**Look Closer: How AI Is Turning Everyday Emails into Phishing Traps**

Imagine receiving an email from your manager, perfectly written in their usual tone, asking for sensitive information. Your manager often asks for information, this email seems to be asking for information that is not a common request. The tone of the email sounds just like them. Do you reply as usual, or do you start to question the request of your manager?

What if the email wasn’t from your manager, but from a cyber criminal using AI to mimic every word? This is the unsettling reality of AI-powered phishing, where the line between real and fake is disappearing fast.

AI has transformed industries—and it’s doing the same for cyber crime. Phishing used to be easy to spot with awkward phrasing and obvious errors. But now, thanks to AI, scammers can create hyper-realistic fake emails, manipulate data, and launch large-scale attacks with terrifying accuracy.

**How AI Powers Convincing Phishing Emails**

Forget bad grammar and strange requests. AI’s natural language abilities allow scammers to generate flawless emails that mirror real conversations. Whether it’s a fake business request or a message from an executive, these AI-crafted emails feel disturbingly real.

AI powered phishing attacks, enable criminals to send out thousands of personalised emails in minutes, pulling data from social media and company sites. Each email feels genuine, making it harder to resist that one malicious link.

**How to Protect Yourself Against AI-Powered Phishing**

With phishing evolving, staying vigilant is key:

* **Be Sceptical:** Even if an email looks legitimate, scrutinise it before clicking any links or downloading attachments. Look for small inconsistencies or unusual requests.
* **Verify Requests:** Always double-check urgent requests for money or information by contacting the person directly.
* **Enable Multi-Factor Authentication (MFA):** MFA adds a vital layer of protection. Even if your password is compromised, MFA makes it harder for hackers to gain access.
* **Update Your Software:** Keep your devices and security tools current to block the latest phishing tricks.
* **Stay Smart on Social Media:** Limit what you share online. Cybercriminals can use personal details from your profiles to target you.

Want to dive deeper into the world of cybercrime? Follow Webb Stirling’s pursuit of The Whisper in our thrilling audio narrative!