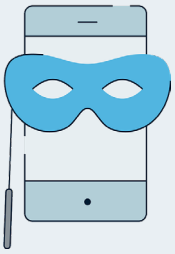
# Deepfake Scams



With the help of AI, scammers can clone the voices of public figures (celebrities, government officials, prominent executives) and try to trick people with fake calls or advertising. The “figure” may try to convince you to make a certain investment or donate to a worthy cause. Because people often trust endorsements from well-known and respected individuals, these deepfakes can be very successful in scamming people out of their money. Read more to learn how to spot red flags, what you need to know, and how to help keep yourself safe.

## Beware of Red Flags

- Inconsistency in the video, look for words and images that seem too perfect.
- Unnatural movements and facial expressions.
- Audio that doesn’t quite match the lips.
- Any message that calls for urgency and secrecy.
- Manager asking for unusual and confidential information.
- The ask is out of the ordinary or the offer is too good to be true.

## What you need to know

- Deepfakes are synthetic media created to be indistinguishable from real people. If you’ve ever used a face-swap app, or watched a video of a celebrity or politician doing something they’ve never done, then you’ve seen a deepfake.
- Deepfake attacks have surged over the past year as AI voice and video clones have fooled people around the globe.
- They can be used to impersonate executives, manipulate audio or video to authorize transactions and trick employees and clients into revealing confidential information.
- Scammers can also use AI to pull information from your online profiles to personalize messages, making them even more convincing.
- Deepfakes can come in a variety of media forms, including image, video and audio.

## Ways to help keep yourself safe

- ☐ To protect yourself, remember to trust your instincts and avoid rushing into any kind of transaction. Taking a step back and assessing any unusual situation can often help avoid becoming a victim of fraud. Even AI-powered fraud.
- ☐ Before making a transaction, sending money or giving up information, be sure to double check the request through another source. Verify the identity of the requester through independent means before responding.
- ☐ Closely examine content for weird distortions like extra fingers or smudged faces. These are telltale clues that the image is fake.
- ☐ Remember to Pause, Reflect and Report to protect yourself and RBC.

**The basic cybersecurity best practice still play a vital role when it comes to minimizing the risk:**

- ☐ Keep up to date on latest’s scams and cybersecurity news by visiting rbc.com/cyber.
- ☐ Use strong passwords.
- ☐ Tighten your social media privacy settings.
- ☐ Limit your online footprint and be cautious about what you share online.

RBC Be Cyber Aware
rbc.com/cyber