Dear All,

The RVC’s Infrastructure Services Directorate (ISD) is responsible for managing the cyber security of the College and its members and so regularly carries out upgrades to further improve the security of the College’s IT systems.

One such improvement, to be introduced on Thursday 22nd November 2018, will alter the Microsoft Outlook authentication process that is used to access the RVC email system from all devices and operating systems. This change (advised by Microsoft) therefore affects all RVC email users but is necessary to maintain the latest security protocols and standards that are in use.

Until now, you have only been asked for your username and password when setting up the Microsoft Outlook application for the first time, as shown in Table A below.

**Table A: Current Outlook user authentication screen**

|  |  |
| --- | --- |
|  | The credentials required are your RVC email address and password, and ticking the ‘Remember my credentials’ check box is recommended. |

However, this method is no longer considered to be 100% secure as it stores the password permanently on users’ device. In order to improve this, Microsoft’s recommendation is now to implement their ‘Modern Authentication’ method, as shown below in Table B. Please note, this requires that users re-authenticate every 90 days to re-confirm their identity.

**Table B: Revised ‘Modern Authentication’ user authentication screens**

|  |  |
| --- | --- |
|  | Enter your RVC email address when prompted. |
|  | Select ‘Work or school account’ option if presented. |
|  | Enter your RVC email address and password, and click ‘Sign In’ |

Should you experience any problems with logging in to RVC email or other IT systems after this security upgrade is carried out on Thursday 22nd November 2018 please contact the ISD IT Helpdesk via [helpdesk@rvc.ac.uk](mailto:helpdesk@rvc.ac.uk) or telephone 0207 4685181 for assistance. helpdesk@rvc.ac.uk or telephone 0207 4685181 for assistance.

*Reminder: ISD do not ask users to supply their password to IT staff for support purposes - if you have concerns that a log in screen or email link is not genuine, do not supply the requested details but instead immediately contact the ISD IT Helpdesk for advice.*