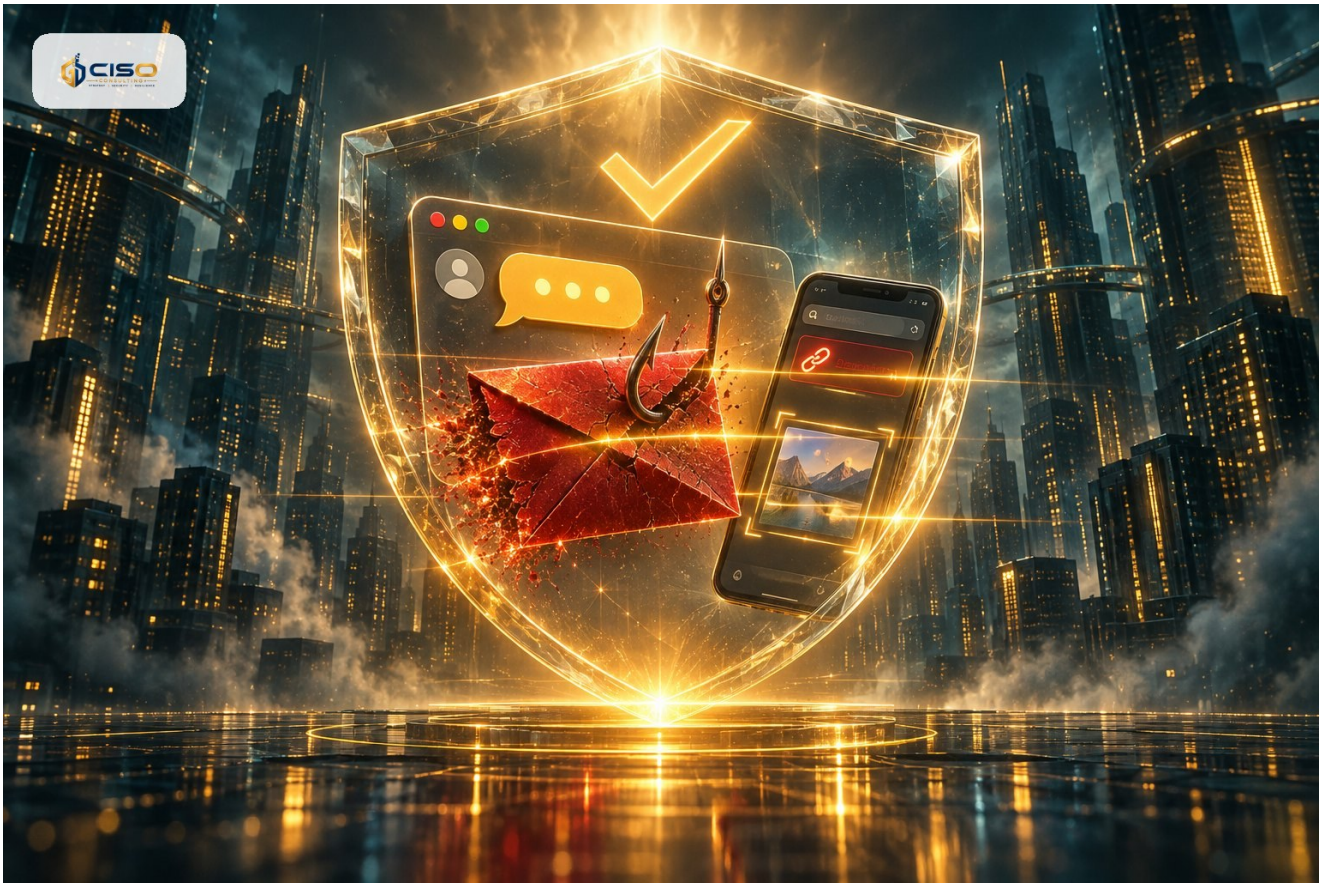
Norton connector brings AI scam checks into Claude chats



Norton's connector for Claude lets users submit suspicious messages, emails, screenshots and links for scam assessment, with explanations and next steps. A Help Net Security test showed clear verdicts on fraud, phishing and a legitimate offer.

- The connector adds Norton's Genie AI scam detection to Claude and needs no Norton account or separate app.
- It offers three tools: scam checking, threat guidance with incident response advice, and Norton product support. Permissions can be set per tool.
- In testing, a fake government fine text was rated an extortion scam with high confidence, and a genuine promotional email was rated safe.
- A cloud storage renewal notice was flagged as phishing, but the tool admitted it could not be

> confirmed as malicious from the available information.
>
> - Advice was consistent: avoid links, and verify through official websites or apps.

Norton has released a connector that brings its Genie AI-powered scam detection into the Claude chatbot. Users can submit suspicious emails, text messages, screenshots and links, and can also ask general questions on cybersecurity, privacy and identity protection. No Norton account or separate application is required.

What the tool does

The connector exposes three tools: one checks links, messages, emails and phone numbers for scams; one gives threat guidance, incident response recommendations and safety education; and one covers Norton product support. Permissions can be managed for each tool individually.

Results appear in a dedicated card showing the classification, confidence level, diagnosis, explanation and recommendations.

What the test showed

A Help Net Security reviewer tested it on an iPhone. A fake text impersonating a government ministry about an unpaid speeding fine was classed as an extortion scam with high confidence, citing impersonation, official-sounding language, legal references and rising urgency. A genuine Black Friday email was rated safe, yet the tool still advised visiting the vendor's site rather than clicking buttons in the email.

A cloud storage renewal notice was classed as phishing because of generic branding, payment pressure and an unverifiable subscription ID. In this case the tool said it could not definitively confirm malicious intent. It advised opening the provider's official app or website, and deleting the message if no matching subscription exists.

Why it matters

For security teams, the value lies in the structured explanations, which can help staff recognise recurring fraud patterns. The review covers a consumer-oriented tool and does not assess enterprise use, data handling or accuracy beyond these examples.

What to do now

1. Remind staff that AI scam checkers are an aid only; suspicious messages should still be reported to the security team.
2. Before allowing any third-party connector to AI assistants, review what data it receives and its permissions, in line with your data-protection and third-party risk policies.
3. Warn staff not to paste customer or confidential data into external AI tools when checking messages.

4. Reinforce the core rule in awareness training: never use links in unexpected payment or fine notices; use official sites or apps.
5. Use these examples (government impersonation, subscription renewal phishing) in phishing simulations.