

DTS phishing campaign December 2022

A free Amazon gift card? How generous! The email that arrived in your inbox looked genuine, but take a closer look:


Always check the "From" address; this is neither Amazon nor the University of Reading.

Email urges you to do something quickly before the offer runs out.

Staff Gift Card: Get yours now!

Amazon <noreply@uor-amaz.info>
To Judith Macfadyen

If there are problems with how this message is displayed, click here to view it in a web browser.



Dear Staff,

As a promotion in partnership with your organisation, we have great news!

According to this agreement, Amazon is pleased to present a £10 gift balance for up to 1000 employees. In order to receive this balance, you need to login and complete a survey. Please start the process [here](#).

Terms of Use:

- Each gift card is allocated for one employee only
- The balance is only available for one-time shopping
- The balance must be used within 1 month after activation
- The balance can only be redeemed on an order worth £10 or more

Thank you
Amazon

Please note that the third-party logos and trademarks used in this email or landing page are used for illustrative or instructional purposes only and there is no connection or relationship between the trademark owner and KHIPU Networks.

Generic greeting, no mention of University of Reading

A handy link to login should always be treated with caution.

This email contains several red flags 🚩. Together there was enough questions which should make you stop and consider whether clicking the link and signing in is a good idea.

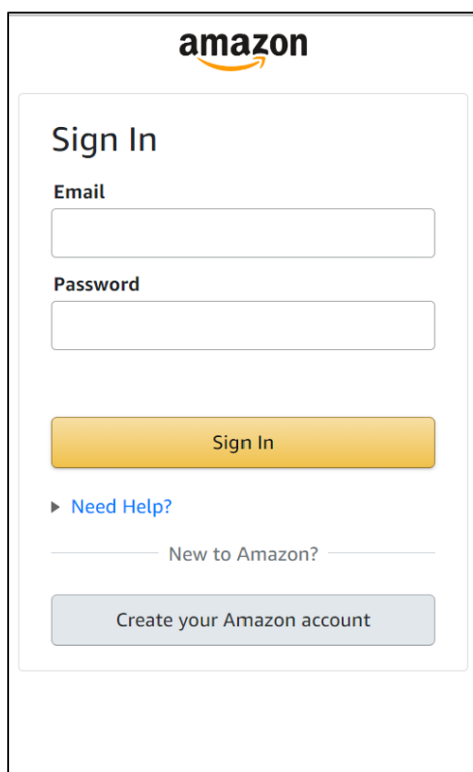
- ✓ Check the email address comes from the company it says it does
- ✓ Check the message makes sense and check spelling
- ✓ Check any weblinks match the company name
- ✓ Check logos and fonts used are the company style
- ✓ Check company addresses are correct
- ✓ Check the small print for clues it may have come from someone else

OK, you clicked the link. What now?

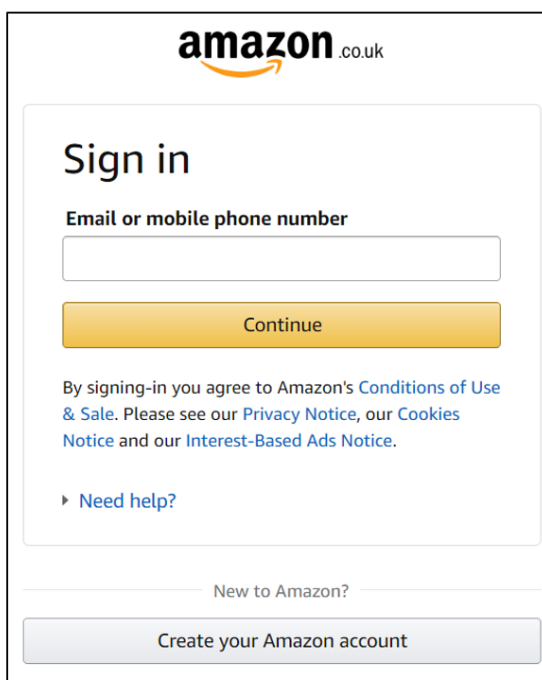
In this awareness campaign, there was another opportunity to reconsider before you give your user name and password to would be attackers. The usual purpose of a phishing scam is to get you to enter your user name, password and any other personal information which the phishers can use.

Next time you log in to any account, make a point of remembering what the login page looks like. Here is a comparison of the login pages for Amazon:

Fake login page – single page for email and password



Correct login page – enter username/email address first



As this is a fake, entering your user name and password safely takes you to further information. If it was a real phishing scam, your username and password would now be compromised.



Please, if you clicked the link & entered your details, do the training offered.
It can stop you becoming the next victim of an email scam.

Your username and password are safe and do not need to be reset.