



Phishing Gets Smarter

How AI Is Changing Online Scams

Have you ever received an email that appeared genuine but was actually a scam? That's phishing – a trick cybercriminals use to steal your personal information. Now, with artificial intelligence (AI), these scams are becoming even more convincing. Let's explore how AI is changing the face of phishing and what you can do to protect yourself in this evolving digital landscape.



How AI is making phishing harder to detect

Personalised attacks

AI can analyse your social media and other online information, compiling applicable details to create customised phishing messages. By gathering bits of personal information, AI can craft emails that appear tailored just for you, making these fake messages harder to spot.

Better writing

AI can write emails with fewer mistakes, making malicious messages look more legitimate.

Voice and video tricks

AI can replicate someone's voice or create fake videos that resemble someone you know. For example, you might receive a call from a friend asking for money, but it could actually be an impersonator using AI technology.

More targeted and adaptive attacks

AI doesn't just create convincing phishing messages; it's revolutionising how cybercriminals approach their scams. These AI-powered systems can:

- Analyse phishing results in real time
- Rapidly fine-tune attack strategies
- Create highly personalised messages for specific targets
- Learn and improve from each attempt

This adaptive approach makes AI-driven phishing increasingly difficult for individuals and security systems to detect. As attacks evolve, they become more sophisticated and tailored to exploit specific vulnerabilities. The result? A new era of phishing that's smarter, more responsive and constantly evolving to stay one step ahead of traditional defenses.



How to protect yourself

AI-generated content may have:

- Unusual phrasing or shifts in tone
- Abrupt changes in writing style
- Out-of-place vocabulary
- Inconsistent personal details

Practical steps to enhance your security:

- Enable Multi-Factor Authentication on all accounts
- Use a Password Manager to create and store strong, unique passwords
- Be cautious when clicking links or downloading attachments, even from seemingly familiar sources
- Verify requests for sensitive information through a separate, trusted channel

**Stay safe out there,
and do not let the
phishers catch you!**



By staying alert and following good online safety habits, you can help protect against these tricky scams.

Remember, if something seems too good to be true, it probably is. Trust your instincts and always double-check before sharing any personal information online. Stay safe out there, and do not let the phishers catch you!