Phishing questionnaire

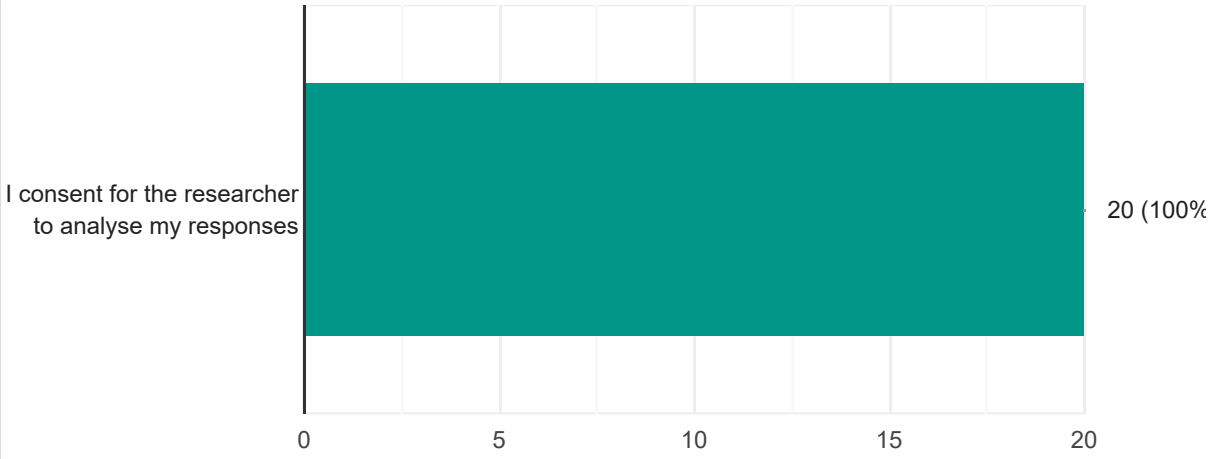
20 responses

Publish analytics

Do you consent to me analyzing the questionnaire responses?

Copy

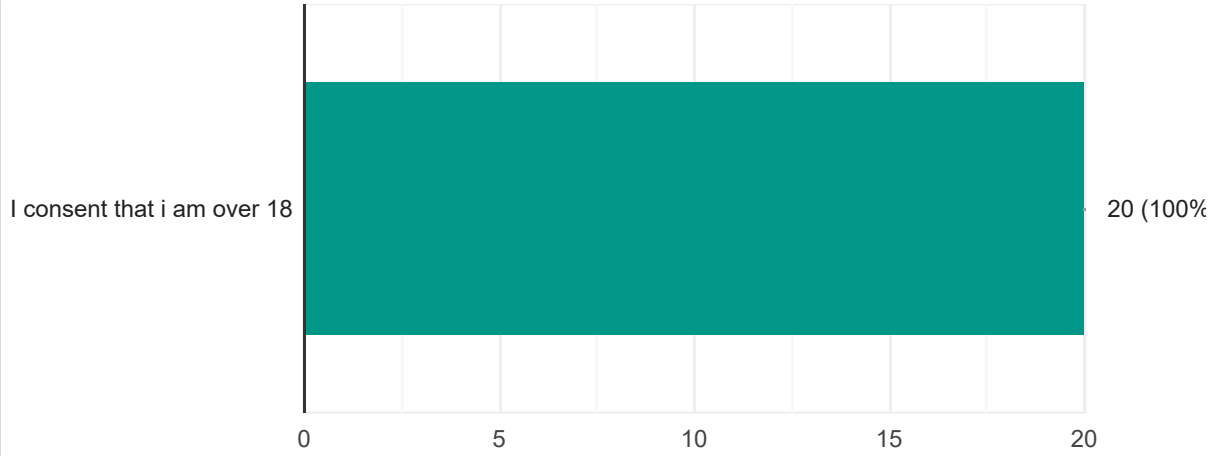
20 responses



Are you over 18?

Copy

20 responses

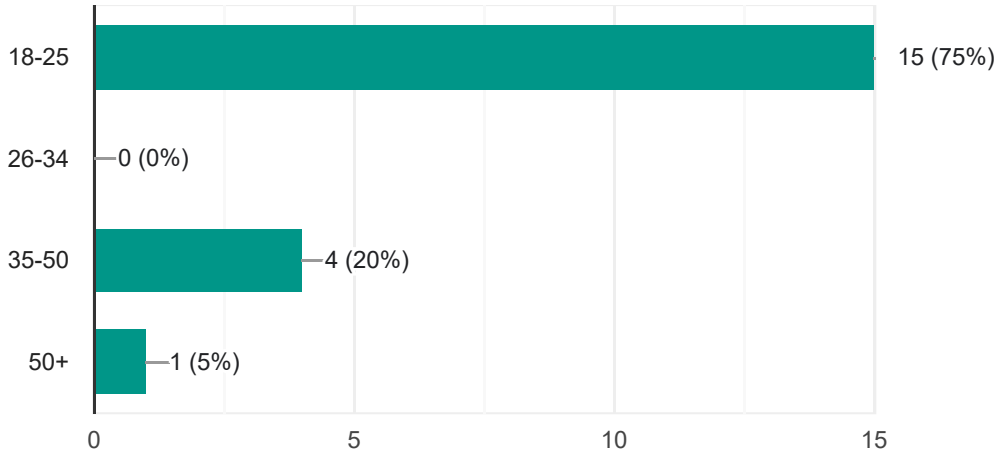


Demographic questions

What is your Age?

Copy

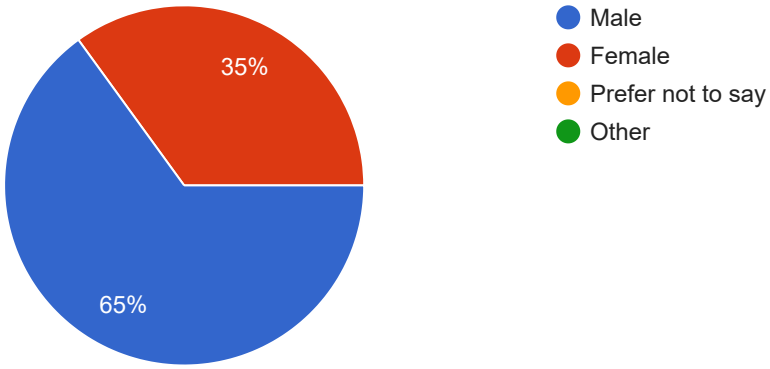
20 responses



What is your Gender?

Copy

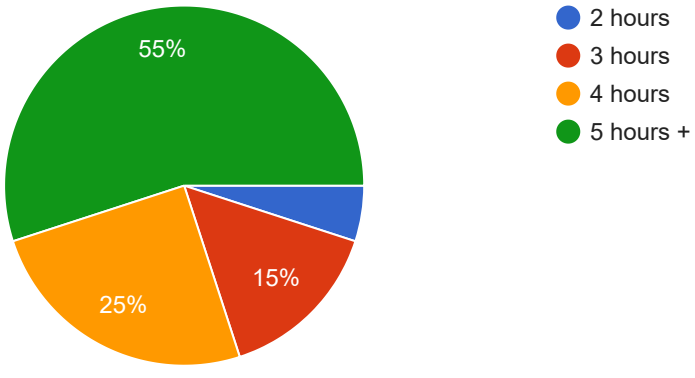
20 responses



Daily how much do you use the internet?

Copy

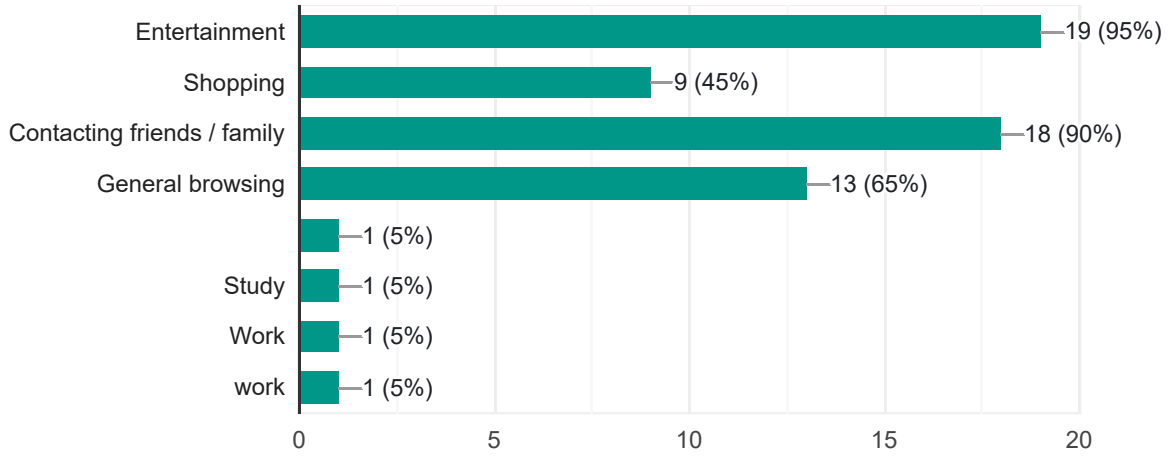
20 responses



What are the main reasons for using the internet?

Copy

20 responses



Email familiarity question

Are you familiar with cc?

20 responses

Yes

yes

Roughly

Yes Carbon Copy

No

No

Carbon copy

Forwards email to specified recipients

yes carbon copy

I think so

Are you familiar with Bcc?

20 responses

Yes

No

Yes

yes

no

No idea

Blind carbon copy i think this one is being able to email people without others knowing? But i could be wrong

Similar to cc

unsure

yes blind carbon copy

Are you familiar with subject in an email?

20 responses

Yes

yes

Yeah

Yes

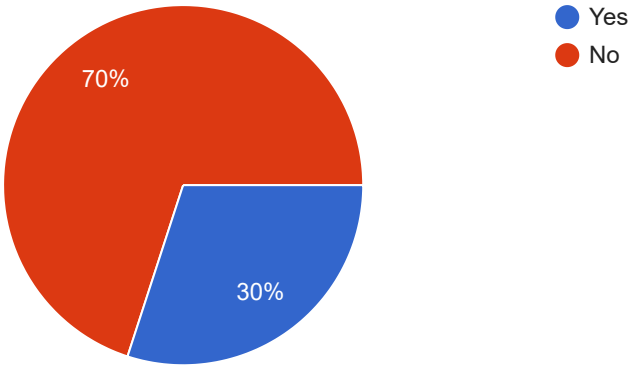
yes

SMS

Do you think the above Message is genuine?

Copy

20 responses

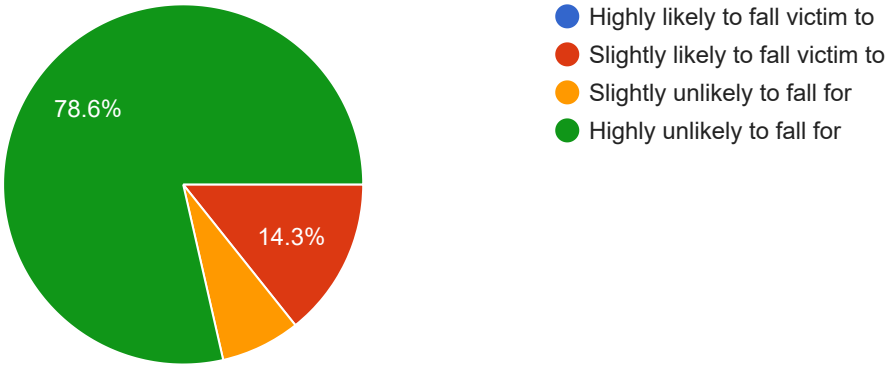


Follow up 1

How likely are you to fall for this?

Copy

14 responses



Also why did you say it's not genuine?

14 responses

Usually companies have a business card attached to the bottom of the email as well as an order number

The url looks extremely sus 🤔

You don’t reply to links

Looks fishy

Bad casing, bad grammar, bad formatting, etc

Incorrect grammar, no logos

I do not own an iphone and would know if I bought one.

Lack of capitalization on the first letter, normally these types of bulk emails are checked.

It looks like a normal typed email, it looks personalised, gives a time frame for delivery

The format of the email was nothing like a legitimate order confirmation email

It has a lack of propper punctuation such as capital letters etc.

Incorrect punctuation

it is common for phones to be used in phishing

I would know if I purchased it or not

Follow up yes

Briefly, what made you think it was a legitimate message?

6 responses

It contained specifics about what the person ordered as well as a tracking link once the order is dispatched.

They regarded Jone by name, they provided specific information regarding his purchase and they did provide information such as an email

I'm a bit on the fence, in a real scenario if I genuinely did order an iphone 14 then i would likely press the link without second thought, however, considering the nature of this google form you made, and the amount of times I've already been hacked on the internet (while embarrassing to admit), it's made me more aware that the url seems way too specific, and does not use backslashes to redirect to a more specific page on a more general website, I would be more hesitant in this case, and that's aside from the fact the email contains weak grammatical skill and looks to be informal (non capitalised words in places where there should be capital letters), often a mistake foreigners make, and foreigners are often the kind of people that would pull off this kind of trick, not being racist. Overall though I would still likely press this, it seems very genuine aside from a few nitpicks. This in reality, could very well be genuine.

Utilised my name and product that had been brought. If that specific model of phone had not been brought then I would think it is fake, however I don't have this info.

yes it provides a tracking link

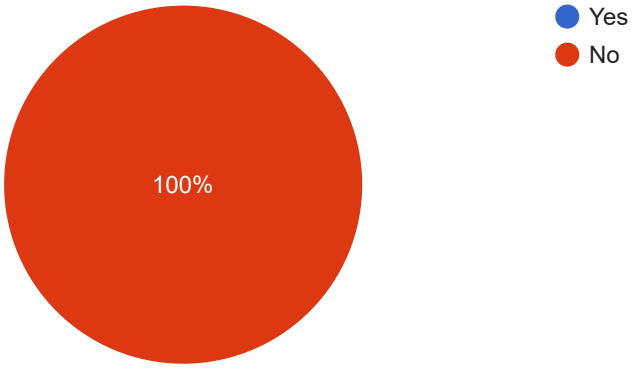
seems reputable

Email 1

Do you think the above Email is genuine?

Copy

20 responses

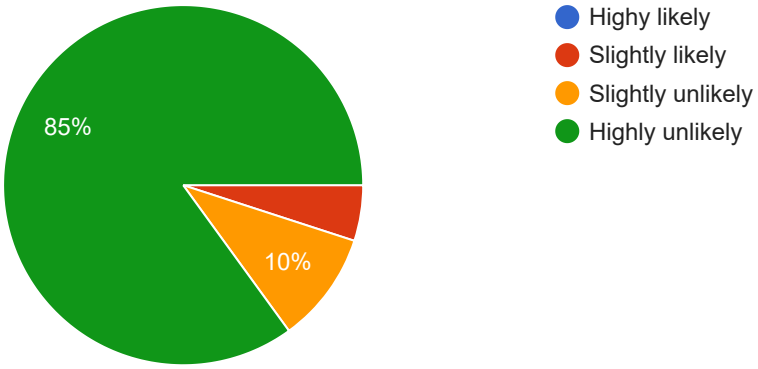


Follow up 2 no

How likely are you to fall for this ?

Copy

20 responses



Also why did you say it wasn't genuine?

19 responses

Because it asked for your account username and password, no one legit would ask for this.

The IT department should already know my password, they shouldn't be asking for it.

Not sending a password for obvoius reasons.

They should already have those details

Bad grammar in the "username and password" bit despite formatting. Also IT department would never ask someone to send password via email, for security purposes.

Because it asked me to supply my email and password

Because no specific information was provided meaning it could of been made for any company and not the company john works for

Way too obvious, a company will never ask for your personal details directly, their email is also very fake-looking although I assume you just made some random example up for this scenario.

Sending account information and other personal information is not advised as emails can be intercepted. In addition, should a company begin migrating email accounts, it is likely there would be some forewarning.

The IT department should already have access to the usernames and passwords of the employees.

it asks for a password which is not something you would give out

The IT department would not contact you in such a way and ask for this information

It asks for your password. Any company doing account migrations would migrate the account and ask you to create a new password, not set up the new migrated account with the same password as before. If this is genuine, the security team have pretty bad standards they follow and will need to revise how they would go about doing account migrations.

Companies don’t ask employees for their passwords over email

vague email address and greeting to all employees, IT department should already have this information anyway.

asks for password

needs username and password which you shouldn't give out

should never share these details

sharing user and passwords is wrong and wouldn't be asked

follow up 2

Briefly, what made you think it was a legitimate email?

0 responses

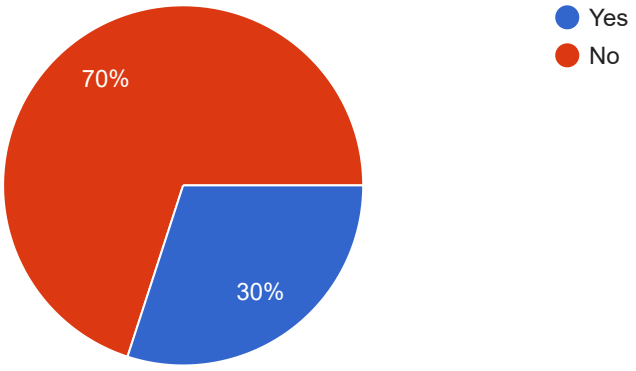
No responses yet for this question.

Email 2

Is the above email genuine?

Copy

20 responses

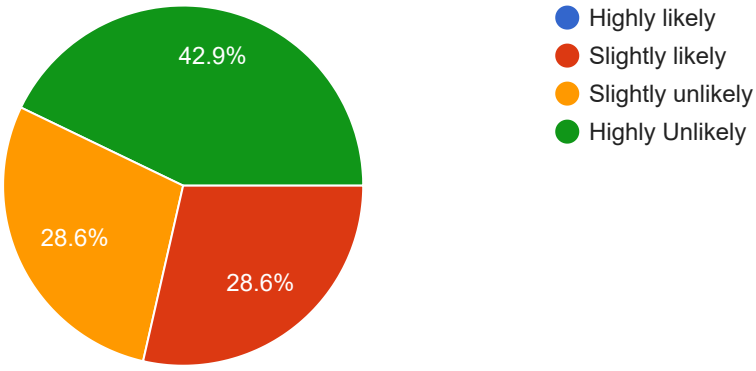


Follow up 3 no

How likely are you to fall for this?

Copy

14 responses



Also why did you say it wasn't genuine?

14 responses

The url is like really sus ඞ

Because it should keep personal information private

I will call them on official number to find out

Bad casing, and there was a student finance scam similar to this sent out via text message a while ago which involved clicking a link to a clone of the government's own website, but was a different one, where you were prompted to enter a lot of personal info. Very easy to fall for

Banks never contact you for information

Banks will usually ask you to go to their own website to check for suspicious activity. Links in the email may not actually go to the bank.

I don't trust any email which sends a link to click, go to the website through the normal means and not through a link in an email.

Banks would not send a link to fix this issue it would be something to be fixed in-store, over the phone, or through an app.

Your bank would most likely call you about such an issue not email

The contact number at the bottom of the email is not the same as the number if you look up 'halifax customer support number' online. There is a missing capital letter at the start of one of the paragraphs. I would have though halifax would use 'halifax@...' rather than 'halifaxbank@...'. The link to confirm your identity is suspiciously long

Nah

I think it would be suspicious if my bank wanted me to log in through a link due to prevent issues surrounding phishing with banks.

they usually hash the details but it could be real

anything requesting banking should call me not email me like this

Follow up no3

Briefly, what made you think it was a legitimate email?

6 responses

It contained specifics such as account number, provided steps on how to protect the account and also gave contact details to contact the bank.

The email link is provided multiple times, as well as the account number which should only be accessible to the bank

Valid and related email provided, very specific information provided that a bank would have regarded account numbers, worded formal and doesn't seem to have errors meaning showing care amd not writes as a spamm to multiple people

Even through a link you should be aware of keyloggers, however in this case they are asking you to CHANGE your password, all you need to do is review what's going on with these suspicious logins and change the password on your own intuition if you feel like it, and if this was a phishing link, they probably wouldn't have the ability to actually change your password on the actual halifax online banking systems through their own link anyways, you'll be giving them a new password which would not be the same as your old password, so they're not getting much out of it.

it has an account number

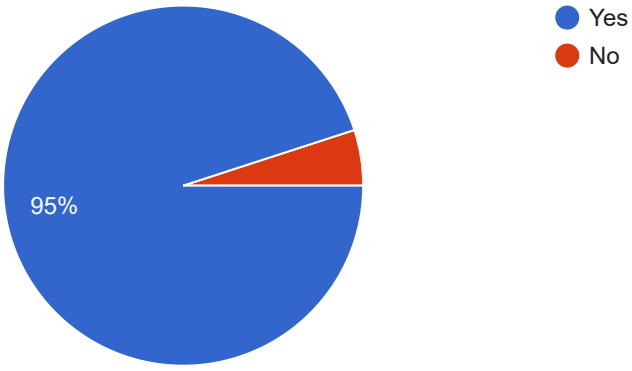
provides bank details

Email 3

Is the email above genuine?

Copy

20 responses

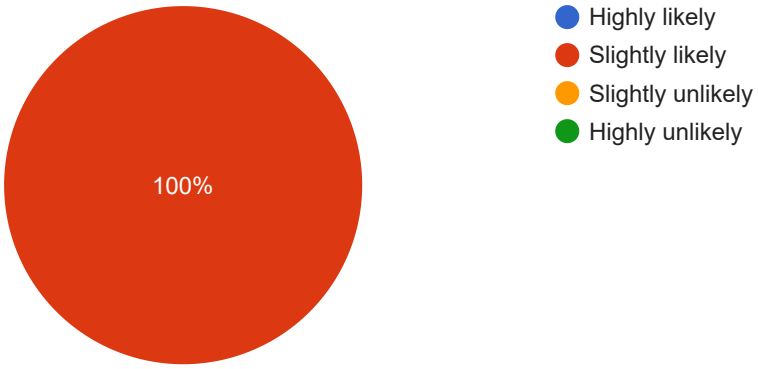


Follow up 4 no

How likely are you to fall for this

Copy

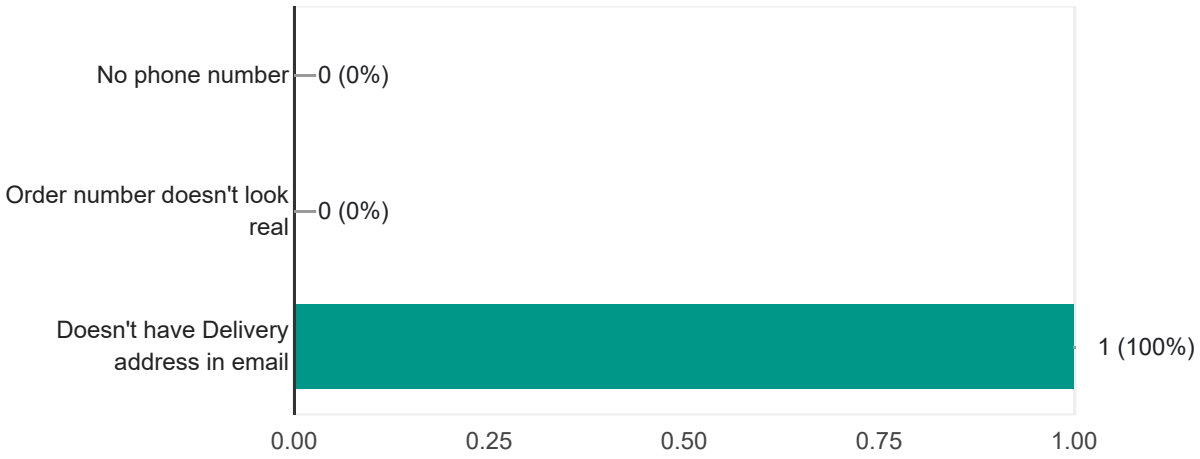
1 response



Pick the reason why you think it isnt genuine?

Copy

1 response



Follow up 4

Briefly, what made you think it was a legitimate email?

19 responses

It contained specifics such as order number and estimated delivery date as well as providing contact examples for customer service.

There are no links that could possibly be dangerous, and the order number is stated.

Mostly cause it didnt mention contacting them through any emails or anything. Just a notification.

Because it tells you to go to the trusted app

Not asking for anything

1. Quite a passive email - doesn't prompt for any personal or sensitive info to be entered.
2. Was sent to John right after he made the purchase
3. Good structure, format, grammar, etc

It didn't actually ask for any information or ask me to click or go anywhere, it was purely informing me that my package was due to arrive and did not ask me to go any further

Specific information provided, addressed by name, no response required prefenting anyreason for information to go out

No links provided, no asking for any passwords, and they even use their own (very likely well moderated) app to track packages rather than a link or website.

There are no links in the email, and the order ID is included in the email. If the order ID is consistent with the order John made, as well as there are no prompt to click any links in the email it is unlikely to be a phishing scam. However, there is a likelihood the order ID was still intercepted.

The email doesn't contain any links and directs you to go to the customer service without a link. This email is also responsive to john placing an order so is expected.

It gives no added information or requiers the need to go to another location, this also looks like a normal confirmation email

The layout of the email and the language used

It is not asking for any information from the recipient, and John can compare the order ID in the email to that on Amazon's website to make sure its genuine.

No dodgy urls

they give order number, and email isn't asking the user for anything.

it provides order details

it contains delivery date

it provides delivery date