



The PC Wizard, ...for all your computer's needs

JOB SCAMS

What should I look out for / How do I check to see if it is a scam?

1. Did you apply for the job or did the company contact you directly by email? Very few genuine UK companies would offer a job by email. Genuine companies have a rigorous selection procedure, which would normally involve a face-to-face interview.
2. Check the web address for the company on Google. E.g. www.companyname.com
 - a. Does the company / website exist?
 - b. Does the website look professional?
 - c. Is the company advertising the proposed job on their website?
 - d. Does the email address given match that on the website or is there a difference?
E.g. thepersonsname@companyname.com or is it more like – thepersonsname.companyname@yahoo.com (A lot of scammers will use a web based email hosting account such as yahoo or google mail etc)
 - e. Do the contact details on the website match those in the email or have they changed the telephone contact numbers?
3. Genuine UK companies are registered and can be checked on www.companieshouse.gov.uk
4. Does the job offer sound too good to be true.... Then it **probably** is!!
5. Do they state in the email that you must use their contact within a law firm, agency or British Embassy/High Commission? If so, do they give the full contact details including name, position, address and telephone numbers in the email?
 - a. YES – Check them.
 - b. NO - BE SUSPICIOUS!!
6. Some job scams fraudulently use the names and job titles of genuine High Commission staff. A genuine email from an official member of staff will always be from our official service provider - @fco.gov.uk
7. Neither the British High Commission nor any of its staff would ever ask you for payment of fees directly. There are no “additional visa fees”.
8. The UK government does not administer or charge for “additional services” such as Travel Insurance, Health Screening checks, Police checks, Home Land Security checks, etc. Any such charges are indicators of likely fraud



The PC Wizard, ...for all your computer's needs

JOB SCAMS

Where can I go for advice on Internet Email Scams or on-line fraud?

There are various websites that give advice on Scams and Fraud and how to protect yourself from them. These include:

Press CTRL and click on the logo



Call
0300
123 2040

Action Fraud is the place for you to find out about fraud. We're the UK's national fraud reporting centre.



Get Safe Online

Get Safe Online; a joint initiative between the Government, law enforcement, leading businesses and the public sector. Our aim is to provide computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely and securely.



Stay Safe Online.org - The National Cyber Security Alliance website giving advice on protecting yourself from online fraud.

How can I protect myself online from on Internet Email Scams or online fraud?

1. Ensure that you have good security protection on your computer / laptop or Macintosh. This should include the minimum of a firewall and antivirus products.
2. If you use web based email (e.g. Yahoo, Google etc), ensure that the Junk Mail option is used as this will filter out a lot of the scam emails. If you receive a mail that you believe to be junk, classify it as a junk email.
3. If you use Outlook or other proprietary email software, ensure that you have adequate spam filtering or additional software to do this.
4. Do not open attachments in emails unless you know where they have been sent from. For additional security, it is recommended to download the attachment to the computer / laptop or Macintosh and then scan it with an antivirus product to ensure that there is no malware attached.



The PC Wizard, ...for all your computer's needs

JOB SCAMS

There are numerous companies that offer software solutions to assist in the security of online protection from online fraud / email scams etc.

Reputable companies recommended by the UK and US banking and financial sectors include (**):

Press CTRL and click on the logo



Trusteer is the world's leading provider of secure browsing services. We keep criminals away from the browser and prevent the theft of any personally identifiable information.



Prevx SafeOnline secures your private information while you bank or shop online - better defending you against internet fraud caused by PC infections.



Comodo AntiSpam easily integrates into your email system to block spam and junk mail without keeping wanted mail from reaching your inbox.

** Please note: The FCO do not personally endorse any of the above products

What should I do if I have received a scam email?

1. You should not pay any money.
2. You should not have any further contact with them. It might be tempting to enter in to a dialogue with these people, however you should not. These people are professional criminals, they will seek to exploit you. Even if you do not pay them any money, they might seek to steal or abuse your identity. Your best defence against these people is to ignore them and delete any emails that you have received from them.



The PC Wizard, ...for all your computer's needs

JOB SCAMS

What if I have already paid money to an scam email?

1. You should report the matter to the Police Authorities, who will investigate your complaint.
2. This is an international crime – investigations must be progressed through the Police and then Interpol.
3. The UK police cannot become involved until they have been contacted by Interpol.

Other scams – lottery scams?

All genuine UK lotteries are registered and have websites

If you did not buy a ticket, you cannot win a lottery

UK lotteries do not email winners or refer to amounts won

Further advice on lottery-related frauds is available from the Gambling Commission:

log on to www.gamblingcommission.gov.uk.