

## Amazon Email Phishing Scam

We all have been advised never to open an email from anyone we don't know. How about taking a survey regarding Amazon AND getting a \$50 gift card?

An email arrives with something like this in the body of the email:



The message goes on to thank you for your recent order on Amazon.com and offers a \$50 gift card for taking the time to review the purchased product. Seems too good to be true. AND IT IS!

“Warning! If you click on the links within the message, your credentials could be stolen and you could become a victim of identity theft.”

“People are receiving fraudulent emails that contain malicious links. The emails look very official, like they really came from Amazon. But beware, they are actually from cybercriminals looking to rip you off.”

The article from the link below contains suggestions from Amazon on how to recognize fraudulent emails:

**“Fake orders**

If you receive an email claiming to be from Amazon confirming an order that you did not place, it's a scam. Instead of clicking links within the email, type Amazon.com into your browser, sign in and go to Your Orders page to verify your purchases. If you didn't buy the item from the email, it's a phishing scam.

**Credential request**

Amazon does not send emails requesting your username and/or password. If you receive an email like this, it's a scam. Handing over your credentials to cybercriminals could lead to fraudulent charges on your account and identity theft. Bad idea.

your credentials to cybercriminals could lead to fraudulent charges on your account and identity theft. Bad idea.

### Update payment information

You should never click a link within an email asking you to update your payment information. Instead, go to your Amazon account and click **Manage Payment Options** in the **Payment** section. If you are not prompted to update your payment method on that screen, the email is not from Amazon.

### Fraudulent links

If you receive an email with a link that supposedly goes to Amazon, hover over the link with your cursor. If it does not say that it's going to direct you to Amazon, it's a phishing scam. It's always better to type a website's address directly into a browser than clicking on a link.

### Attachments

Emails purportedly from Amazon that contain attachments or prompts to install software on your computer are scams. You should never download PDF, Word or Excel files attached to unsolicited emails to begin with. If you do open one of these documents and it says that you need to turn on macros, close the file and delete it immediately.”

[https://www.komando.com/happening-now/417881/look-out-amazon-gift-card-phishing-scam-spreading?utm\\_medium=nl&utm\\_source=notd&utm\\_content=2017-09-06-article-title](https://www.komando.com/happening-now/417881/look-out-amazon-gift-card-phishing-scam-spreading?utm_medium=nl&utm_source=notd&utm_content=2017-09-06-article-title)