Transacting

Phishing Emails.

Even reputable companies and organisations can sometimes find themselves in trouble over phishing emails and scams. Their branding can be replicated and people might assume that an email received is genuine, even if it is not. But, there are things to look out for to help you avoid being caught out by **phishing emails**.

GO HIGHER
West Yorkshire

How to complete this activity:

- Read the tips carefully (how to spot a phishing email).
- Carefully review each example email and identify the phishing emails.

How to spot a phishing email:

- Emails demanding 'urgent action' or a lost opportunity if you don't respond – 'don't miss out!'.
- Bad grammar and spelling mistakes.
- Unfamiliar greetings.
- Strange email addresses.
- Poor quality logos.
- Suspicious attachments.
- Emails requesting payments or personal information.
- Too good to be true emails – prizes etc.

Using the above, let's see if you can spot which of the following emails are actually phishing emails!

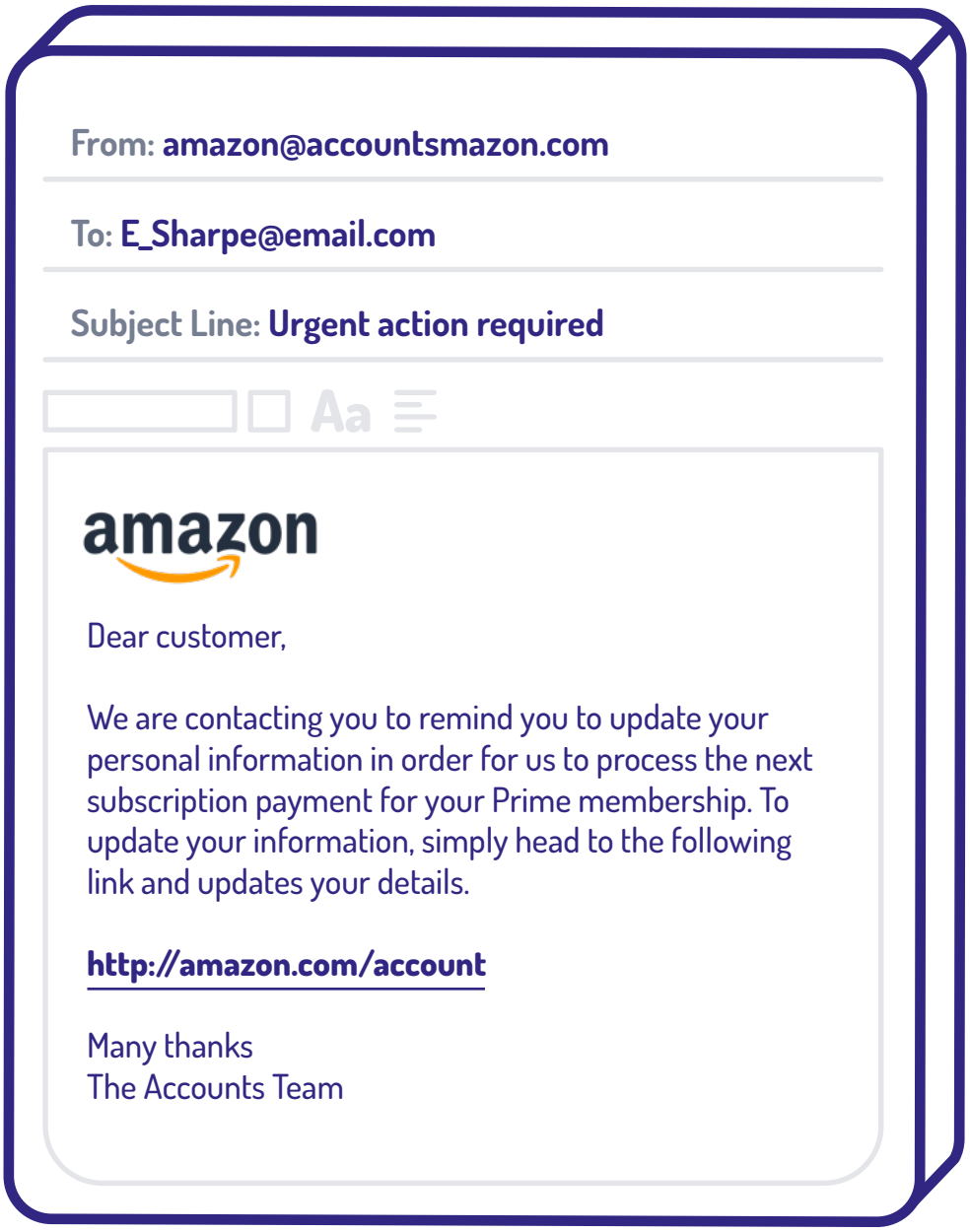
You might want to label the elements of each email that make it a phishing email!

Transacting Activity

Phishing Emails.

GO HIGHER West Yorkshire

Label the elements of each email that make it a phishing email. See if you can spot the genuine email.



From: amazon@accountsmazon.com

To: E_Sharpe@email.com

Subject Line: Urgent action required

amazon

Dear customer,

We are contacting you to remind you to update your personal information in order for us to process the next subscription payment for your Prime membership. To update your information, simply head to the following link and updates your details.

http://amazon.com/account

Many thanks
The Accounts Team

Transacting Activity

Phishing Emails.

GO HIGHER West Yorkshire

Label the elements of each email that make it a phishing email.
See if you can spot the genuine email.

From: **accountsteam@paypal.co.uk**

To: **E_Sharpe@email.com**

Subject Line: **Account status update – Response Required**

PayPal

Dear Costumers,

Recently there has been activity in your Paypal account that seems unusual. To help protect your account we have temporarily frozen all monies going in and out. Therefore, until you have clarified the recent activity on your account, no withdrawals can take place.

To unfreeze your account, simply click here to **Log in**. Then, update your account details and review your account activity.

Thank you for your time.
The PayPal accounts team.

Transacting Activity

Phishing Emails.

GO HIGHER West Yorkshire

Label the elements of each email that make it a phishing email.
See if you can spot the genuine email.

From: accountsteam@linkedin.co.uk

To: E_Sharpe@email.com

Subject Line: Your action is required

Aa

LinkedIn

Dear,

We think that someone else might have accessed your LinkedIn account or you signed in from another computer or devise.

When this happens we require you verify your identity with a security challenge.

Verify your LinkedIn Account Now

Please note this is nothing to get alarmed About, this is just a precautionary measure.

Thank you

Transacting Activity

Phishing Emails.

GO HIGHER West Yorkshire

Label the elements of each email that make it a phishing email.
See if you can spot the genuine email.

From: **hsbcuk@mail.co.uk**

To: **E_Sharpe@email.com**

Subject Line: **New Document**

HSBC UK

Dear Miss Sharpe,

We have sent a document relating to account ending 4563 for you to view in My Documents through digital banking. This is an important document that we need to ensure you have seen as you may need to take action on it.

How to access 'My Documents'

Via Mobile Banking
Log on to The HSBC Mobile Banking app
2. Select 'More' then 'My Documents'
3. Click on the unopened document

Thanks for banking with HSBC UK.

Remember – stop and think before you click on links in emails you are unsure about. Try speaking to the company directly to clarify whether or not the communication is genuine.