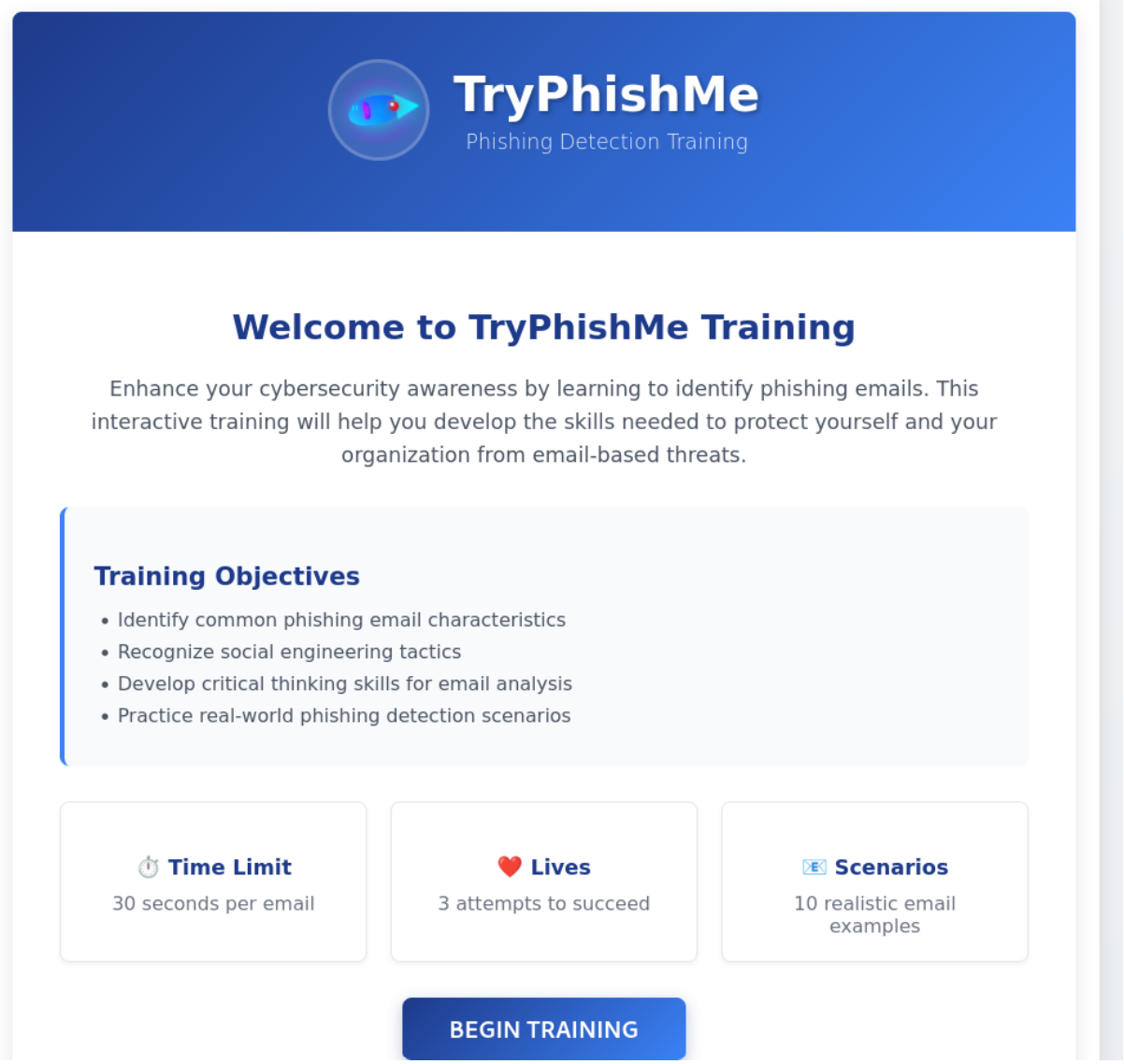
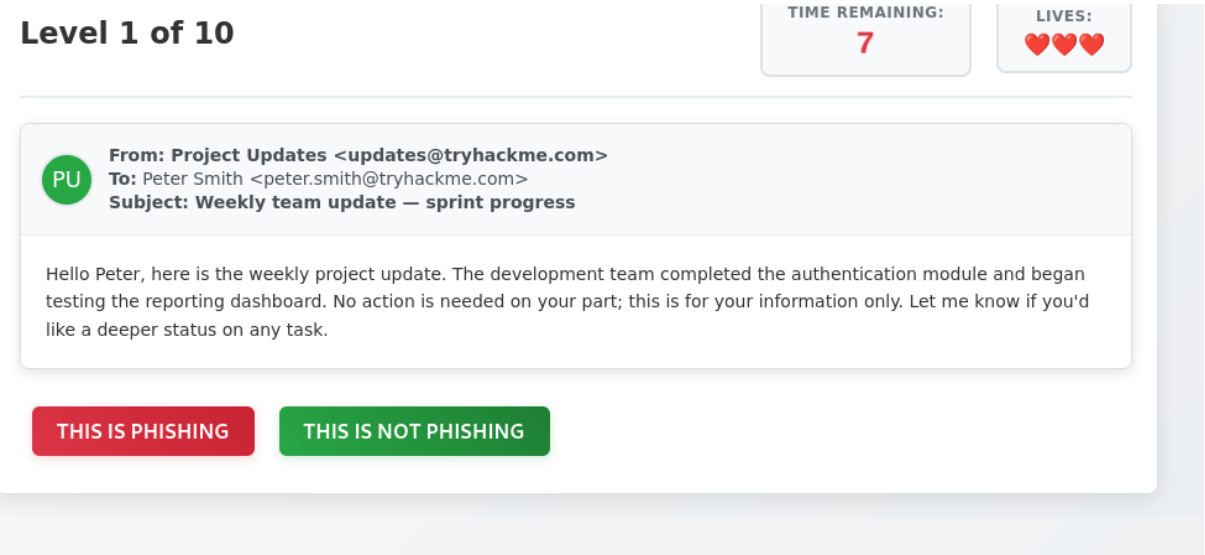
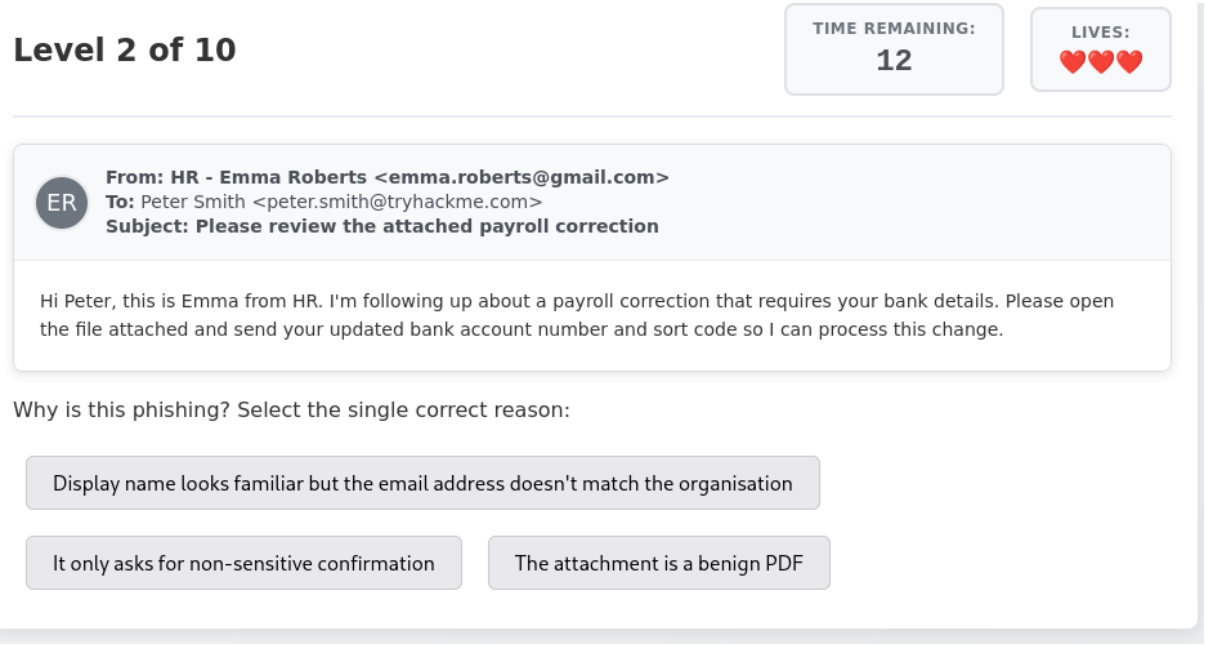
The Phishing Pond -tryhackme

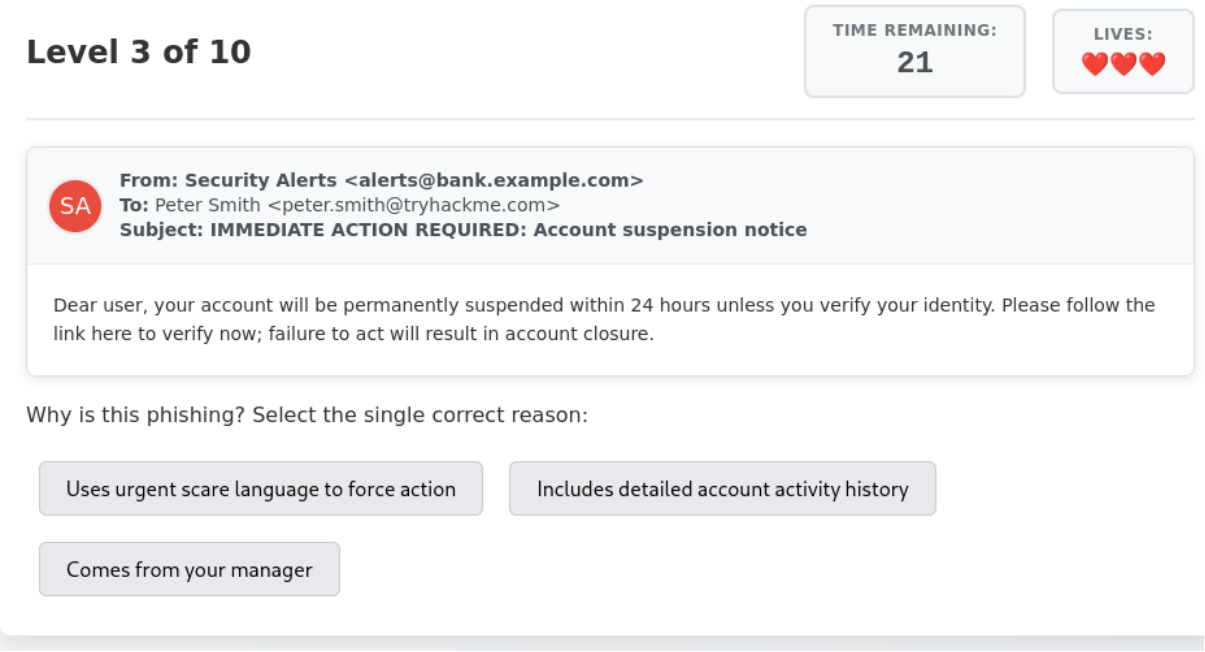




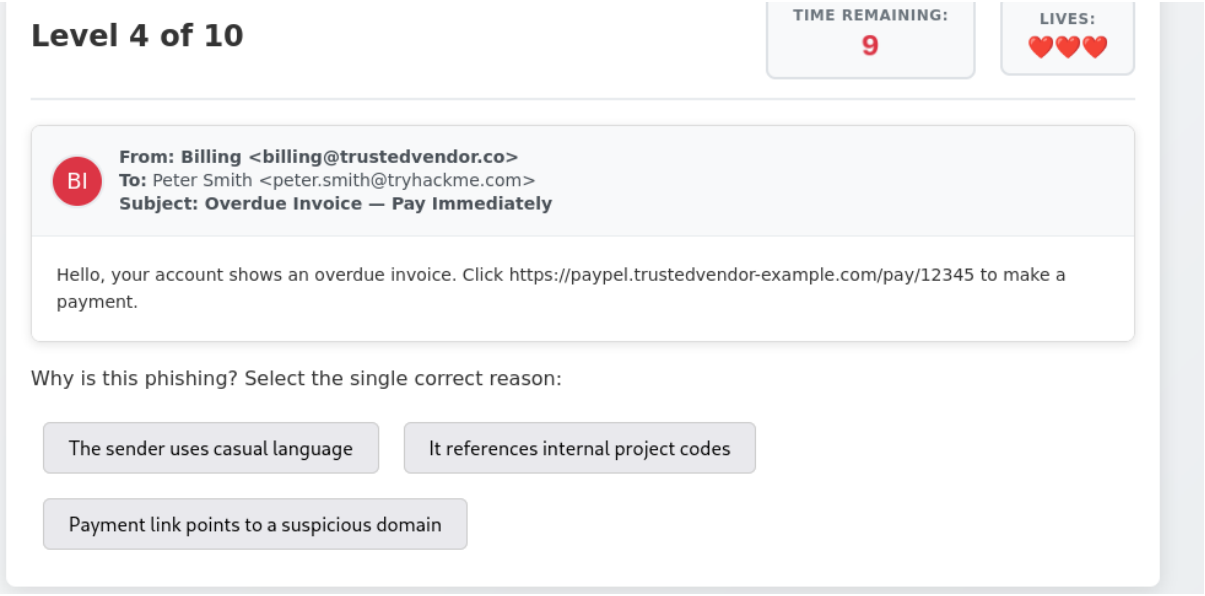
This is not phishing because the email is internal, same company names and contains no urgent requests, asks for no sensitive information, and comes from a legitimate company domain.



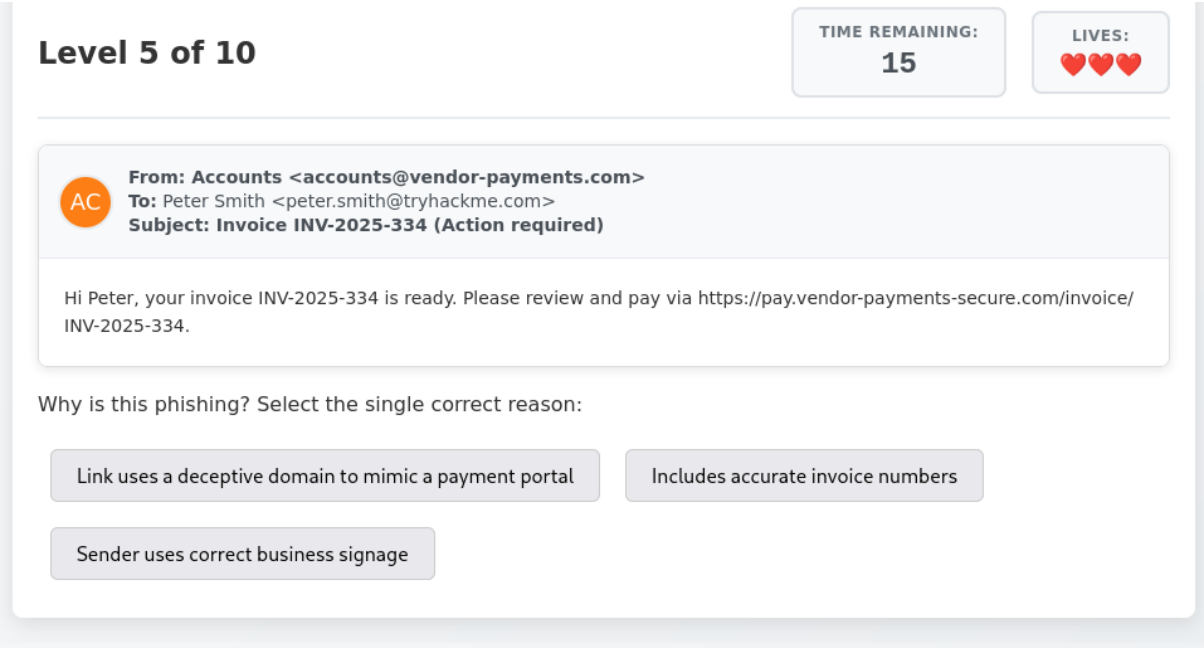
Phishing. The display name looks familiar (“HR - Emma Roberts”), but the email address is a personal Gmail (@gmail.com), not an official company domain. It also asks for sensitive bank details via an attachment.



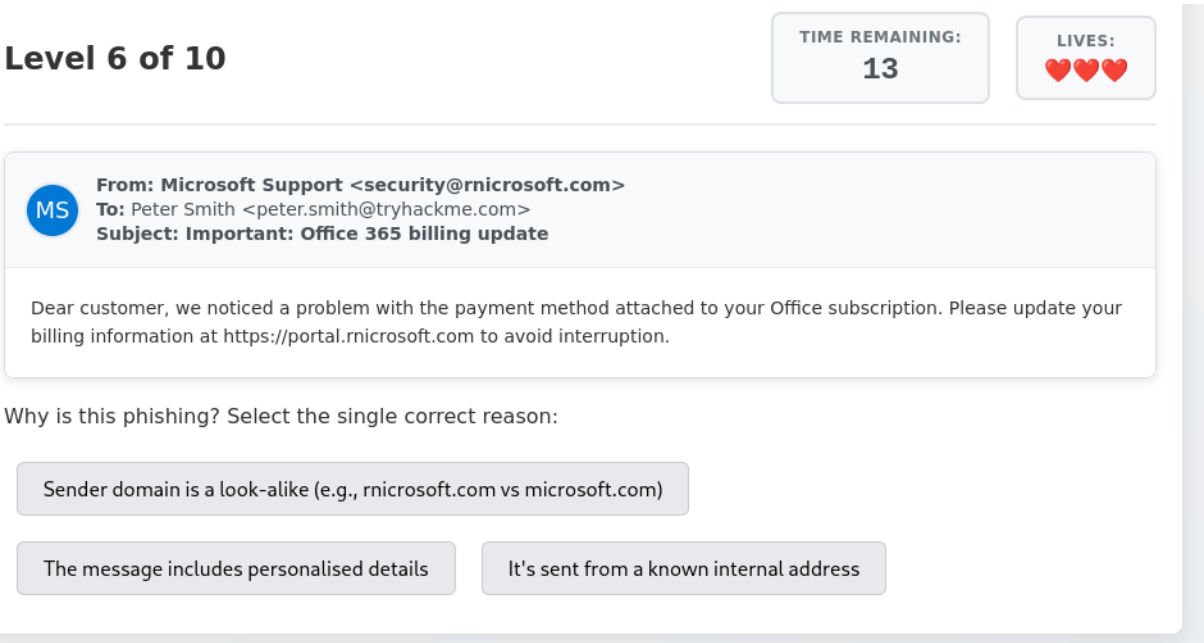
Phishing. Uses urgent scare language (“IMMEDIATE ACTION REQUIRED”) and threatens account suspension to rush the recipient into clicking a link without verification.



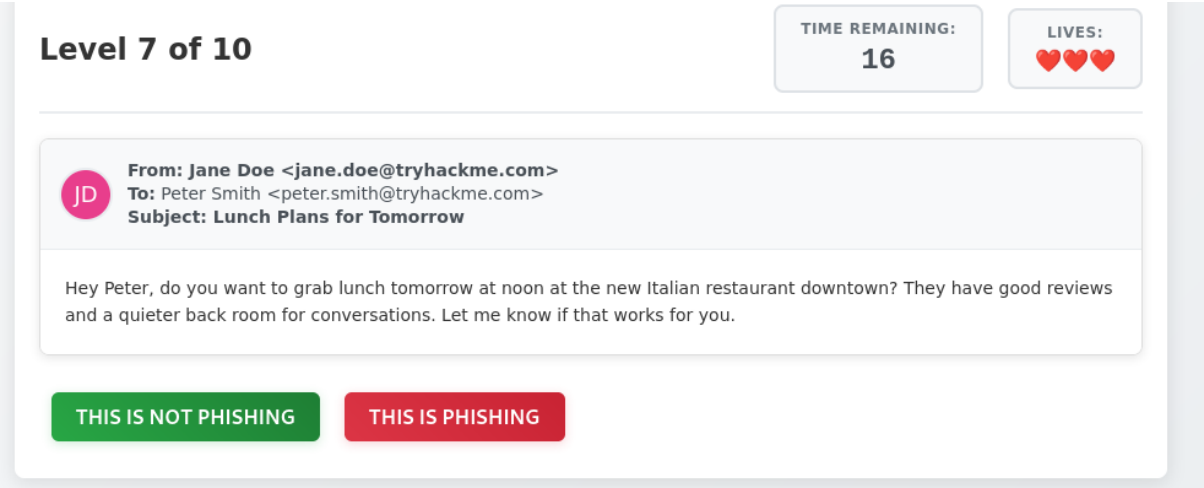
Phishing. The payment link points to a suspicious domain (paypel.trustedvendor-example.com), which is a misspelling of “PayPal” designed to deceive.



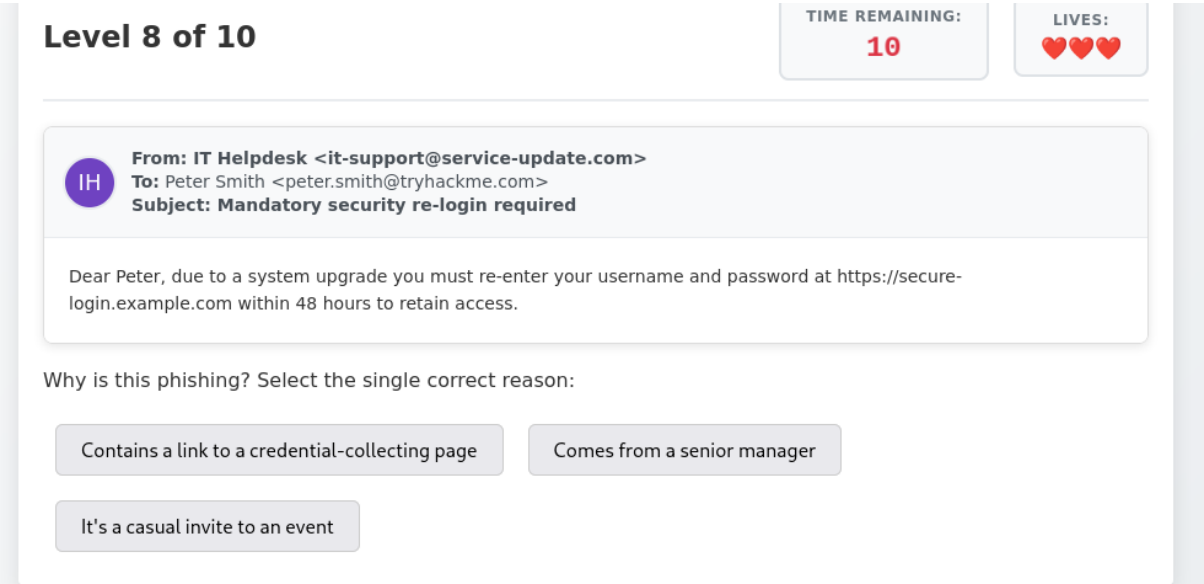
Phishing. The link uses a deceptive domain (vendor-payments-secure.com) that mimics a legitimate payment portal to trick users into entering payment information.



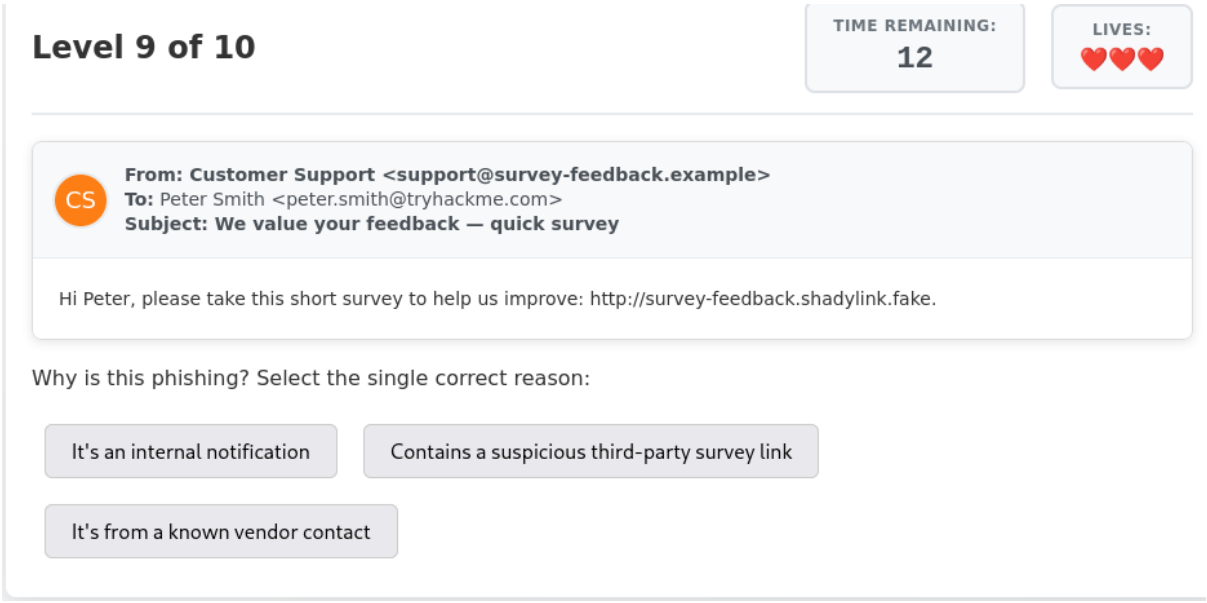
Phishing. The sender domain is a look-alike



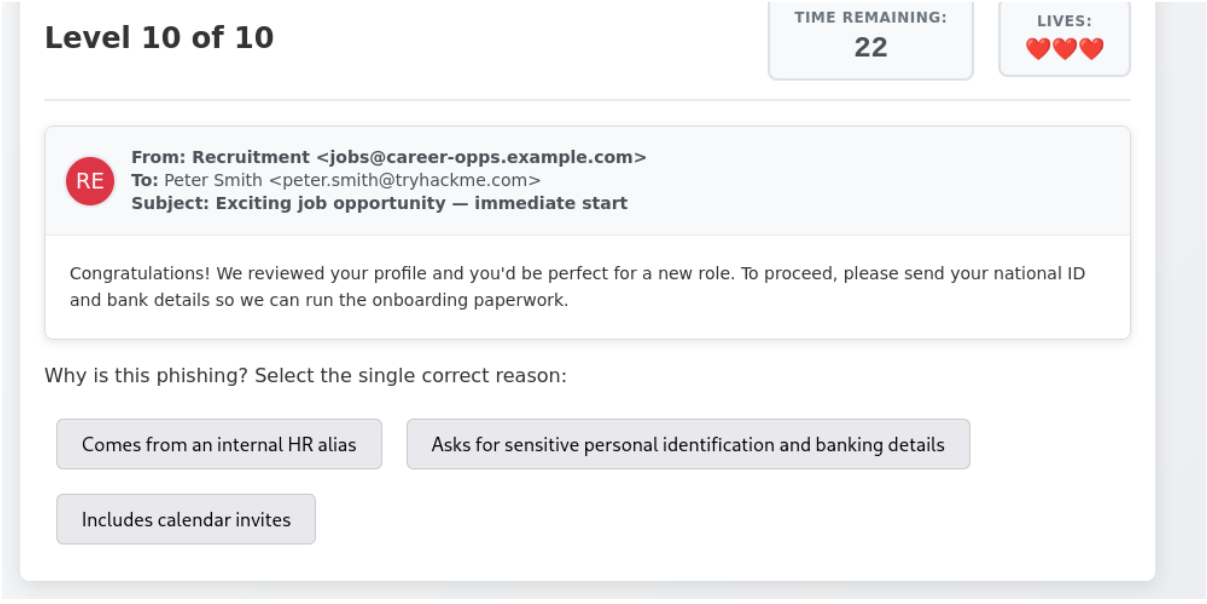
Not Phishing. This is a casual, non-urgent email from a colleague at the same company domain (tryhackme.com), with no request for sensitive data or suspicious links.



Phishing. Contains a link to a credential-collecting page disguised as a legitimate login portal, urging quick action due to a “system upgrade.”



Phishing. Contains a suspicious third-party survey link (shadylink.fake) that could lead to malware or data harvesting.



Legitimately phishing. Asks for highly sensitive personal identification and banking details under the guise of onboarding, which is not standard practice for legitimate job offers.

🎉 Congratulations! 🎉

You completed the game successfully!

Your flag: **THM{i_phish_you_not}**

Lives remaining: 3

Total time: **8m 31s**

🔄 Play Again