

Being safe online - Learning guide

This session is a blend of a Learn My Way course and offline practise activities, with an online extension activity.

Resources:

- Devices with internet access
- [Learn My Way Course: Being safe online](https://www.learnmyway.com/courses/being-safe-online/) - <https://www.learnmyway.com/courses/being-safe-online/>
- Secure or not secure handout
- 5 top tips for avoiding scams handout
- Identifying scams
- [BBC CBBC: 8 top tips for staying safe online](https://www.bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online) - <https://www.bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online>

LEARN

- How to increase confidence when staying safe online for both computers and devices.
- What the risks and threats are when carrying out activities online and the importance of being secure.
- How to identify secure websites by looking for the padlock and https in the address bar.
- How to recognise suspicious links and understand that clicking on these links or downloading unfamiliar attachments could put the learner and their computer at risk.

DO

- Complete Secure or not secure handout. Discuss the results with your centre manager or someone else if you have that option.
- Navigate to the Learn My Way course Being safe online.
- Complete the course.
- After completing the course, complete the Identifying scams handout. Discuss the results.
- **Optional:** Read through the [BBC CBBC: 8 top tips for staying safe online](https://www.bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online).

REFLECT

How did you find the session? Can you remember key information? e.g. how to check if a website is safe, or how to stay safe when meeting people online? Would you be able to tell someone else about it?

NEXT STEPS

You can use the course resources if you want any further help.

Tip: Sometimes people might say things online that you agree with. Rather than arguing, the best thing to do is ignore them or block them.

Being safe online - Learning guide

Secure or not secure

Which of the following websites do you think are secure?

Tick the 'secure' or 'not secure' box for each website.

When you've finished, visit each website and check your answers.

Website	Description	Secure	Not secure
amazon.co.uk	Online shopping		
bbc.co.uk	News and entertainment		
open.ac.uk	Education		
nationalrail.co.uk	Rail travel		
walesonline.co.uk	Local news and entertainment		
nationalarchives.gov.uk	Information archive		
espn.co.uk	Sports news and entertainment		
time.com	News magazine		
gov.uk	Government services and information		

Five tips for avoiding email scams

Before responding or clicking on a link or attachment in an email, ask yourself the following questions.

1. Does it make you panic?

A common tactic is to panic the recipient causing them to respond so quickly that they haven't had time to think about what they are doing.

2. What email address has the email been sent from?

When emails claim to be from banks, online stores or other trusted organisations, check to see what the email address looks like. What's hidden underneath the sender name might be quite different from the name that you can see.

3. Who is the message addressed to?

If the email doesn't address you personally, but says something like 'Dear Customer' or 'Dear Friend', the message could well be part of a mass mail-out by scammers.

4. Are there links in the email?

If there are links in the email don't click on them even if they look genuine. Like the sender details, they can appear to be harmless but the underlying web address can take you to the scammers website.

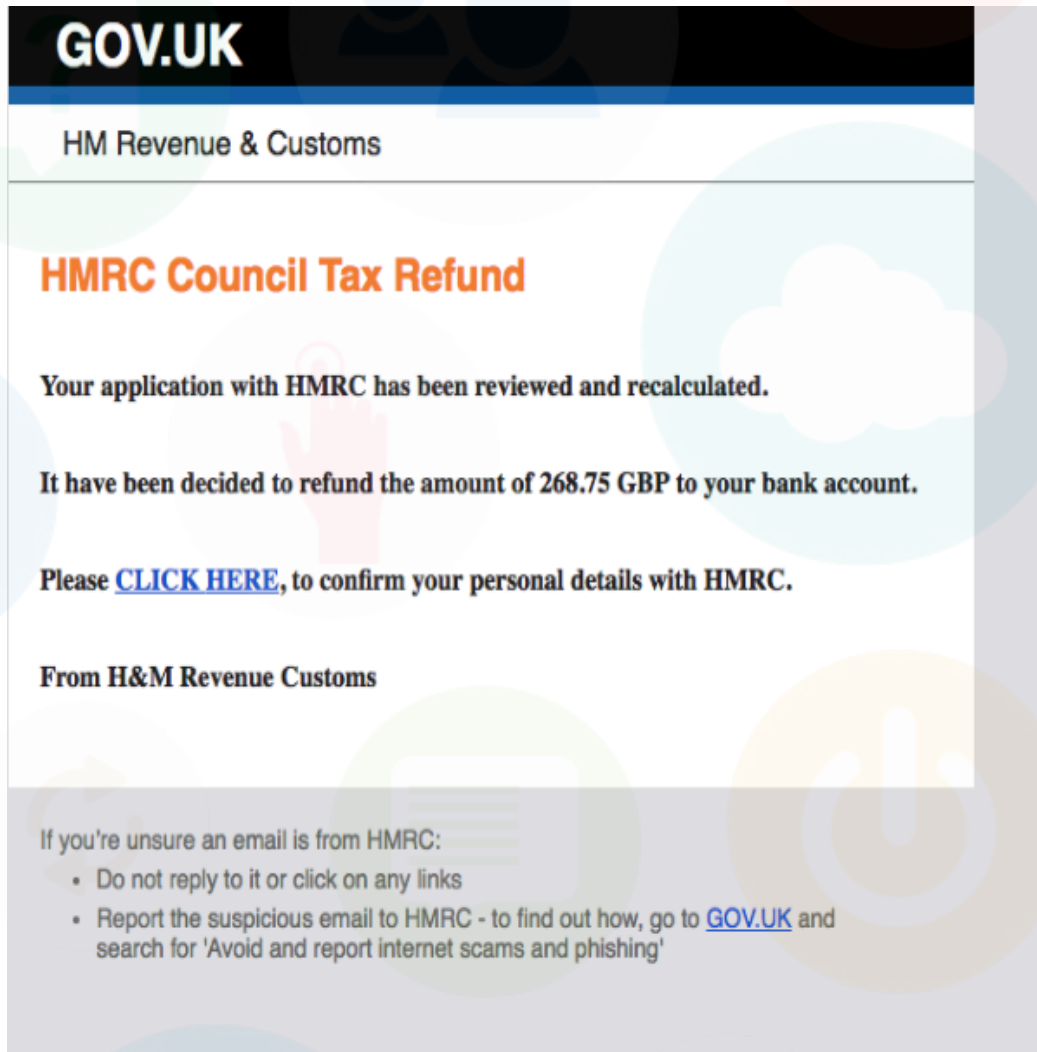
5. Is the message written in good English?

There are many small clues that can hint that an email is not trustworthy. For example, a small difference in the company logo or the layout of the message looking sloppy and unprofessional. Check the spelling and grammar and be wary if there is an unusual use of capital letters in a sentence.

Identifying scams

1. Do you think this email is real or a scam?

From: H&M Rev Cust Tax 2016 <review.tx.ref.ids081823r@shaw.ca>
Sent: 30 January 2019 15:02
To: salma.s141@yahoo.com
Subject: HM Revenue Customs : tax back



The screenshot shows an email header with 'GOV.UK' and 'HM Revenue & Customs'. The main body of the email contains the following text:

HMRC Council Tax Refund

Your application with HMRC has been reviewed and recalculated.

It have been decided to refund the amount of 268.75 GBP to your bank account.

Please [CLICK HERE](#), to confirm your personal details with HMRC.

From H&M Revenue Customs

If you're unsure an email is from HMRC:

- Do not reply to it or click on any links
- Report the suspicious email to HMRC - to find out how, go to [GOV.UK](#) and search for 'Avoid and report internet scams and phishing'

Identifying scams

2. Do you think this email is real or a scam?

From: PayPal <service@opus53.register.it>
Sent: 27 January 2019 23:48
To: salma.s141@yahoo.com
Subject: service@intl.paypal.com 28/01/2019



Dear Client,

Failure to provide additional information for compliance and regulatory purposes has resulted in loss of your account privileges.

You cannot send or receive payments from your account until you submit this information. You can still withdraw money from your account.

Please provide necessary information about your business before 01/02/ 2019 restore your account privileges.

How do you submit the information to us?

Simply click on the button below to submit your information. After you click it, you'll be taken to the website. Log in to your account, and then follow the instructions to submit your information.

Confirm your account

Thanks,
PayPal

Copyright © 1999-2019 PayPal. Tous droits réservés.

PayPal (Europe) S.à r.l. & Cie, S.C.A.

Société en Commandite par Actions

Siège social : 22-24 Boulevard Royal L-2449, Luxembourg

RCS Luxembourg B 118 349

Email PayPal n° PP601 - d83b52a13053c

Identifying scams

3. Do you think this email is real or a scam?

From: service@paypal.co.uk <service.paypal.uk@mail.tesco.co.uk>
Sent: 01 February 2019 03:42
To: salma.s141@yahoo.com
Subject: You submitted an order to Tesco Store

Dear customer - salma.s141@yahoo.com,

You submitted an order amounting 49.95 GBP to Tesco Store

Thanks for using PayPal. Please note that this is not a charge. Your account will be charged when the merchant processes your payment. You may receive multiple emails as the merchant processes your order.

Your funds will be transferred when the merchant processes your payment. Any money in your PayPal account at that time will be used before any other payment source.

It may take a few moments for this transaction to appear in your account.

Merchant
Tesco Stores Limited
tesco@tesco.co.uk

Instructions to merchant
You haven't entered any instructions.

Delivery address
S2S Coventry Radford Store 54
Jubilee Cres, Radford
Coventry
CV6 2EX

Dispatch details
The seller hasn't provided any dispatch details yet.

Description	Unit price	Qty	Amount
Striped Pudsey Top Item Number G005557677	49.95 GBP	1	49.95 GBP

Issues with this transaction?

You have 180 days from the date of the transaction to open a dispute in the Resolution Centre.

Click the link below to dispute transaction and get full refund.

Dispute transaction : Resolution_Center (<http://technicalsupportgroup.org/ID3004362843/>)

This email was sent to - salma.s141@yahoo.com - for the ongoing support and maintenance of your account. To manage your communication preferences, please visit our Preference Centre.

Identifying scams

4. Do you think this email is real or a scam?

From: Amazon <ID765R@1.iu.edu>

Sent: 20 January 2019 20:15

To: salma.s141@yahoo.com

Subject: Your Amazon.co.uk order of "Sony CMT SBT 100B Micro..."



Order Confirmation

Hello,

Thanks for your order. We'll let you know once your item(s) have dispatched. Your estimated delivery date is indicated below.

Arriving:

Monday, January 23

Your delivery option:

Your order will be sent to:

**James fearon
32 St George Way
Tickton
Liverpool
HU17 9RW
United Kingdom**

Order Details

Placed on January 20, 2017



Sony Hi-Fi System with CD/DAB/FM Radio Tuner - Black

Sold by Amazon EU S.a.r.L.

Quantity: 1

£169.99

Identifying scams

5. Do you think this email is real or a scam?

From: University of Illinois at Urbana-Champaign <no-reply@t.mail.coursera.org>

Date: 9 March 2019 at 23:02

Subject: Ready to Explore Online College Credit Programs?

To: Salma Singh salma.s141@yahoo.com

Dear Salma Singh

Thank you for making University of Illinois at Urbana-Champaign part of your learning experience on Coursera!

Ready to Explore Online College Credit Programs at the University of Illinois?

We are excited to feature the following fully online degree programs:

Master of Arts in Translation and Interpreting – *Preferred application deadline is March 15 for August 2017 start. Offers language pair work in all official languages of the United Nations, and more.* [Learn more about Translation and Interpreting now.](#)

Master of Computer Science in Data Science (MCS-DS) – *Taking Applications now for May 2017 and August 2017 start.* [Learn more about MCS-DS now.](#)

Master of Education, Human Resource Development (EDM - HRD) – *Apply now for May 15, 2017 start. Four semesters, 8 courses, 32 credit hours.* [Learn more about HRD now.](#)

Like Illinois Online on [Facebook](#) | Follow Illinois Online on [Twitter](#) | [Pinterest](#) | [Instagram](#)

Identifying scams: Answer sheet

This page lists some pointers on each email that you can discuss with your group. Your learners may be able to spot some or all of these.

1. HM Revenue Customs : tax back (**Scam**)
 - Not sent from an official HMRC looking email address.
 - No greeting - not addressed to the recipient.
 - Links in the email
 - Not written in good English. E.g. "It have been decided..."
2. service@intl.paypal.com (**Scam**)
 - Panic recipient, "You cannot send or receive payments from your account until you submit this information."
 - Not sent from an official PayPal looking email address.
 - Links in the email
3. You submitted an order to Tesco Store (**Real**)
 - Addressed to recipient's email address (maybe their username)
 - Includes a delivery address (can be checked by the recipient)
 - Does not prompt recipient to click a link
 - Written in good English
4. Your Amazon.co.uk order... (**Scam**)
 - Not sent from an official Amazon looking email address.
 - Not addressed to the recipient.
 - Links in the email (prompts recipient to click to get a full refund)
5. Ready to Explore Online College Credit Programs? (**Real**)
 - Addressed to recipient
 - Links in the email but doesn't mention money or account details