AirCyISOC
Air Cyber and Information Services Operations Centre

ROYAL AIR FORCE

Social engineering

Everyone's a target. Don't become a victim.

GET SAFE ONLINE .org

www.getsafeonline.org

What is social engineering?

Social engineering is the act of manipulating or deceiving somebody into a specific action with the intent of obtaining personal, financial or other confidential information. It plays on basic needs such as financial wellbeing, good health, being loved, wanting to please or legal compliance. Social engineering involves impersonating an organisation or individual who is trusted by the target, whether it's their bank, a government department, an IT support provider, a parcel delivery firm or someone they've met via online dating.

How is it perpetrated?

Social engineering can be carried out via emails, texts, direct messages, social media posts, phone calls and even face-to-face. Attacks can be simple as one text message directing the recipient to click on a link to what turns out to be a fraudulent but authentic-looking website, or more complex, committed using multiple co-ordinated approaches. You can encounter them in both your personal and work life.

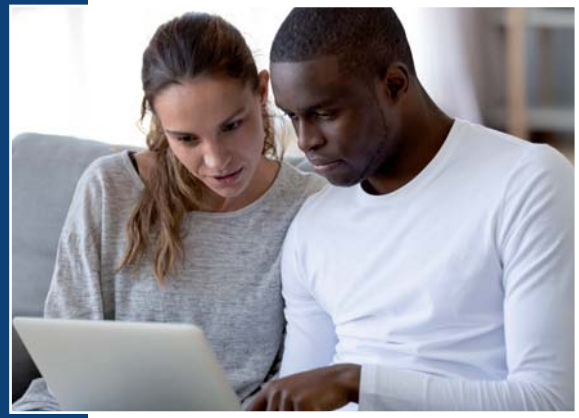
What's the objective?

Most social engineering attacks are perpetrated with the objective of committing financial fraud or identity theft. For RAF personnel and our families, however, there's another dimension: attempting to breach our systems to obtain classified information or commit sabotage, terrorism or other hostile acts.

ROYAL AIR FORCE

Top tips to avoid social engineering.

- Never give out personal or financial data including usernames, passwords, PINs, ID numbers or memorable phrases.
- Never provide details of colleagues, operations, deployments, locations or other classified information apart from via authorised secure comms.
- Be very careful that people or organisations who request payment card or other confidential information are genuine, and even then, never reveal passwords. A bank, HMRC, retailer or other reputable organisation won't ask you for your password or PIN via email, phone call or any other means.



- If you're in any doubt about the authenticity of a caller or what they're asking, end the call, then phone the organisation they claim to represent on the number you know to be correct (and not one the caller has provided). Always be safe … not sorry.
- Don't open email attachments from unknown sources as they could contain malware, including spyware or ransomware. Delete them, but first take the details to report if appropriate.
- Don't click on links in emails from senders you don't recognise. Instead, roll your mouse pointer or finger over the link to reveal the actual sender. If they're different, it's not authentic. Even emails that seem to come from someone you might know – but seem unusual – may be from a fraudster or hostile actor who has spoofed the sender address. If in doubt, call (but don't email) the sender on the number you know to be correct.
- Don't attach external storage devices like USB sticks or hard drives – or insert CD-ROMs/DVD-ROMs into your computer – if you're uncertain of the source. A tried and tested way for fraudsters to spread malware is to leave devices lying around in the certain knowledge that someone will connect them out of curiosity.

Reporting

If you suspect that a cyber incident or any other type of data or personnel compromise has occurred as a result of social engineering or any other threat vector, contact your Station Cyber Protect Team. If it is in the form of a fraudulent email to your MOD account, forward it as an attachment to SPOC-SPAM.

For comprehensive, practical, expert advice visit **www.getsafeonline.org**

#RAFsafeonline

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 a number of government departments, 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**

GET SAFE ONLINE .org

ROYAL AIR FORCE

www.getsafeonline.org

GET SAFE ONLINE: WORKING TOGETHER WITH...

TESCO · NatWest · Gumtree · Standard Life · first direct · HSBC · ROYAL AIR FORCE · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ClearScore · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT