AI identity theft

AI-powered identity fraud is becoming increasingly sophisticated, staying informed and maintaining strong security practices provides effective protection against these evolving threats.

Criminals use AI to create convincing voice and video impersonations of trusted individuals, including family members, authority figures, and executives.

AI enables cybercriminals to rapidly scan social media and public records to build detailed victim profiles, create fake identities using real people's information, and bypass traditional security measures like knowledge-based authentication.

Five key things to take away:

Maintain fundamental security practices

Use password management systems and enable multi-factor authentication

Develop healthy scepticism

Always verify shocking content or urgent calls/emails through alternative channels or reputable sources

Watch out for specific warning signs

Watch out for unsolicited communications that seem out of character, impersonal or demand money

Consider this practical prevention measure

Create secret family passwords for emergency verification

Stay informed

AI is always evolving and tactics are becoming more sophisticated. Stay informed about the AI scam trends