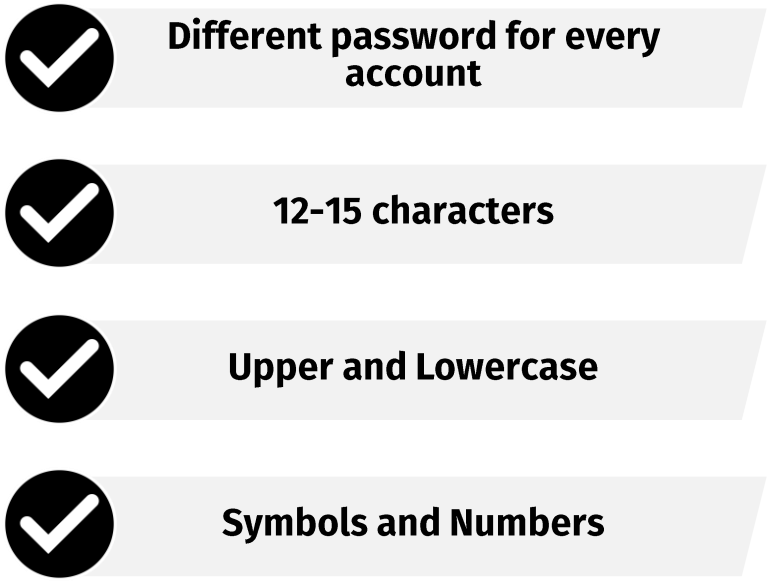
Digital security overview

August 2020

Basic password hygiene

- Your passwords are the first line of defence against many internet ills so think of the following suggestions as **essentials**!
  - Use a password manager – a good password manager creates strong, unique passwords for all your accounts – that means if one password is breached, the others remain secure
  - Go long – the longer and more complex your password, the less likely it is to be hacked (at least 12-15 characters)
  - Keep your unique characters separated in your password (e.g. *JJ3@gft()96* as opposed to *Sport2017*)
  - Don't reuse passwords across all your accounts
  - Don't trust your browser – while it's convenient to store passwords in your browser, the underpinning security behind those prompts is often undocumented so you're not sure how safe your password is
  - Add two-factor authentication (2FA) for all of your logins – either through a code sent to your phone or through an authenticator like Google Authenticator

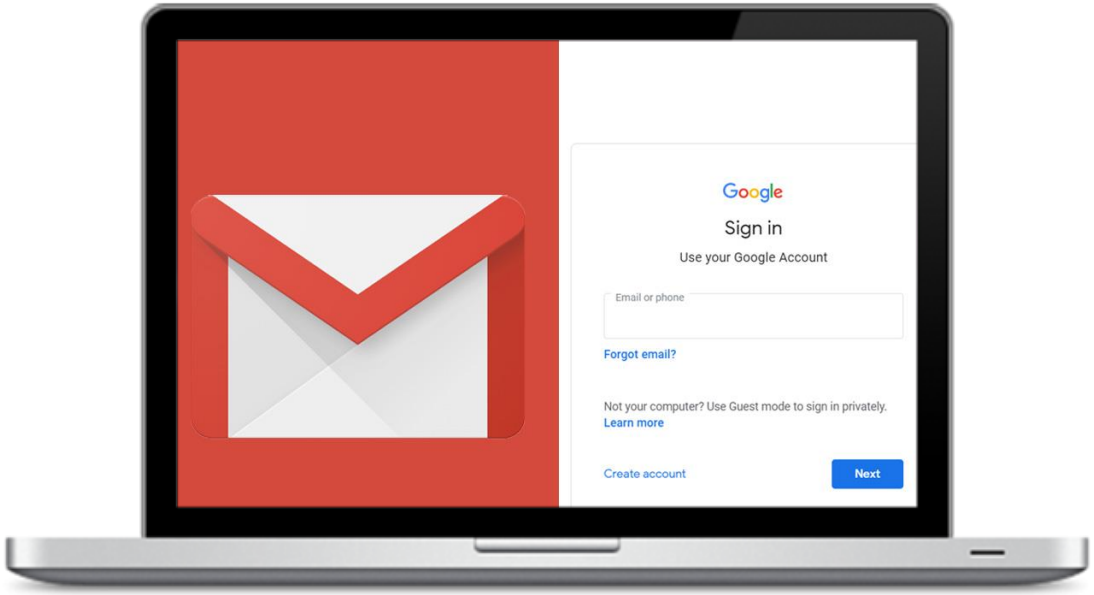


Protect your devices

- Athletes should keep all their devices (phones, computers, tablets etc) secure, whether they are being used personally or professionally
- This can be done by:
  - Keeping all devices password protected
  - Using and upgrading antivirus software
  - Ensuring that they do not leave their devices exposed or unattended
  - Installing all security updates for browsers and systems monthly or as soon as updates are available
  - Log into accounts and systems through secure and private networks only

Keeping emails safe

- Emails often host scams and malicious software – to avoid virus infection or data theft, employees should:
  - Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “click here for fun!”)
  - Be suspicious of clickbait titles (e.g. offering prizes/advice)
  - Check email and names of people they have received emails from to ensure they are legitimate
  - Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive exclamation marks)



Additional cybersecurity procedures

- Turn on two-factor authentication (2FA)
  - It is recommended that athleties have 2FA enabled on their email accounts and any additional platforms they use (including social media)
  - This is an extra security step which requires people to input a six-digit code which is sent to them via text message or generated
  - 2FA can be turned on within the apps or via browser

- **Revoke access to unued third-party apps**
  - It Is good practice to regularly check which third-party apps are connected to your social media accounts. Remove any which you do not recognise or those from apps which you no longer use
  - Following a hack or attempted hack it is advisable to revoke access to **all** third-party apps and add them again on a case-by-case basis if required