## The Growing Threat of Deepfakes: What You Need to Know

Imagine a world where seeing isn't believing—a place where anyone's face and voice can be convincingly manipulated to say or do anything. Welcome to the unsettling realm of *deepfakes.*

These AI-generated videos and audio clips have rapidly evolved from quirky internet novelties to one of today's most alarming digital threats. Originally a source of entertainment, deepfakes are now being weaponised to deceive, defraud, and harm individuals and businesses on a global scale. As this technology becomes more advanced and easier to access, understanding its potential dangers—and how to protect yourself—has never been more critical.

**What Are Deepfakes?**

Deepfakes are created using artificial intelligence and machine learning, allowing computers to alter or replace someone’s likeness or voice convincingly. The result is fake content that looks and sounds real, often making it difficult to detect by the untrained eye or ear. For example, deepfake videos can show someone saying or doing something they never did, while deepfake audio can mimic a person’s voice with near-perfect accuracy.

According to [Deloitte](https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-safeguarding-against-deepfake-technology-noexp.pdf), deepfakes represent a significant threat, especially in the realms of cybersecurity, politics, and personal reputation. The use of AI to fabricate videos and audio can disrupt businesses, manipulate elections, and destroy individual reputations, making it one of the fastest-growing cybersecurity concerns globally.

**The Rise of Deepfakes: Alarming Statistics**

The impact of deepfake technology has been staggering, with statistics showing rapid growth in both its usage and the dangers associated with it. [Eftsure](https://eftsure.com/en-au/statistics/deepfake-statistics/) reports that deepfake attacks increased by 43% in the last year alone, with many being used to scam businesses through fake identity impersonations and financial fraud. These fraudulent activities have cost companies millions of dollars worldwide, and deepfake attacks are projected to rise as the technology becomes more sophisticated.

Even more concerning, deepfake technology is becoming easier to access. What was once the domain of highly skilled developers is now available through user-friendly software that can be used by anyone with minimal technical skills. As a result, experts predict a continued surge in deepfake scams, particularly in financial fraud, blackmail, and misinformation.

**Deepfakes and Misinformation**

Deepfakes pose a serious risk when it comes to misinformation. These fake videos can be used to spread false information or manipulate public opinion, often with devastating effects. A well-crafted deepfake could make it appear that a political figure made an inflammatory statement or a CEO announced false company news, creating chaos and confusion. The ability to generate realistic-looking fake content threatens the integrity of news and social media platforms, where deepfakes can spread rapidly.

In Australia, the government’s eSafety Commissioner has identified deepfakes as a growing challenge in the fight against disinformation. Deepfakes are not only used in political campaigns but have also emerged in criminal contexts, such as extortion and revenge, where manipulated media is used to coerce or harm individuals.

**Practical Tips to Protect Yourself from Deepfakes**

1. **Be Sceptical of What You See Online**
	* Always question videos or audio clips that seem too shocking or out of character. Deepfakes are often designed to trigger strong emotions, so take a moment to investigate before believing or sharing them.
2. **Verify the Source**
	* If you come across questionable content, check whether it’s from a reliable source. If it’s from social media or an unfamiliar website, search for the same content on trusted news sites. Always cross-check critical information.
3. **Look for Inconsistencies**
	* Deepfakes often contain subtle mistakes like unusual facial movements, mismatched lip-syncing, or inconsistencies in lighting and shadows. If something feels “off” in a video, it might be manipulated.
4. **Enable Multi-Factor Authentication (MFA)**
	* Protect your online accounts from being accessed using deepfake-impersonated identities by enabling MFA. This adds an extra layer of security beyond your password.
5. **Monitor Your Online Presence**
	* Regularly search for your name online to ensure no one is using your image or voice without your consent. If you find anything suspicious, report it to the platform immediately.

**Workplace Tips to Combat Deepfakes**

1. **Educate Employees**
	* Provide regular training to employees about the risks of deepfakes, how they can recognise suspicious content, and what actions to take if they encounter it.
2. **Verify Sensitive Communications**
	* For important communications like financial transactions or executive decisions, use voice or video calls to verify authenticity instead of relying on emails or recorded messages.
3. **Encourage Reporting**
	* Ensure your workplace has clear procedures for reporting suspected deepfake incidents. The quicker a potential threat is identified, the faster it can be addressed.