Important Information for Schools

Spam Email

We are aware of an increase in Spam emails being received by schools and local government agencies since the beginning of April 2017 being delivered to email users mailboxes.

The following information provides advice and guidance on how to identify spam and malicious emails which may purport to be from legitimate sources such as Derbyshire County Council.

Please note, spam email increases the risk of ransomware and further distribution of spam to other recipients and infection of viruses and trojans.

Derbyshire schools receiving emails where the display name of the sender appears to be from a Derbyshire County Council source, for instance SchoolSAP should check the underlying email address and that it has come from a genuine address such as [name]@derbyshire.gov.uk

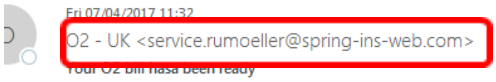
Emails where the email address (not display name) is unknown should be deleted immediately. Staff are reminded of the following when dealing with unexpected or suspicious emails;

- Do not open attachments;
- Do not click on embedded links within emails from unknown sources, instead roll the cursor over the link to reveal its true destination;
- Do not reply to unwanted emails;
- Do not forward suspicious emails

How to check the source of an email

Example 1

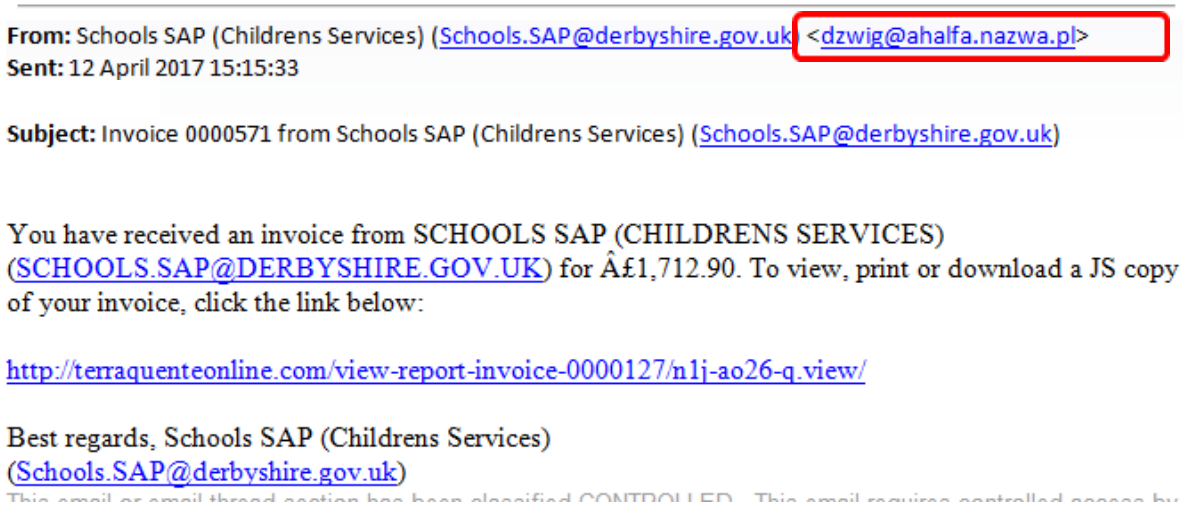
The email below appears to have been sent from o2. However, when you examine the From information you'll notice that the senders email address bears no relation to an o2 email address. Typically, the email address would be in the format [name]@o2.co.uk.



Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Example 2

The following is spam email sent from outside of our organisation, but appears as though it was generated by the School SAP team. If you check the From details you'll notice that it's from an email source outside of our organisation, and not from a @derbyshire.gov.uk email address.



From: Schools SAP (Childrens Services) (Schools.SAP@derbyshire.gov.uk) <dzwig@ahalfa.nazwa.pl>
Sent: 12 April 2017 15:15:33

Subject: Invoice 0000571 from Schools SAP (Childrens Services) (Schools.SAP@derbyshire.gov.uk)

You have received an invoice from SCHOOLS SAP (CHILDRENS SERVICES) (SCHOOLS.SAP@DERBYSHIRE.GOV.UK) for Â£1,712.90. To view, print or download a JS copy of your invoice, click the link below:

http://terraquenteonline.com/view-report-invoice-0000127/n1j-ao26-q.view/

Best regards, Schools SAP (Childrens Services)
(Schools.SAP@derbyshire.gov.uk)

Action

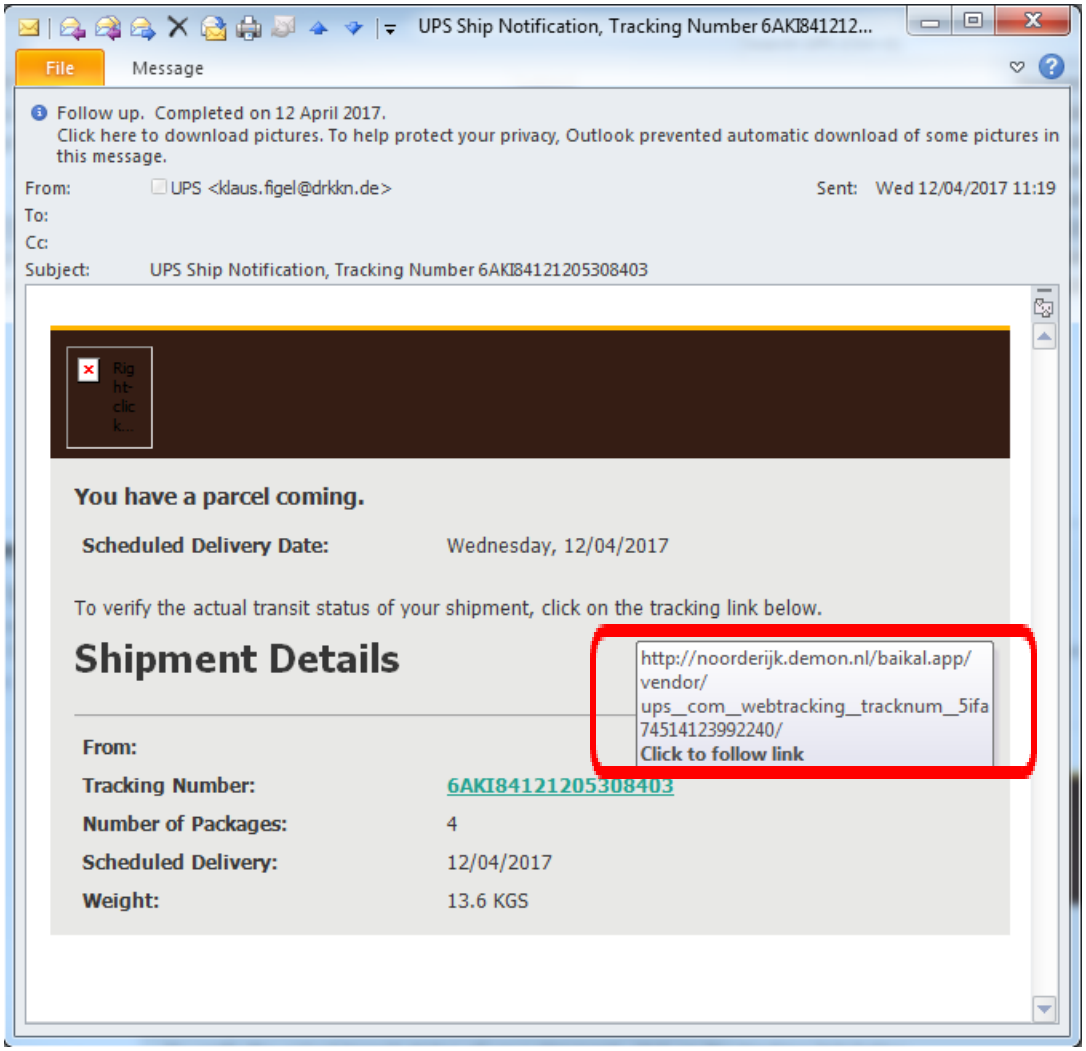
- If you suspect the nature of the email check the From details.
- If you do not trust the email delete it – do not forward it or click on any links or attachments.

How to check a web link in an email

The email below appears to have been sent from UPS. Within this email there's a link against the tracking number.

When you hover over the link (do not click) you will see the web address (URL) of the website you would be taken to if you clicked on the link.

The link includes UPS in the detail but the actual address is hosted in the Netherland (http://noorderijk.demon.nl) and would not display the official UPS website.



Action

- If you suspect the nature of the email check the web links, if you are suspicious of the link, delete the email
- Remember, do not forward it or click on links or attachments.
- If you've received an email that you were not expecting or is not relevant, delete the email.