Crime Prevention Advice

Criminals are targeting Snapchat users, taking over accounts and trying to extort money sometimes threatening to reveal private photos

How the fraud works

The criminals start by contacting you over Snapchat, often from an account that has already been hacked so it can look appear to be someone you know.

The stories that fraudsters tell vary; they may claim to be a friend who is locked out of, or needs help with their account, or that there's been an incident and that they need money to help. They may claim they want to add you to a friends list or "circle" and need your details to add you.

The stories change but the methods used by fraudsters' remain the same; their aim is to trick you in to handing over control of your account and access to your details, contacts & photos.

The intent of the crime varies, some fraudsters use a compromised account to ask for money, (by sending messages to contacts claiming there is an emergency and asking friends to help out. Others want to access the victims private photos and demand money to stop them being published.
The compromised account can then also be used to hack other accounts.

Common Examples

A common fraud is when a friend or mutual friend contacts someone on social media (e.g. snapchat or Instagram) asking for the their email address and phone number so they can add them to their "circles" In some instances this is in order to like or vote for their "make up albums" or promote their business.

The fraudster will then ask for a code that gets sent to the victims' phone which they claim is a unique voting code or allows them to add the victim to their circle. This is a lie. The code is actually an account reset code that allows the fraudster to gain control of the victims account.
These codes are legitimately used, for example if you want to change your phone number or email address for your Snapchat account, Snapchat will send a code to your registered number to confirm that it is you making the request. Instagram & WhatsApp have similar processes in place. Criminals are trying to get around this security process. Never share this code.

It is also common for the victim to be asked to add the criminals email address to their snapchat account under the guise that this allows them access to their "circle." In reality it makes it easier for the fraudster to take over the victims account and makes is harder for the victim to get the account back!

How to protect yourself

- If you receive a suspicious or unexpected message from a friend or “mutual” on social media, contact them via other means to check the message is genuine.
- Always double check friend requests and don’t accept them from people you don’t know.
- Don’t give your login details (email & password) to anyone. Only enter your login details on the official website or app.
- Be extremely weary of sharing your phone number or email address over social media. / Instant messaging.
- Never share any codes or pin numbers.
- Create a strong password. Use three random words which mean something to you but are random to each other - this creates a password that is strong and more memorable. Have a strong and separate password for your email**.**
- Set up 2 factor authentication (2FA) – It’s quick and easy to set up and adds another layer of security to your online accounts. This means that even if a hacker has your email address and password they still can’t get in to your account.
  The website Turnon2fa contains up-to-date instructions on how to set up 2FA across popular online services such as Instagram, Snapchat, Twitter and Facebook.
- Remember, once an image or video is online, it’s potentially there forever.
- Always challenge requests for your information.