PROTECT YOURSELF KNOW THE SCAM

Video conferencing advice

It is more important than ever that we stay connected with family and friends; offering support to one another during these unprecedented times. Technology can play a big part in allowing us to work and socialise from afar, however the use of video communications without certain safeguards can bring risks to your privacy and cyber security. For this reason South Australia Police has developed a guide to video conferencing so that you can continue to stay connected, safely and securely.

What are the risks?

There are a number of risks to consider when participating in a video conference:

- **Some video conferencing software uses weak security measures**, which means it may not be suited for sharing confidential and/or personal information.
- **Video conferencing is susceptible to a term known as 'bombing'**, where uninvited users intrude on video calls, harass users, and share offensive or malicious content.
- **Meetings can be recorded by hosts or participants,** so be mindful about what is said and what content is shared.
- **Participant credentials (email addresses and passwords) may be captured and exploited.** Around half a million logins are being sold on the dark web.

For more information about working from home securely, and current scams affecting South Australians, visit **www.police.sa.gov.au/scams**

SOUTH AUSTRALIA POLICE
KEEPING SA SAFE

Government
of South Australia

PROTECT YOURSELF KNOW THE SCAM

Tips for conducting video conferencing safely

The host

- **Establish meetings securely** with unique meeting IDs and passwords.
- **Limit meetings** to accommodate only essential participants and be aware of unidentified participants.
- **Instruct participants not to forward the conference link or password** to anyone outside the meeting, or share the link via social media.
- **Prevent intruders and 'bombing'** by implementing strict settings such as:
  - ○ Screen Sharing - Host Only.
  - ○ Join before Host - Disabled.
  - ○ Allow Removed Participants to Re-join - Disabled.
  - ○ File Transfers - Disabled.

Participants

- **Use a unique password when setting up an account.** That way, if your credentials are leaked, hackers will not also get access to other accounts you use, such as social media and/or banking.
- **Be mindful of what is shared** – avoid sharing sensitive information, files or password on these apps where possible.
- **Consider using a second device during video conferences**: If you are participating in a conference on your computer, use your phone to check your email.
- **Where possible, do not use social media platforms to sign in** as this dramatically increases the amount of personal data the conferencing software has access to.
- **Keep your video conferencing software updated** so that it has the latest security update.