Deepfakes: what you need to know

Stay alert. Think before you click or speak.

WHAT IS A DEEPFAKE IN THE CONTEXT OF CYBERCRIME?

A deepfake is a digital forgery created using artificial intelligence that makes someone appear or sound real when they are not. Existing images, videos, or voices are taken as a base, and an algorithm modifies them so the person seems to do or say something different. As a result, the line between what is real and fake becomes increasingly blurred.

HOW ARE DEEPFAKES MISUSED?

Deepfakes are exploited in several ways by cybercriminals. They can be used to make public figures appear to say something damaging, or to impersonate executives within an organization. In fraud cases, they may involve a fabricated voice or video convincing someone to transfer money. They can also be employed to damage reputations or spread misinformation and disinformation.

HOW DO WE PROTECT OURSELVES BETTER AGAINST DEEPFAKES?

Deepfakes are becoming increasingly realistic and harder to distinguish from authentic material.

Because of this, researchers and companies are developing technologies to detect digital forgeries. Large-scale efforts are also exploring ways to guarantee authenticity, such as digital watermarking and verified sources.

Look for:

Weird lip-sync or blinking
Robotic voice or odd pauses
Sudden background noise changes

Think:

Does it feel rushed or pushy?
Is the message out of character?
Coming from an odd number or platform?

What to do:

Double -check with the person another way
Report anything suspicious
Don’t act on pressure alone