- Be very wary of unexpected emails, even from people you know.
- Do not click on links in emails. A link may look reasonable but where you go if you click may be completely different. If you really want to follow a link take a note of it and type it into a browser.
- If you get a request from a relative or friend saying they have lost their phone or changed their number and need help, the chances are it's a scam. If you really want to check it out, try using methods not suggested by the email or message itself.
- You will never have won a competition you didn't enter.
- The police will never request you to help solve a fraud by performing a bank transaction.
- Be wary of sharing information such as birth date, first school, pet, birthplace etc since these are often used to verify your identity.
- Have you received a call, text message or email from someone pretending to be in a position of authority asking you to buy gift cards?
  This may be someone claiming to be from American Express, your Bank, your boss or CEO, the HMRC or even the police.
  If so, this is likely to be a SCAM.
- You can alter your email to signal who is contacting you. E.g. if my email is johnsmith@gmail.com I can give it to a website or query as johnsmith+boots@gmail.com and when it is used I can tell it's Boots contacting me, or someone Boots has shared my email with. This method can also be used to filter out emails you don't want to receive. The emails will come to the base address but you can see it is addressed to the new one.