SEC-INF-002 – Compromised Account

PUBLIC

What is a compromised account?

If you disclose your University account credentials (username and password) to another user or a rogue site (not a valid **plymouth.ac.uk** resource) these details should be treated as being compromised. As you have no control over all the interactions that the account will perform from that point onwards.

In this instance, you **must immediately** undertake the following actions:

Corporate Responsibility

- Advise and/or assist staff with compromised accounts in changing their University account passwords;
- Suspend compromised accounts until such time as passwords have been changed;
- Providing information and training materials to improve and maintain staff awareness of information security threats

Personal Responsibility

- Contact the University's Service Desk immediately (servicedesk@plymouth.ac.uk) or call 01752 588588 to notify them of the compromise;
- Either get the Service Desk to, or change your University account password yourself – this will prevent the old credentials from being re-used;
- If these credentials have been used to access other (non-University) sites these credentials should be changed too;
- Check your bank, financial statements and social media sources you use regularly to identify and false charges or suspicious activity;
- Contact your bank to advise that your University account has been compromised and ask them to place a fraud alert on your account;
- Contact Payroll (payroll@plymouth.ac.uk or call 01752 588252) to ensure that your personal details, including your bank account have not been altered.
- Take any further action, or precautionary measures in line with University policy and best practice dependant on the nature of the incident that resulted in the compromised account; including, but not limited to, ensuring all your devices are up to date in terms of operating system and application security patches to reduce the risk being infected by malware.

Is there any additional advice or guidance?

Do not re-use old credentials, if your account has been compromised in the past, these details could have been posted online and could subsequently be re-used at a later date.

If you are struggling to manage lots of distinct passwords for different websites, consider using a Password Manager and there is guidance in the SEC-GDL-019 - Password-Managers document.

If you require more information on how to spot a Phishing email, there is guidance in the SEC-GDL-005 - Anatomy of a Phishing Email or Professor Steven Furnell's Phishing Video (Something Phishy: The Ongoing Threat of Classic Phishing).