# Security Guide for Individuals Likely to be Targeted by Foreign Intelligence Services in the UK

Generated by Grok 3

May 31, 2025

## 1 Introduction

Foreign Intelligence Services (FIS) target individuals in the UK to gather sensitive information, influence decisions, or undermine national security. High-risk groups include government officials, military personnel, scientists, business executives, journalists, activists, and tech professionals. This guide outlines resources and protective measures available to those likely to be targeted, drawing from UK security agencies such as MI5 and the National Protective Security Authority (NPSA).

## 2 Who is at Risk?

FIS target individuals with access to sensitive information or influence, including:

- **Government Officials**: Politicians, civil servants, or diplomats with access to policy or classified data.
- **Military Personnel**: Active or retired members with knowledge of defense strategies or technology.
- **Scientists/Researchers**: Those in fields like AI, biotech, or quantum computing.
- **Business Executives**: Leaders in tech, energy, telecom, or finance with proprietary data.
- **Journalists/Media Figures**: Individuals shaping public opinion or with insider access.
- **Activists/Dissidents**: Those critical of foreign regimes, especially from countries like China or Russia.
- **Tech Professionals**: Engineers or IT specialists with access to critical systems.

# 3 Common FIS Tactics

Understanding FIS methods helps in recognizing and countering threats:

- **Cyber Espionage**: Phishing, malware, or hacking to steal data.
- **Recruitment**: Offers of financial or material benefits to elicit information.
- **Elicitation**: Seemingly normal conversations to extract sensitive information.
- **Surveillance**: Monitoring online/offline activities, including through interpreters or compromised environments.
- **Intimidation**: Threats to dissidents or their families to suppress opposition.
- **Disinformation**: Spreading false information to influence or destabilize.

# 4 Resources and Protective Measures

The following resources and measures are available to help protect individuals from FIS targeting:

## 4.1 National Protective Security Authority (NPSA)

The NPSA, part of MI5, provides tailored security advice to businesses, organizations, and individuals at risk of espionage:

- **Security Guidance**: Advice on protecting sensitive information, including cyber, physical, and personnel security. Visit www.npsa.gov.uk for resources on countering espionage.
- **Cyber Security Tools**: Tools like the Cyber Security Toolkit for Businesses to secure digital assets.
- **Training Programs**: Workshops and online training to recognize and mitigate FIS approaches, especially for high-risk sectors like technology and academia.
- **Threat Awareness Briefings**: Regular updates on state threats, including specific FIS tactics.

## 4.2 MI5 and Counter-Espionage Support

MI5 works to disrupt FIS activities and offers support to potential targets:

- **Reporting Suspicious Activity**: Contact MI5 via www.mi5.gov.uk/contact-us to report suspected FIS approaches, such as unsolicited contacts or offers of gifts.

- **Protective Security Advice**: MI5 collaborates with police and organizations to alert individuals of potential recruitment attempts and provide advice on avoiding them.
- **Investigations**: MI5 investigates FIS activities under the National Security Act 2023, which criminalizes assisting FIS, including accepting material benefits without legitimate basis.

## 4.3 Foreign, Commonwealth & Development Office (FCDO)

For individuals traveling abroad, where FIS targeting risk increases:

- **Travel Advice**: FCDO provides country-specific guidance on over 200 destinations, including risks from FIS. Check www.gov.uk/foreign-travel-advice.
- **Embassy Support**: Contact UK embassies for assistance if targeted abroad. Find embassy details on the FCDO website.
- **Pre-Travel Briefings**: Guidance on securing devices and avoiding elicitation during travel.

## 4.4 Centre for the Protection of National Infrastructure (CPNI)

The CPNI, a child agency of MI5, supports critical national infrastructure but also offers resources for high-risk individuals:

- **Security Advice**: Integrated advice on protecting information, personnel, and physical assets. Visit www.cpni.gov.uk.
- **Industry-Specific Guidance**: Tailored for sectors like tech, energy, and academia, which are frequent FIS targets.

## 4.5 Law Enforcement and Legal Protections

- **Police Support**: Work with local police or Counter Terrorism Policing to report FIS-related crimes. Contact via www.police.uk or 101.
- **National Security Act 2023**: Provides legal recourse for prosecuting FIS-related offenses, such as accepting illicit payments or engaging in harmful conduct.
- **Investigatory Powers Commissioner's Office (IPCO)**: Oversees MI5's use of intrusive methods (e.g., surveillance) to ensure compliance with laws like the Regulation of Investigatory Powers Act 2000.

## 4.6 Additional Resources

- **GOV.UK**: Centralized access to government services and security advice at www.gov.uk.

- **Investigatory Powers Tribunal (IPT)**: For complaints against intelligence agencies, submit forms at www.ipt-uk.com.
- **US Embassy (for dual nationals or US-affiliated individuals)**: Contact for support if targeted by FIS, especially in Five Eyes contexts. See uk.usembassy.gov.

# 5 Practical Steps to Stay Safe

- **Be Vigilant**: Recognize suspicious contacts, especially unsolicited offers or overly curious inquiries about your work.
- **Secure Devices**: Use strong passwords, encryption, and avoid storing sensitive data on devices when traveling.
- **Limit Sensitive Discussions**: Avoid discussing work in unsecured environments, such as hotels or public spaces.
- **Report Incidents**: Immediately report suspected FIS approaches to your employer's security officer, MI5, or police.
- **Pre-Travel Precautions**: Attend briefings, secure devices, and avoid carrying sensitive materials abroad.
- **Post-Travel Debriefing**: Share unusual experiences with your organization's security team to enhance future protections.

# 6 Conclusion

Individuals likely to be targeted by FIS in the UK have access to robust resources through the NPSA, MI5, CPNI, FCDO, and law enforcement. By leveraging these tools, staying vigilant, and reporting suspicious activities, you can protect yourself and contribute to national security. For further information, visit the websites listed or contact relevant authorities promptly.