HOW TO SPOT FAKE E-MAILS

Check the reply e-mail

It's easy to spoof the address an e-mail is sent from. Check out what the reply address is – does it look right?

Personal addressing means nothing

If your e-mail and information about your work is available on the internet, it's easy for someone to find it and address.

Take care with attachments

Take extra care when an e-mail comes with attachments – these can contain viruses. Only open these if you're sure.

Beware links

Just like attachments, links can also lead to your computer being infected with viruses. Hover over the URL to see where it goes, and whether this looks legitimate.

Look at checking tools

There are ways of better spotting spam which can be done at server level, such as SPF and DKIM checkers – research these for more.

Look at the layout

Does it look different to the sort of e-mails you normally receive from the sender indicated in the mail?

Look out for errors

While spammers are getting better, there are still often basic language mistakes in e-mails which should raise suspicions.

Is it asking for personal information?

Malicious e-mails often aim to steal personal data, such as bank information or beyond. Be very careful around sharing this.

IFLA International Federation of Library Associations and Institutions

ifla.org