JCQ CIC

Joint Council for Qualifications CIC

Guidance for centres on cyber security

Effective from November 2023

Produced on behalf of:

AQA Questions matter
cea Rewarding Learning
City & Guilds
NCFE
OCR Oxford Cambridge and RSA
Pearson
wjec cbac

Introduction

Awarding bodies are committed to maintaining the highest standards of cyber security to safeguard sensitive information provided by centres, including personal student data, and to protect the integrity of secure assessments. Centres and centre staff have a critical role to play in maintaining and improving cyber security.

In today's digital landscape, it is crucial that centres adhere to industry best practices to mitigate the risk of cyber threats. This document provides key guidelines that align with industry standards to help centres and centre staff protect their digital assets.

Account management best practices

The following are some essential guidelines for managing user accounts securely. This guidance should be followed for all awarding body user/email accounts that are used to provide or manage access to awarding body systems, information or data. By following these best practices, centres and centre staff can significantly reduce the risk of unauthorised access and protect sensitive information and other valuable assets.

Create strong unique passwords

- Use a password creation approach such as **three random words** to generate suitably secure passwords.

  Research shows that password length is a more valuable defence than complexity.

- Never use easily guessable information such as birthdays, singular names or common words for a password.

  Attackers can easily discover these and will frequently try to find out this sort of information.

- Always use a strong unique password for every account used and never use the same password across any other account.

  When passwords are reused, a single account breach puts all accounts with the same shared password at immediate risk. Attackers frequently use breached email and password lists to try to gain access to other services.

Keep all account details secret

- Never share login/password details or additional factor/authentication codes with anyone else.

  Attackers will often try to trick people into sharing those details with them by pretending to be from their awarding body, a technical support team or other organisation.

- Each person who needs access to a system should request their own user account and never share an account assigned for their use with anyone else.

  Remember that anything done with an account assigned to someone will be attributed to that person in the first instance.

Enable additional security settings wherever possible

- Activate two-step verification (2SV)/two-factor verification (2FA) or multi-factor authentication (MFA) wherever available. Doing this adds a layer of account security that requires users to take an additional action or to provide an additional verification such as a fingerprint, code, or confirmation via an authentication app.

  2SV/2FA /MFA only helps to protect users if the extra steps/factors are protected. Attackers will try to trick users into granting access/sharing codes, so these factors need to be kept as securely as passwords.

Update any passwords that may have been exposed

- If it is believed passwords may have been exposed/become known to others, they should be changed as soon as possible. The new passwords should not be shared with anyone.

- When changing passwords, strong unique passwords (e.g. **three random words**) should always be used. Old passwords should not be reused nor should cycling through a small set of passwords across multiple accounts be used.

  When passwords are reused, or follow a discernible pattern, attackers have tools that will help them to identify such password reuse/cycling patterns.

Set up secure account recovery options

- Updated account recovery options such as alternate email accounts or phone numbers should be set up or kept to facilitate access to accounts in case of a lockout or compromise.

  Attackers will try to use account recovery options (e.g. another email account specified as the recovery account) to take over an account, so wherever possible 2SV/2FA/MFA security should be enabled on all such accounts to ensure they remain secure from hackers.

Review and manage connected applications

- Regularly review and remove access for third-party applications or services that no longer require access to accounts.

  Attackers can breach services that users have been given access to and then use that access to attempt to access the user's accounts. Access should only be provided to trusted services. Centre staff should be particularly cautious when interacting with content and services (e.g. quizzes, prize draws, surveys etc.) on social media platforms as these are often used by attackers to access user information.

- Be cautious when granting permissions to applications and grant only the necessary access required for them to function.

  This is particularly relevant where apps ask for permissions that don't seem to make sense given the nature of the app. For example, a Word Search app that wants access to a user's contacts and be able to send SMS messages should be regarded with suspicion. Only download and install applications with established reputations from trusted sources.

- Passwords should not be saved to local web browsers. This is particularly important where there is shared access to a device or web browser. An exception to this is where a secure password manager extension is used in a browser that requires unlocking (e.g. with another password) before the saved account details can be retrieved, however care should be taken to ensure that this is locked/signed out of after use.

- Saving account details (usernames/passwords) on local web browsers that anyone using that browser can then access weakens account security. Enabling additional security controls on accounts such as 2SV/2FV/MFA or using a secure password manager can prevent others from accessing accounts in such circumstances.

- When using a shared browser, browser history and caches should be cleared out after use. The use of private browsing functions to reduce the usage trail left on any such browser should also be considered.

Stay alert for all types of social engineering/phishing attempts

- Care should be taken if unsolicited or unexpected emails, instant messages, or phone calls are received asking for account credentials or personal or confidential information. Passwords and 2FA/MFA authentication codes should not be given out to anyone.

  Attackers will often try to 'hack the human' first as it's cheaper and quicker for them than a technical attack. Centre staff should develop a healthy wariness of anyone or anything that seems to want to gain their trust, rush them into doing something or that just seems off. If in doubt, hang up/don't reply and don't click on links or take any action and check with a trusted party via a secure channel (i.e. call awarding body customer services via a known support number).

- Users should never approve or authenticate a login request that they did not initiate.

  Attackers who obtain a username and password will try to get the user to share any 2FA/MFA code with them or to approve the login request via some other means. They may try to convince the user that they need to confirm their identity and will send a secret code that the user needs to read out to them or ask for approval of a request they send in an authenticator app. In reality they are attempting to login to the account, are triggering the 2FA/MFA challenge and are trying to trick the user into giving them that code or approving access. Requests to share codes/approve logins should not be approved and requests to do so should be treated with a high degree of suspicion.

- Do not click on suspicious links, download attachments or scan QR codes from unknown sources.

  QR codes are easy for attackers to generate and are being increasingly used in phishing attacks. Caution is needed when scanning a QR code and wherever possible a secure QR code scanner with a good reputation should be used to help gauge whether a QR code is suspicious or malicious.

- Verify the authenticity of any communication by contacting the organisation directly through official known channels.

  Be wary of unsolicited inbound phone calls even where the caller's number appears genuine. Attackers will sometimes use number 'spoofing' services that mask their real number and make it look like the call is from a genuine trusted number. If in doubt, hang up and call back via a known trusted number.

- Report any phishing attempts which reference awarding bodies/their systems to the awarding body concerned immediately.

  JCQ and awarding bodies can send out communications to centres where notable attacks are observed, but rely on centres and centre staff to flag notable attacks to them. Any such attempts should be reported to awarding bodies.

Monitor accounts and review account access regularly

- Centre staff accounts should be routinely reviewed for any suspicious, unusual or unauthorised activity.

  If any suspicious, unusual or potentially unauthorised activity on awarding body systems is observed this should be immediately reported to the relevant awarding body, particularly if is believed that user account security may have been compromised.

- Ensure user access is reviewed promptly for staff who have left the centre.

  Leaving ex-employee access in place increases the danger of inappropriate/unlawful access to systems and data.

- Review levels of access regularly to ensure accounts have the minimum level of access required for their current role.

  Over-privileged accounts present an increased risk should an attacker gain access to the centre's systems. It might seem easier to give staff access to everything, but if an attacker gets into a user account, they will also have access to everything!

Cyber security best practice

Centres should stay informed about the latest security threats and trends in account security and educate staff on how to identify phishing attempts, secure devices and protect systems and data.

The National Cyber Security Centre (NCSC) provides excellent and comprehensive **cyber security advice for schools** that are relevant for all centres – the key points from this have been included in the previous section.

The NCSC advice and guidance should be observed for any IT systems used within a centre, particularly those where learner information, learner work or assessment records are held. Doing so can prevent adverse effects to staff and learners in the event of a cyber attack.

Other topics covered by the NCSC training and guidance include:

- Establishing a robust password policy
- Enabling multi-factor authentication (MFA)
- Keeping software and systems up to date
- Implementing network security measures
- Conducting regular data backups
- Educating employees on security awareness
- Developing and testing an incident response plan
- Regularly assessing and auditing security controls

By adopting these industry standard cyber security best practices, centres can significantly reduce the risk of cyber attacks and protect their valuable data and assets.

If centres experience a cyber attack which impacts any learner data, assessment records or learner work, contact with their awarding body should be made immediately for advice and support.