Email Security

Malicious cyber-attacks can happen to anyone, and they usually come via email. Take a look at some of the different types of risks and how to stay safe online.

Protect yourself and your device.

Ransomware

All ransomware emails are different but they will all include an attachment. This may be a zipped or encrypted file.

Ransomware is a type of software that blocks or limits you from accessing your computer's system. It may lock your screen or encrypt your files, threatening to publish or delete the files until a ransom is paid.

The email might include a code and instructions to execute. It might have a friendly tone with content or information relating to a parcel delivery, an invoice, account or document, etc.

Email scams

Scams are generally delivered in the form of a spam email (but remember, not all spam emails contain scams).

Scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

Examples of email scams include:

- emails offering financial, physical or emotional benefits that are, in reality, linked to a wide variety of frauds

- emails seeming to be from ‘trusted’ sources such as your bank, the Inland Revenue or anywhere else that you have an online account. They ask you to click on a link and then disclose personal information.

Phishing emails

Phishing is when cyber criminals send emails pretending to come from well-known banks or a trusted organisation in an attempt to defraud you or steal your identity.

They usually have a sense of urgency and will try to trick you into clicking on a link that goes to a fake website.

Outsmart the cyber attackers - check for the typical flaws in a phishing email:

- The email address will be different from the trusted organisation’s web address.
- The email is often from a free email host, such as Yahoo, Hotmail or Gmail.
- The email doesn’t address you by name, but addresses you as your email address or “Dear customer” etc.
- A sense of urgency, such as threatening that ‘your account may be closed...’.
- A request for personal information such as username, password or bank details (UAL and banks etc never ask for this via email).
- A prominent link to a bogus website.

Use email safely

- UAL will never urgently ask you to confirm or alter your personal or log-in details, via email.
- Never click on links in emails from unknown sources. You can check a link’s destination by hovering the cursor over the link: the true destination shows in the bottom left corner of your screen.
- Never open emails that you think are spam.

- Never open attachments from unknown sources.
- Never make purchases or charity donations in response to spam email.
- Never click ‘remove/unsubscribe’ or reply to emails from unknown sources.
- Check junk mail folders regularly in case a legitimate email gets through by mistake.
- If in doubt, call the IT Service Desk (020 7514 9898).Find more about email and protecting yourself from cyber-attacks at getsafeonline.org.

Passwords

- The first time you login to your UAL email you’ll be asked to change your password.
- Make sure your password is secure by using a combination of letters, numbers and symbols. Don’t re-use old passwords.
- Complete the security information on Password Self Service so you can reset your password if you forget it.
- Forgotten your password? Reset it.
- Your password will expire 365 days after your reset it. Ensure that you change your password regularly.