

**User Credentials and Handling Compromise**

Version 1.0

**Contents**

[**User Credentials** 3](#_Toc85809091)

[**Signs of Account Compromise** 3](#_Toc85809092)

[**How did it happen?** 3](#_Toc85809093)

[**Protect your credentials** 3](#_Toc85809094)

[**Resolve the Account Compromise** 4](#_Toc85809095)

[**Strengthen Your Credentials** 4](#_Toc85809096)

[**1.** **Do Not Share Passwords** 4](#_Toc85809097)

[**2.** **Do not save passwords on shared devices** 5](#_Toc85809098)

[**3.** **Switch on Password Protection** 5](#_Toc85809099)

[**4.** **Change Default Passwords** 5](#_Toc85809100)

[**5.** **Use Two-Factor Authentication for Important / Sensitive Accounts** 5](#_Toc85809101)

[**6.** **Password Management** 5](#_Toc85809102)

# **User Credentials**

A user credential is traditionally a username and password that is assigned to a specific user. When your credentials have been compromised, it means someone other than the user has possession of the account information.

# **Signs of Account Compromise**

The sign of a compromised account will be activity that was not initiated by one of your authorised users. Any changes to user accounts that are not authorised evidence a compromise:

* Users unable to access their account.
* Phishing emails being sent from user accounts to colleagues / email contacts.
* Multiple password changes or forgotten password resets, especially in a short timeframe from unknown locations.
* Suspicious logins, or multiple unsuccessful login attempts.
* Unusual inbox activity, including emails with multiple recipients, and high numbers of BCC recipients.
* New inbox rules, such as automatically forwarding emails, moving emails to folders, or deleting messages.
* Profile changes with amendments to personal details, contact information, or unusual signatures.

Frequently it is the users themselves that become aware of issues, but network monitoring will also pick up unusual activity.

# **How did it happen?**

User credentials can be compromised by users themselves through password sharing or unsecure password practice, such as writing down credentials. It is also possible for malware installed on a computer to collect passwords, or for criminals to attack devices where default admin passwords are still in use.

# **Protect your credentials**

* Install updated antivirus software on your devices and update your software when prompted to do so.
* Set your antivirus program to scan your computer automatically, including a scan of all incoming emails.
* Don’t open unsolicited emails or attachments that come from addresses you don’t recognise or are not expecting.
* Support colleagues by reporting suspicious emails to [Action Fraud](https://www.actionfraud.police.uk/) / [NCSC](https://www.ncsc.gov.uk/information/report-suspicious-emails)
* Look closely at website addresses and ensure the address bar has a padlock, before entering any sensitive data. Consider manually typing addresses, rather than clicking on links.

# **Resolve the Account Compromise**

#### **Reset the user password**

Ensure that new passwords are not sent to an email account which has been compromised.

Make sure that there is a requirement to reset default passwords and refer users to the [NCSC password guidance](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email) on ‘**Three Random Words’** for strength and complexity, as well as referring to the school’s own Acceptable Use Policy.

#### **Check email forwarding addressees**

Open the email admin centre and find the relevant user account. Select and edit email forwarding to check and remove suspicious forwarding addresses.

#### **Check inbox rules**

Once the user is signed in, click the **settings** (gear/cog) icon and select **mail. Review** the **inbox rules d**isable or delete suspicious rules

#### **Check for signature changes and out of office replies**

Users should check for changes to email signatures as attackers can place malicious links in signatures and out of office replies.

Mailboxes which have been used to send spam email may have been blocked by the system. Once compromises have been resolved, the user may need to be unblocked.

# **Strengthen Your Credentials**

Laptops, computers, tablets, and smartphones may contain critical data - the personal information of staff / students, and also details of the online accounts that are accessed. It is essential that this data is available to you, but not available to unauthorised users.

## **Do Not Share Passwords**

IT systems should **not**require staff to share accounts or passwords to get their job done. Every user should have personal access to the right systems, at the right level of access (the lowest needed to do their job) to minimise the chance of unnecessary exposure.

Acceptable user policies should include the need to keep passwords private.

## **Do not save passwords on shared devices**

Passwords - when implemented correctly - are a free, easy, and effective way to prevent unauthorised users accessing your devices. When passwords are saved on shared devices, other users can use them to gain systems they are not authorised to use.

## **Switch on Password Protection**

Set a screen-lock password, PIN, or other authentication method (such as fingerprint or face unlock). Passwords should be easy to remember, but hard for somebody else to guess. The NCSC has some useful advice on [choosing a password using three random words.](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email)

If you’re mostly using fingerprint or face unlock, you’ll be entering a password less often, so consider setting up a long password that’s difficult to guess. Use capitals, alpha numeric, and special characters – be creative!

## **Change Default Passwords**

Change **all**default passwords before devices are distributed to staff. You should also regularly check devices (and software) specifically to detect unchanged default passwords.

## **Use Two-Factor Authentication for Important / Sensitive Accounts**

If you’re given the option to use [two-factor authentication](https://www.ncsc.gov.uk/cyberaware/home#section_4) (also known as 2FA) for any of your accounts, you should do; it adds a large amount of security for not much extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

## **Password Management**

If you're in charge of how passwords are used in your organisation, there are several things you can do that will improve security. Most importantly, your staff will have dozens of non-work-related passwords to remember as well, so only enforce password access to a service if you really need to.

Where you do use passwords to access a service, onlyenforce periodic and not regular password changes. Passwords only need to be changed when you suspect a compromise of the login credentials, but a periodic change is still considered good practice.

Staff will forget passwords, so make sure they can reset their own passwords easily.

Password managers are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all your other passwords, make sure it’s a strong one or use fingerprint / facial recognition.