Dear Subscriber,

We have recently updated our website to improve our security. Due to this an account update has been issued and your account information is required immediately or we will lock your account permanently. Please click the link below and follow the instructions to ensure your account is enabled and not blocked.

RESOLVE (http://clasicafidesk.jimdo.com/)

Note: It is important that your personal information is accurate and complete. This information may later be used to help verify the owner of the account.

Thank u
Help Desk Team

Copyright © Trinity College Dublin. All rights reserved

---

**How to recognise a phishing message**

While TCD staff and students are generally very good at spotting a phishing attempt, it is still a real problem and has affected at least 100 people in College over the last year.

We’ve highlighted a few typical elements to a phishing email below so that you can recognise one right away!


**Deceptive subject line**
The subject line is designed to scare or entice you to open the email.

**Forged email address**
The sender’s email address may be forged, even if it looks legitimate.

**Urgent request**
An urgent request with immediate consequences attempts to intimidate you into responding without thinking.

**Official looking logos or signatures**
Scammers can easily access official looking logos or signatures from websites and include them in their phishing emails. Do not assume the email is legitimate simply because it includes an official looking graphic.

**Disguised or modified link**
When you hover your mouse over a link, the actual URL you are being directed to is displayed at the bottom of your browser window.

**Request for personal information**
IS Services will never request your username or password information through an email. Be very wary of any message that requests personal information through email.