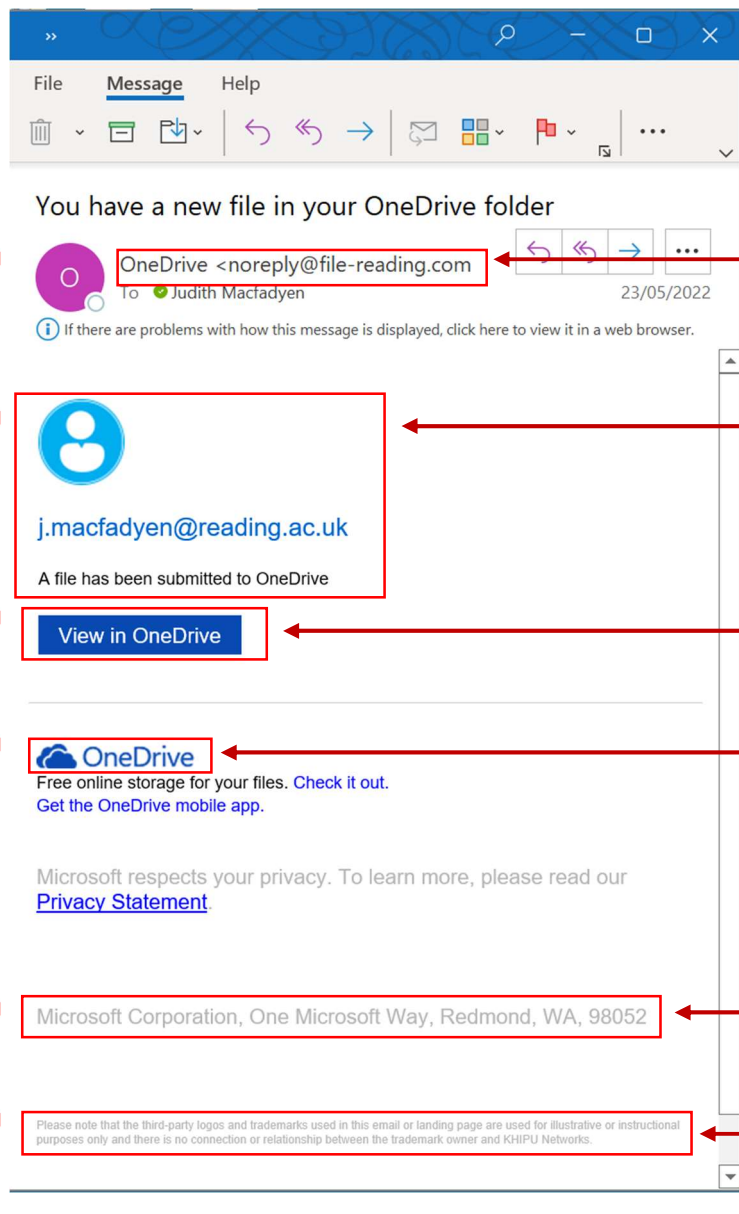


DTS phishing campaign May 2022

The email that arrived in your inbox looked genuine, but take a closer look:



What should you have spotted in this phishing email?

Odd looking “From” address, neither Microsoft nor University of Reading. Haven’t seen it before = suspicious. Best check the rest.


What is this asking me to do? It doesn’t tell me who has shared a file, and I’ve never had an email before when I’ve uploaded something to OneDrive. Something doesn’t feel right.

Hover over the links, they all go to <https://www1.file-reading.com/uor2831>. That’s not my OneDrive weblink.

Old logo! Definitely not right.

This is the correct address for Microsoft? But hang on, anyone can look this up. There are too many other errors.

Small print tells you it’s from KHIPU. Even if you don’t know who they are, you do know they aren’t Microsoft or UoR.

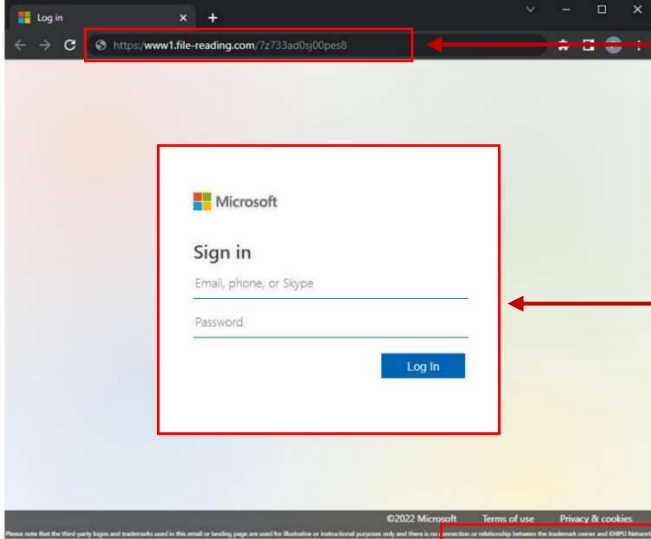
This email contains several red flags . Together there was enough information to make you stop and consider whether clicking the link and signing in was a good idea.

- ✓ Check the email address
- ✓ Check the message makes sense
- ✓ Check spelling – controversially, everything was correct in this email!
- ✓ 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.

This is the login screen you were taken to:



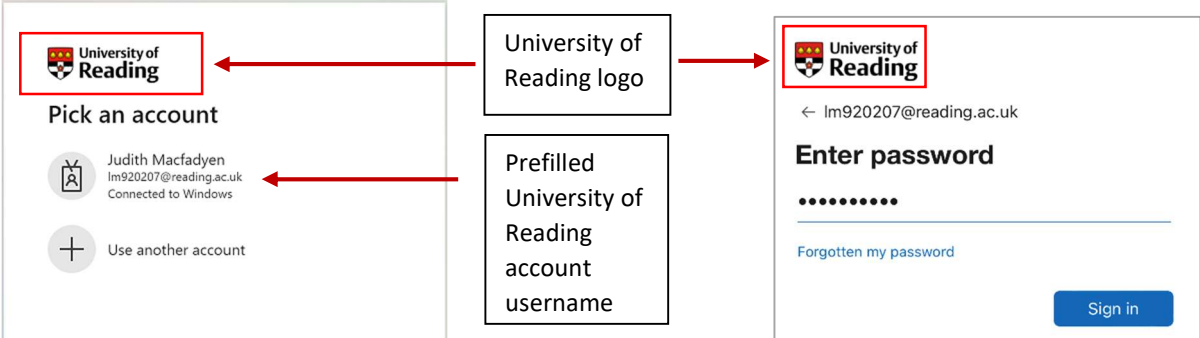
Web address doesn't mention Microsoft or OneDrive.
Correct address:
login.microsoftonline.com

Single page to log in, with password on same page, whereas Microsoft has a separate password page.
In a genuine Microsoft login, the Password page would have the UoR logo

KHIPU Networks?

The screenshot shows a browser window with a URL that does not include 'Microsoft' or 'OneDrive'. The login form is on a single page, and the footer contains '©2022 Microsoft' and 'KHIPU Networks?'. Red arrows point from the callout boxes to the URL bar, the login form, and the footer.

Here is what you would expect to see if you were signing in to your University OneDrive:

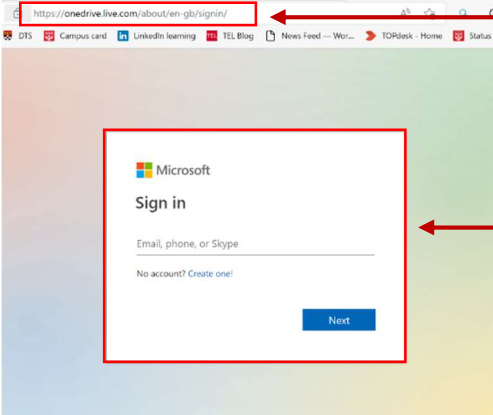


University of Reading logo

Prefilled University of Reading account username

The sequence shows two screens. The first screen has the University of Reading logo and a 'Pick an account' section with a prefilled account 'Judith Macfadyen'. The second screen shows the 'Enter password' page with the same logo and a 'Sign in' button. Red arrows point from the callout boxes to the logos and the prefilled account information.

This is a genuine Microsoft login page.



Web address includes the word **OneDrive**

In a genuine Microsoft login page, you enter your email, then go to the Password page.
The Password page then has the UoR logo on it, as your Microsoft account has been recognised by your username.

The screenshot shows a browser window with a URL that includes 'onedrive'. The login form is on a single page with a 'Next' button. Red arrows point from the callout boxes to the URL bar and the login form.