Take 5 To prepare

NHS East of England Ambulance Service NHS Trust

Resilience and specialist operations team briefing note:

Think Before you Link

Hostile actors and criminals are known to be using professional networking sites and social media platforms to approach UK and Western nationals working in sensitive employment across government, the private sector, the public sector, academia and think tanks. These malicious actors piece together information from multiple sources to draw meaning from their intelligence gathering.

Their end goal is to recruit UK and Western nationals to provide them with sensitive intelligence, willingly or unwittingly. In these cases, individuals may not recognise that the information they are providing is sensitive (e.g. they may be asked seemingly benign questions).

Who are they targeting?
Individuals are particularly vulnerable to approaches if they include the following details on their profile:

- Identifying as an employee or member of HMG or Civil Service
- Identifying as working in the private sector or academia, with access to classified or commercially sensitive technology or research either directly or indirectly (e.g. the defence industry)
- Mentioning that they have security clearances, especially security cleared (SC) or developed vetting (DV)

How do they trick you?
Typically, hostile actors and criminals contact the target posing as an interested 'employer' or recruitment consultant presenting a unique business opportunity. They ask for further details about the target's background, try to 'sell' the business opportunity, and insist on discussing it privately, away from the initial website. This kind of engagement is an attempt to understand the level of access the individual has to sensitive information, draw it out from them, and build a longer-term relationship.

Watch the Think Before you Link video

Recognise
the profile?

Realise
the potential threat

Report
to your Security Manager

Remove
them from your network

#WeAreEEAST

Case Study: Matthew

Background:

Matthew was a DV-cleared UK civil servant working overseas. His professional networking profile included his e-mail address and his employment history. This employment history mentioned his previous area of expertise in government which, **by association, indicated that Matthew held sensitive security clearance**.

Digital Footprint
Think carefully about the information you display publicly online as this can make you a target for malicious profiles.

The approach:

Matthew was approached on the networking site by an individual, allegedly called Helen, who claimed to work for a think tank with a business proposition. Matthew had not heard of the think tank or the recruiter before which felt a little unusual to him. However, after checking their shared contacts he found that they had a **friend in common and therefore assumed the profile must be genuine**. Matthew explained away his doubts and decided to accept the connection.

Common Contact
Don't assume that people in your network have checked out their contacts. Just because you have a mutual contact does not mean the profile is always genuine.

The recruiter quickly contacted Matthew directly, **flattering his skillset** and outlining an attractive consultancy opportunity.

Flattery
Malicious profiles use flattery to establish contacts and keep targets engaged. Be sceptical until you get some signs that the profile is genuine.

The offer was **vague and did not include specific details** of the role. Matthew was not entirely clear what this consultancy opportunity would entail but presumed that the think tank would not disclose this information until they had interviewed him. When he asked for specifics, the recruiter explained the need to retain client confidentiality and Matthew felt satisfied by this. Having worked in the Civil Service, Matthew thought this demonstrated a level of discretion and professionalism.

Lack of Detail
Malicious profiles use vague language to describe their business opportunities. If no specifics are forthcoming you should be very suspicious.

Engagement:

After exchanging a number of messages over a period of approximately one month, the recruiter suggested moving to personal emails. Contact became more frequent, which seemed a little persistent but Matthew felt flattered by their interest in him. Matthew was more focused on the offer as it seemed like the perfect job opportunity.

The so-called recruiter and Matthew discussed recent international events, with the recruiter seeking Matthew's opinion based on his skills and expertise. The recruiter had always seemed very informal and friendly in her messages.

Take 5 To prepare

NHS East of England Ambulance Service NHS Trust

Resilience and specialist operations team briefing note:

Outcome

Matthew wanted to appear respectful and polite in return so when the recruiter suggested a face-to-face meeting, he accepted. The two subsequently communicated by e-mail, instant message, and telephone call, as well as meeting on several occasions

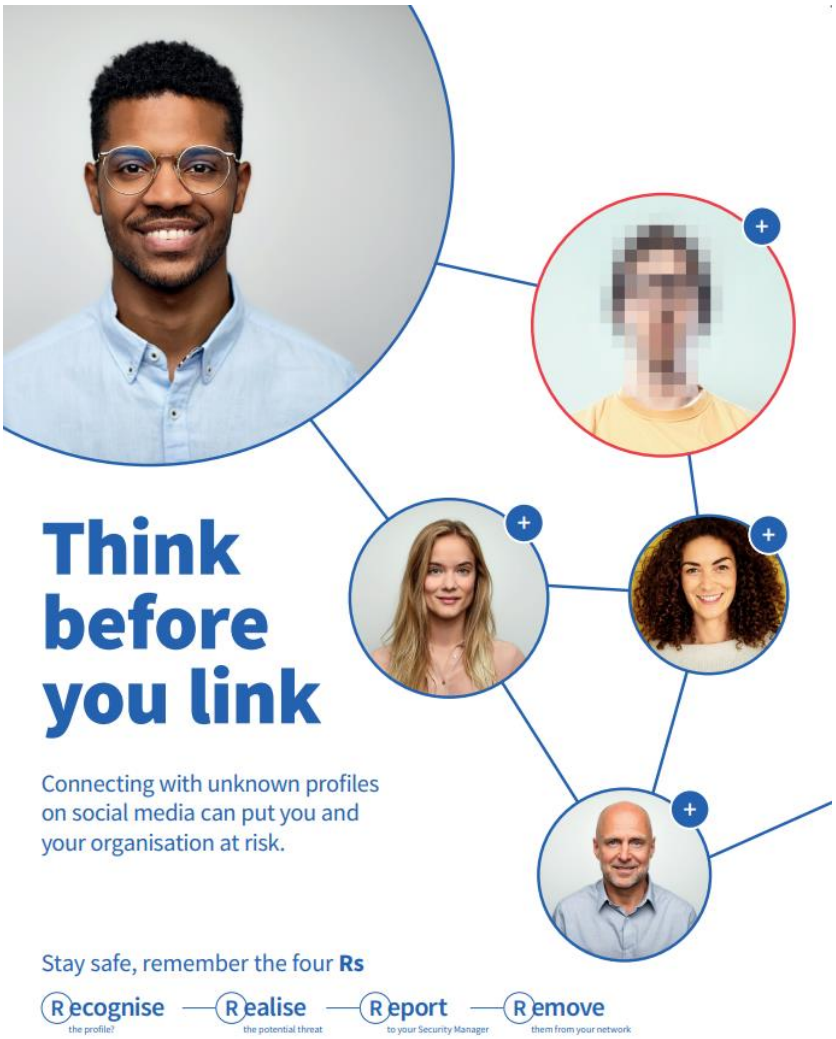
It was only when Matthew's brother questioned his interaction with the recruiter that Matthew became suspicious. His brother suggested the offer may be **'too good to be true'**. At this point Matthew broke contact with the recruiter. Despite these suspicions, Matthew did not mention the approach in his vetting renewal interview.

Too Good to be True

If you're approached with an opportunity that seems too good to be true, it probably is!

Reporting

If you've had a suspicious interaction online your organisation's security team may want to know about this. Reporting this activity helps protect yourself, your colleagues, and your organisation.



Watch the Think Before you Link video

#WeAreEEAST