartTraveller SMS service? Might be from them.
https://www.smartraveller.gov.au/consular-services/subscribe

Reading the full SMS message is safe but don't respond in any way, and don't click on any phone or web links in the message.

If you keep getting bugged by the same number, block it.

If you are unsure if it is real or not:
1. Search Google for **scam "...some of the text of the message..."** (in quotes) and see if any results. If nothing found it could possibly be legit or it could be a brand new scam. For example *scam centrelink "entitled to more money"*

2. If you think it might be legitimate, and it is from a trusted source, check it out independently by contacting them using their official contact info on their **real** web site, **not** from links in the message.

Have a think about who you have given your phone number to recently - online, on a form, or over the phone.

Have you downloaded any new apps lately and given them access to your personal details? Check out the app reviews to see if there are any concerns about privacy.