Version 1.0 (last updated 12th September 2014)

Mobile Device Security

Overview

As part of ISD's program of security enhancements to our systems this guide gives details on the activation of security settings which have been applied to mobile devices accessing the UEA email system.

This change affects Staff, Post Graduate Researchers, and Visitors who access email via a mobile device such as an iPhone, iPod touch, iPad, or other type of Smartphone or Tablet. If you do not access your email via this method then you will not be affected.

UEA has now enforced the use of a 6 digit PIN code or lock code on any mobile device that is currently set-up with access to UEA email systems. The aim of this is to stop any unauthorised viewing or use of UEA email in scenarios such as when a mobile device is left unattended or if lost. These changes have been driven by a need to improve security, and have been endorsed by Information services governance committees.

Passcode Feature

You are now required to activate and setup a passcode lock on your mobile device if you are accessing UEA Email. **It is very important that you follow these instructions.**

Phishing Reminder: Official UEA emails will never ask you for your password or account details.

Before setting up email on your mobile device:

- Backup your device
- Ensure that a REGULAR on-going backup process is in place to minimise the potential for future data loss.

During the setup of email on your mobile device:

- Ensure you follow the passcode rules & complexity requirements

Your passcode must be:
1. A minimum length of 6 characters / digits
2. No repeating patters e.g. 112233 or 111222

Your passcode must NOT be:
1. Any of the three previous passcodes you have used (only applicable if you have changed your passcode in the past)

Remote Wipe Feature

ActiveSync allows a mobile device that has previously been synchronised with the UEA email service to be remotely wiped by either the user (via Outlook Web Access/Webmail), or the system administrators of the service if a device were lost or stolen.

Devices will never be remotely wiped by the service administrators unless they are specifically requested to do so by the user who is the owner of the device.

What to do if you do not wish to be bound by this policy:
We are aware that a significant number of users use their personal mobile devices to access UEA Exchange email services. As such these users may be resistant to having such measures applied to their devices. Whilst we acknowledge these concerns, ITCS are obliged to ensure that the security and confidentiality of email and other UEA data stored on mobile devices remains so and is guaranteed. Officially supported mobile devices remain those provided by the University and as such we must ensure that these are secure. Users of personal devices are not being discouraged from continuing and there are now apps available which will allow you to separate your UEA environment from your personal environment. An example of this would be www.divide.com

IT Helpsheets have been created specifically for accessing email via mobile devices. These are available from the Online IT Helpdesk Wiki.

Further help or assistance

If you have any concerns over these proposed changes, please contact the IT Helpdesk on 01603 59 2345 or via email (it.helpdesk@uea.ac.uk), and your queries or concerns will be passed on to the Project team.