

## **The Office of the eSafety Commissioner has recently received several online complaints about compromised Snapchat accounts**

### **THE ISSUE**

Snapchat is an app that allows users to share images and videos ('snaps') with friends. Before a user can access Snapchat, they must first create an account protected with a password. Typically, content shared with friends is 'ephemeral' and is deleted a short time after being viewed.

Recently, Snapchat released a new feature – 'Memories'. With Memories, users can preserve content in a secure archive on their phone. The feature includes a section called "My Eyes Only" – a PIN protected area where explicit snaps can be stored.

The Office has learned that some students have shared their Snapchat account passwords with friends or people they've met online. This has led to unauthorised individuals gaining access to accounts, and intimate or unwanted images or videos being shared, or threatened to be shared.

In some cases, once individuals have accessed an account, they're also requesting to know the user's 'My Eyes Only' PIN. Attempting to solicit information from a person in this way is a form of social engineering.



[Click for our advice](#)

### **WHAT IS SOCIAL ENGINEERING?**

Social engineering is the act of manipulating people into performing actions or divulging confidential information like passwords and PINs. The attacker uses social pressure, deception or threats to influence a person into doing something against their interests. Social engineering is not hacking. Hacking involves the use of computer technologies to gain unauthorised access to systems and networks. Students sometimes use the term 'hacking' when in fact they have shared their password.

### **WHY IS SOCIAL ENGINEERING AN ISSUE?**

Social engineering can be used to steal identities, violate people's privacy and to obtain 'high-value' information, such as intimate images. This type of cyber-threat can be subtle, and may appear as a simple request to help a friend. Spotting social engineering attempts can be challenging.

## **SELF-DEFENCE AGAINST SOCIAL ENGINEERING**

Your child can decrease their chances of social engineering by following these steps:

- **Set strong passwords and PINs** for all devices and accounts – see more information on setting [effective passwords](#)
- Use [two-factor authentication](#) to secure all accounts, including [Snapchat](#)
- **Never give out confidential information (even to friends)** – this includes passwords and PINs
- **Treat unsolicited emails with scepticism**
- **Review account activity regularly** – most social networking sites and apps, including [Snapchat](#), allow users to see where they're logged in and what apps or tools are connected.

## **WHAT TO DO IF YOUR SNAPCHAT ACCOUNT IS COMPROMISED**

If your child's Snapchat account is compromised, and intimate images or videos have been accessed and shared with others, follow these steps:

1. Visit [Snapchat's Safety Centre](#)
2. Click on the "Report a safety concern" button
3. Choose the "Report a safety concern" option
4. Choose the "A Snap or Chat I've received" option

5. Choose the "It contained nudity" option, or another option if more appropriate
6. Click 'Yes' for the question "Still need help?" and fill in the required text boxes – try to provide as much information as possible in the 'What information should we know?' text box. This could include information about the particular way an account was compromised, or the ways in which intimate or embarrassing content has been shared without consent.

## **COMPLAINING TO THE OFFICE OF THE ESAFETY COMMISSIONER**

If Snapchat has not resolved your issue within 48 hours, you may be able to complain to the Office of the eSafety Commissioner.

The eSafety Commissioner will take action against cyberbullying material that is serious. Specifically, the material needs to seriously threaten, intimidate, harass or humiliate a child before we can step in. For information about the eSafety cyberbullying complaints scheme and to lodge a complaint see our [website](#).

We encourage young people experiencing cyberbullying and related issues to contact the Kids Helpline. Their counsellors are available 24 hours a day, 7 days a week, free of charge. Counsellors can also chat online at [Kids Helpline](#).