Vulnerability report replies

Two replies for unsolicited security reports: a polite decline for beg bounty emails, and a professional acknowledgement for a genuine, detailed disclosure.

Copy, adapt and send. Replace anything in [brackets] with your own details.

WHICH REPLY?

- ☐ Beg bounty: asks for payment first, gives no details, findings are generic (missing header, SPF or DMARC, WordPress version).
- ☐ Genuine report: names the URL, plugin and version, steps to reproduce and impact, and does not demand money first.
- ☐ Either way: do not click links or open attachments. Check the claim yourself with your own tools.

REPLY A: POLITE DECLINE (BEG BOUNTY)

Subject: Re: [their subject]

Hello, thank you for getting in touch. We do not run a paid bug bounty program and do not pay for unsolicited reports or scans. If you believe you have found a specific vulnerability, you are welcome to send the full technical details (affected URL, steps to reproduce and impact) to [security contact]. We review every report and fix confirmed issues, but no payment is offered. Regards, [Name], [Business name].

REPLY B: GENUINE DISCLOSURE

Subject: Re: [their subject] (our reference [SEC-number])

Hello [Name], thank you for the detailed report about [issue, for example the outdated plugin on /page/]. We have confirmed it and are working on a fix, which we expect to complete by [date]. We will email you when it is done. Please do not publish details until then, or until [date], whichever comes first. [We do not offer rewards, or: our reward policy is (summary).] With your permission we would like to credit you as [name or handle] on our [security page or changelog]. If you find anything else, please use [security contact]. Thank you again, [Name], [Business name].

AFTER YOU REPLY

- ☐ Log the report: date, sender, claim, what you checked and what you fixed.
- ☐ Fix confirmed issues: update the plugin, add the header, tighten SPF or DMARC.
- ☐ Publish a security.txt file at /.well-known/security.txt with your contact and policy.
- ☐ Never pay before seeing details, and never pay twice for the same finding.