With so many people looking for work – and so much being advertised – you need to be sure you're applying for a genuine job.

Don't fall victim to an employment scam.

GET SAFE ONLINE.org®

www.getsafeonline.org

Royal Gibraltar POLICE

Like many other aspects of life, the job market has been turned upside down by the COVID-19 pandemic, with a succession of business closures, redundancies and migrant workers returning home.

Now, with restrictions easing and life returning to normal, the employment market is becoming busier with many more jobs being advertised – mainly online – and huge numbers of applications for each role.

Employment scams have always been commonplace, ranging from being charged for nonexistent DBS or CV checks to money laundering.

But the current situation is being heavily exploited by cybercriminals, with 74% of job seekers applying for jobs that weren't genuine during the pandemic*. Fall for one, and you could become a victim of financial or identity fraud, or even unwittingly pick up a criminal record. Read our expert tips, and don't let this happen to you.

*Disclosure & Barring Service / JobsAware

#safejobhunting

Your top tips for safe job searching

- **Do thorough research** to ensure job sites, employment agencies and prospective employers are reputable with a physical address and landline phone number.

- When listing your profile, select the option of keeping it public, confidential or private according to your needs.

- Never divulge information such as NI, passport or driver's licence numbers, bank account/payment card information or date of birth, either typed on your CV or application, or in photos/scans. This could lead to identity theft. Supply these only when you've met the employer, landed the job and are satisfied that everything is legitimate.

- Devise and use strong passwords, keep them protected and don't use them on more than one online account or other website. Please read our advice on the Get Safe Online website about how to devise strong passwords and keep them protected.

- If you receive an email claiming to be from a potential employer who has seen your CV on a job site, take care when clicking on links and ensure they lead to a legitimate job posting.

- Don't call advertisers for telephone interviews, it could be an expensive premium rate number. Instead, make sure prospective employers call you.

- Be wary of jobs that offer income for very little work or seems too high to be true, don't need any experience or press you to apply immediately. These could involve you in money laundering or muling.

- Bear in mind that many fraudulent job ads can be found on social media sites.

- Be wary of requests for up-front payment for CV services, DBS or other security checks or headshots.

- Don't conduct the entire process via website, email, text or messaging: most genuine employers will require a face-to-face (or video) interview and that way, you can check them out too.

- Ensure that potential employers are genuine before meeting for a face-to-face interview, to ensure that your personal safety isn't at risk.

If you've been the victim of a recruitment scam, report it to **SAFERjobs** at **www.safer-jobs.com**

If you think you've been a victim of online fraud, contact your bank and then report it to the Royal Gibraltar Police via the dedicated web portal at **www.police.gi/report-online** or by telephone on **+350 20072500**.

For comprehensive, practical, impartial advice on safe job searching online, visit www.getsafeonline.org/personal/articles/job-searching

SEND YOUR CV

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, contact your bank and then report it to the Royal Gibraltar Police via the dedicated web portal at **www.police.gi/report-online** or by telephone on **+350 20072500**.

www.getsafeonline.org

Royal Gibraltar
POLICE