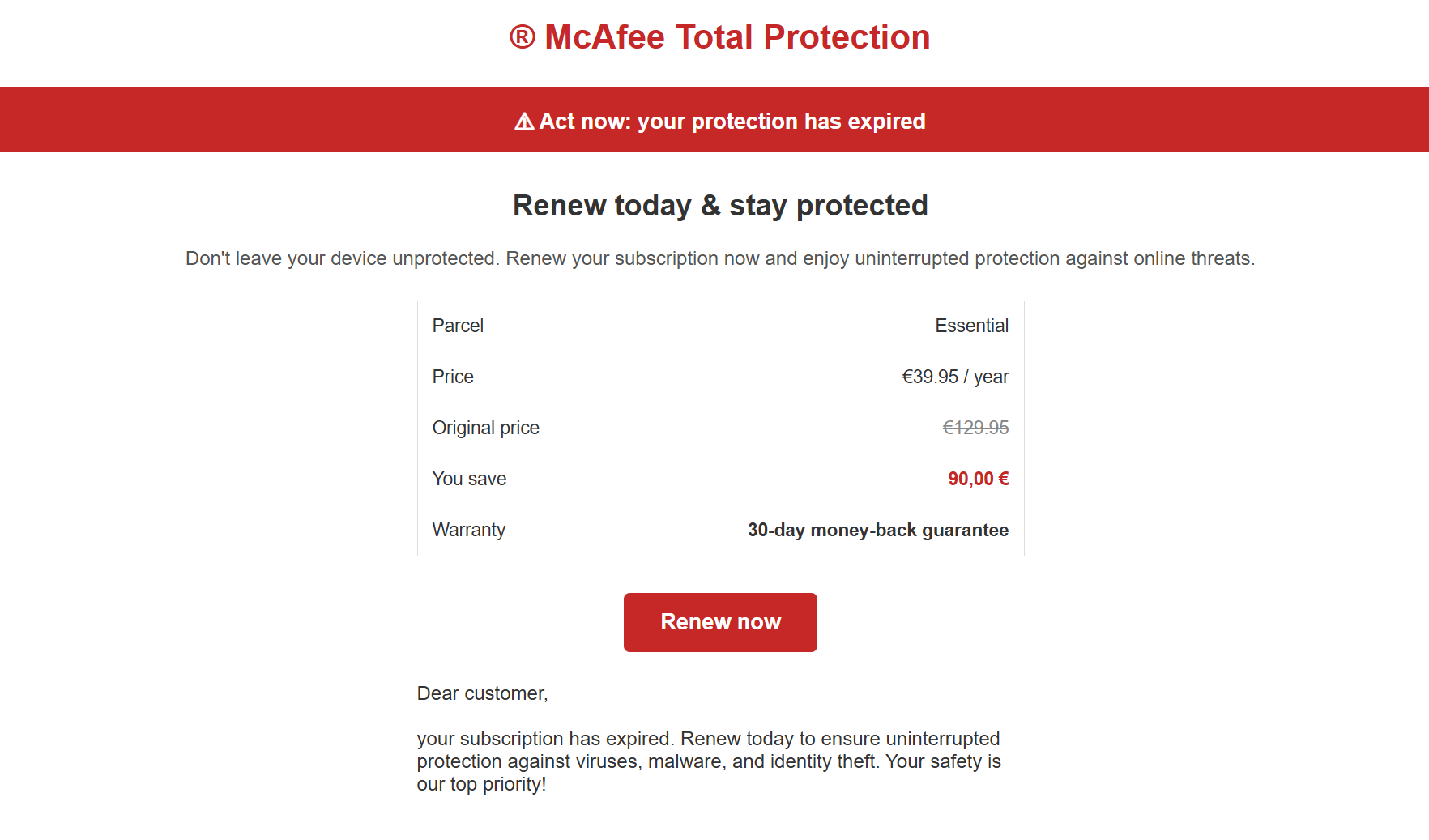
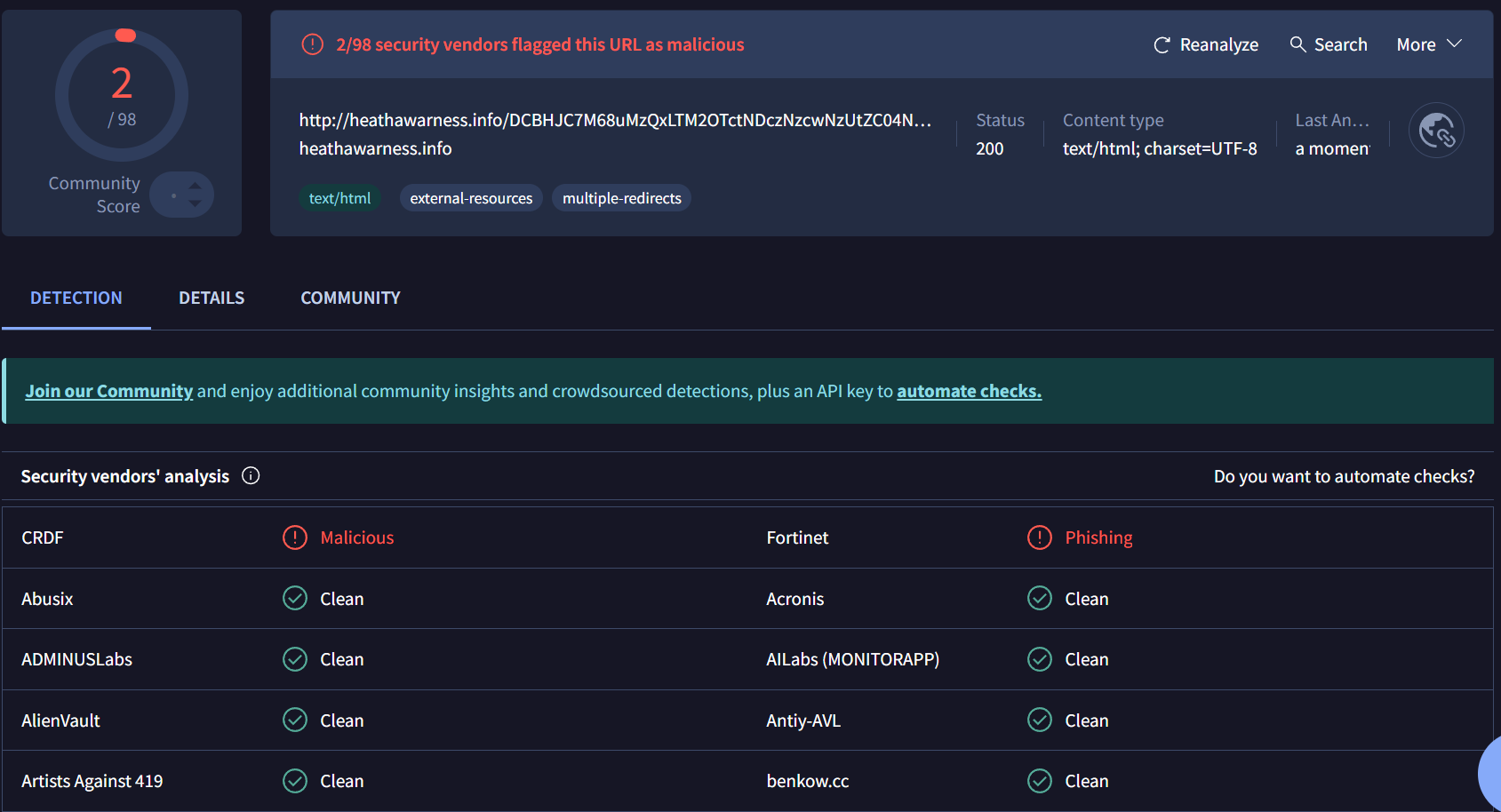
ANALYZE A PHISHING SAMPLE EMAIL

# Brief: The analyzed email has been identified as **malicious**. Header inspection revealed failed SPF and DKIM authentication, a spoofed sender address, and suspicious embedded links directing to an external phishing site. These indicators confirm that the email is fraudulent and potentially harmful.



#Suspicious Trait:

* Spoofed sender address: Mcafee™ [newsletter@khmlouszddic.com](mailto:newsletter@khmlouszddic.com)
* **Failed authentication:** SPF, DKIM, or DMARC checks failed in the email header.
* Suspicious links or attachments: <http://heathawarness.info/DCBHJC7M68uMzQxLTM2OTctNDczNzcwNzUtZC04NS00LTUwOC0yNzUzNS0yNzIxLTAtMC0wLXpZZEtLVHJsVS0yMzQ5MDNkOA>
* 
* **Generic greetings:** Uses “Dear Customer” instead of a real name.
* **Urgent or threatening language:** Messages create panic (“your subscription has expired”).
* **Requests for sensitive information:** Asks for passwords, banking info, or verification details.
* **Technical Evidence:** spf=pass (sender IP is 20.243.186.48) smtp.mailfrom=khmlouszddic.com; dkim=none (message not signed) header.d=none;dmarc=bestguesspass action=none header.from=khmlouszddic.com;compauth=pass reason=109

#Conclusion: The email displays phishing traits such as a spoofed sender domain, failed SPF/DKIM checks, urgent language urging credential submission, and a suspicious link redirecting to a fake login page. These indicators confirm the message is fraudulent.