



Phishing is a type of spam email that tries to **trick** you into disclosing sensitive personal or financial information such as your UCD Connect **login** or **credit card** information.

Phishing emails are extremely common in UCD with staff receiving a large number of unwanted phishing emails each week. Most phishing emails thankfully go directly into your spam, however the most realistic and sophisticated emails can go into your inbox and can be hard to recognise.

In order to help **protect** your work, personal and financial information is it very important that you are able to **identify** and **safely ignore** phishing emails. Just like any theft disclosing personal, work or financial information to an unauthorized person can be very distressing and damaging. So you need to be **vigilant!**

Below are a number of ways that will help you spot a phishing email.

1. **Urgent emails** – be wary of statements like “click today” “get in touch asap”
2. **Suspicious links** – Never trust links in email. Go directly to the official URL. (see example below)
3. **Unexpected attachments** – never open an attachment you’re not expecting
4. **A request for personal information** – never send your personal information or login details in an email
5. **Unexpected emails** – unsolicited contact from your bank provider, for example, is highly unusual
6. **Poor grammar, generic and informal greetings** – spelling mistakes, typos and unusual phrasing, a lack of personalisation and formality is indicative of a fraud
7. **Striking gold** – if it is too good to be true, then it is too good to be true.

If in doubt or you need advice please contact the IT Helpdesk at 01 716 2700 or email ithelpdesk@ucd.ie

The following is an example of a phishing email sent to users in UCD

Sender's Email Address:
Official IT Helpdesk communication is always sent from ithelpdesk@ucd.ie

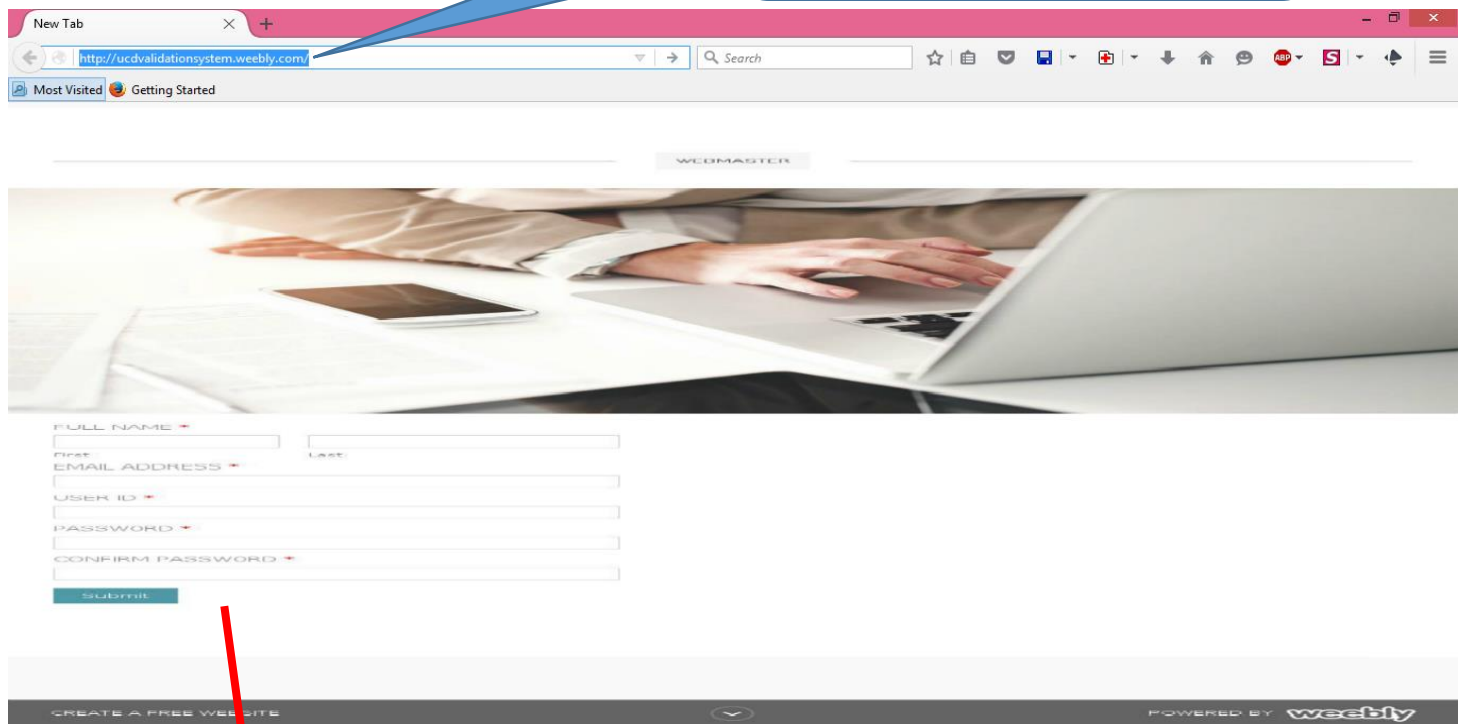
Bogus URL:
Website is bogus e.g. <http://ucdvalidationsystems.weebly.com> , it's not an official UCD page e.g. <http://www.ucd.ie>

Email Content:
From: UCD CONNECT <phisher@phishing.com>
Date: 26 November 2015 at 09:17
Subject: Deactivation of Account
To: Undisclosed Recipient
|
Staff and Student
Your email has exceeded the limit. Please contact your system administrator, to have access to your email account after upgrade **CLICK HERE** to verify your identity.
UCD Admin Team

The following is an example of a website link used in a phishing email to UCD users

<http://ucdvalidationsystem.weebly.com/>

Website is a bogus site. It's not an official UCD page e.g. <http://www.ucd.ie>



IT Services will never ask for your Login ID, password or other personal information via an e-mail link. If you are suspicious please contact the ithelpdesk@ucd.ie for advice

FULL NAME *
First Last
EMAIL ADDRESS *
USER ID *
PASSWORD *
CONFIRM PASSWORD *
Submit