Cyber Byte

March 2026.

Applicant Beware - Who Is Recruiting You?

When an unsolicited email arrives in your inbox, you are more likely to be suspicious as it can bear the hallmarks of a scam: Urgency, High reward, too good to be true…

Cyber criminals, as we know, use a variety of methods to steal information, so it is important we keep our guard up against scams.

But have you considered scams offering fake job roles? Scammers create these attempting to steal personal information, and may even use Messenger, WhatsApp, and social media to advertise the scam.

These can look very convincing, offering a high salary, generous bonuses, work anytime, from anywhere, with minimal effort required inducements. All the too good to be true incentives, as they attempt to hook you to reply to them.

A method deployed at scale is the use of online job platforms to attract applicants who may, have direct or indirect access to privileged information or have shared too much personal or business information in that extra effort to be noticed.

Our colleagues at the NPSA (National Protective Authority) have created excellent guidance to improve situational awareness of this type of scam and we encourage you to review it.

This guidance helps you to recognise suspicious adverts, along with scam recruiter behaviours, to help understand how you can protect yourself, and your organisation, reporting concerns and ceasing engagement if something does not look right.

Our colleagues at Take Five have excellent resources to additionally improve awareness and support your response in relation to identifying and dealing with online scams.

It is important to remain sceptical of unsolicited job offers and if something feels too good to be true, trust your instincts.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.