INTRODUCTION TO SECURITY

CPNI

Centre for the Protection of National Infrastructure

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

WHY IS SECURITY IMPORTANT?

What are the most common security risks that your organisation faces daily? Would you challenge a stranger who's not displaying their security pass? What are the proper procedures for handling confidential data, or destroying sensitive documents?

We all aware that security is important, but creating a standardised security culture across the board – from administrative staff to senior executives – presents a particular challenge for organisations, both private and public.

Security breaches of any kind can result in loss of revenue, productivity or share price; they can damage an organisation's reputation; they might result in confidential data being leaked; or worse, they can result in physical harm to staff members or the public.

We all need to think and act in a security-conscious and collaborative manner, as well as to take personal responsibility for our actions, so that we can help prevent incidents and breaches from happening.

WHERE MIGHT THE SECURITY RISKS COME FROM?

Potential security risks can come from a range of sources. For example:

- A criminal
- A terrorist
- A violent activist
- A spy
- Or one of us, such as by accidentally disclosing sensitive material

There are various ways that individuals like these might try and cause harm to your organisation. These could be through cyber-attacks, physical acts of theft or sabotage, manipulation of you or your colleagues, or by other means.

To help us to stay safe and secure, we have developed some security campaigns to encourage you to adopt certain security behaviours. As part of these campaigns you will meet *four security agents* – characters that represent the different kinds of approaches that an employee might take when confronted with a security issue.

Find out more about these agents in the next section, and reveal the agent most like your personality by completing our quiz – '*What kind of security agent are you?*'

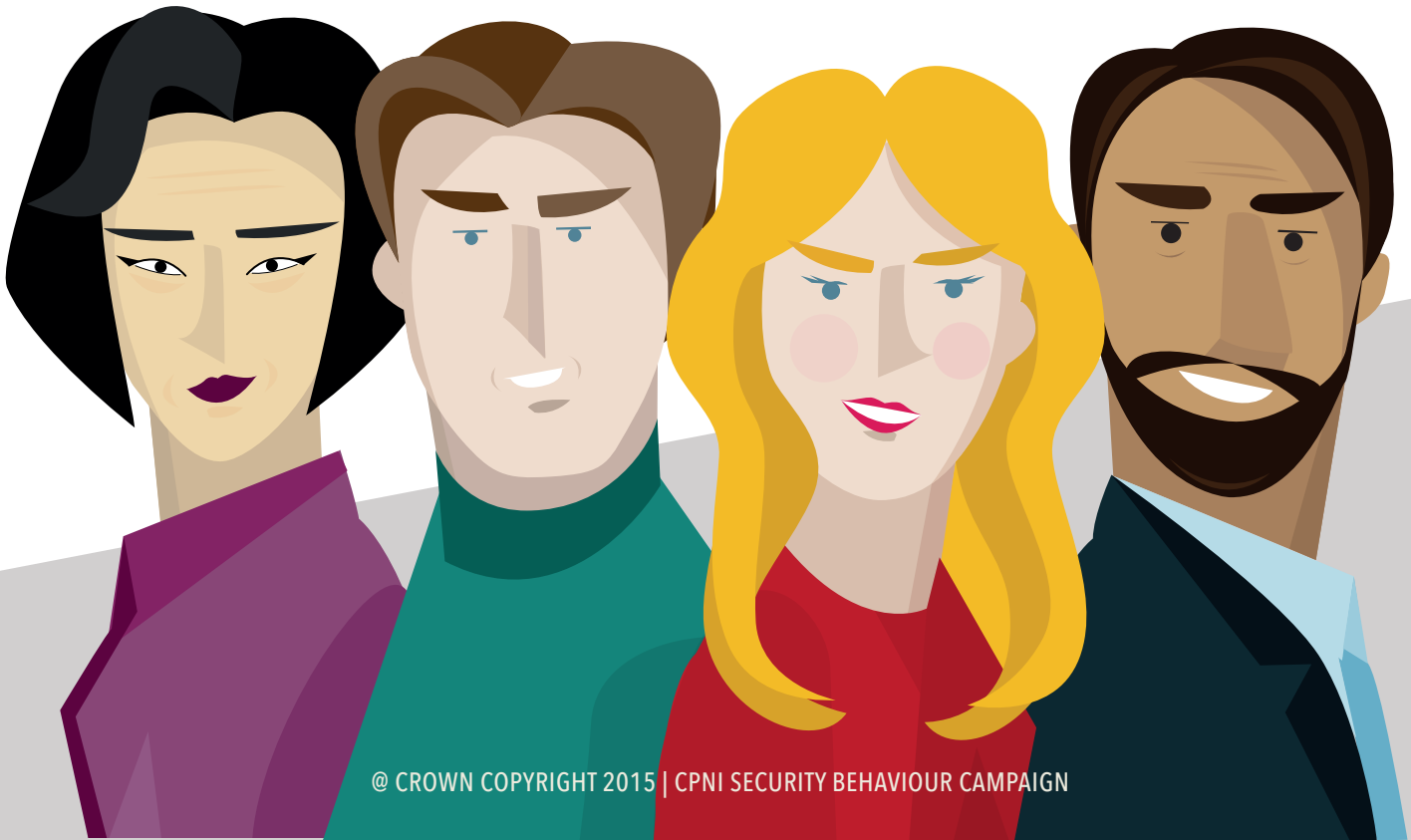
WHAT KIND OF SECURITY AGENT ARE YOU?

This is your mission, should you choose to accept it: Take the "What kind of security agent are you?" quiz.

Answer the following questions honestly to find out how you would react in certain everyday scenarios where your organisation's security could be at risk.

How you answer will determine your 'security agent' persona, i.e. the kind of security-conscious behaviour you tend to exhibit on a day-to-day basis in your workplace. The results will also give you an idea about some of the other security agent personas you may come across in the workplace, and help show how a team of colleagues can combine their strengths to work towards keeping an organisation secure.

So, have a go at the quiz and ask yourself: "What would I do?"



WHAT KIND OF SECURITY AGENT ARE YOU?

1. What would you do if you saw a colleague not wearing their security pass around the office?

A – Approach them immediately, point out that they're not wearing their pass and ask them to put it on. It is policy after all!

B – Ask the person if they have been issued with a security pass and either take them to be issued with one, or offer them a helpful tip so they don't forget to wear it again.

C – Check if they wear their pass tomorrow, this may have been just a temporary lapse. If it happens again, you may need to approach them or inform their manager.

D – Ask them if they're aware of the security pass policy, point them to where they can find a copy, and suggest they put on their pass as soon as possible.

2. What would you do if you saw a colleague rush off to an important meeting and leave their computer unlocked, or laptop open?

A – Stop them immediately and alert them to the fact they've left their computer unlocked, or laptop open.

B – Close or lock the device for them and leave them a note to say that you've done this.

C – Make note of the incident and let a line manager or colleague know if you see this happen repeatedly; it might be time for a policy reminder about locking computers/laptops.

D – Close or lock the device for them and then follow up with an email, explaining why it's important to lock one's computer and encouraging them to do so in the future.

WHAT KIND OF SECURITY AGENT ARE YOU?

3.What would you do if you overheard a discussion, which you knew to be about some highly sensitive and confidential information, being held in a corridor where external visitors often pass through?

A – Approach the individuals and ask them to stop the discussion immediately – they risk compromising the security of highly sensitive information.

B – Point out where the nearest vacant meeting room is and politely suggest they continue their conversation privately in there.

C – Not say anything at the time, but make a note of the individuals involved, what they discussed, before informing either your line manager, their line manager or a security representative.

D – Remind the individuals that visitors frequent the corridor and suggest they continue their discussion elsewhere or at another time.

4. You notice that some sensitive work documents have been left for all to see on top of the printers at the end of the day, when they should have been locked away for the night. What do you do?

A – Pick them up and confront the owner of the documents as soon as you can – their negligence could have caused a security breach.

B – Pick them up and either clear them away or destroy them appropriately – you're often the one tidying things up in the office when other people forget.

C – Pick them up and make your line manager or your local security representative aware – you've spotted a number of "near miss" security incidents lately and the office has become noticeably less security-focused.

D – Pick them up and then explain to the owner why the material must be kept secure. If the perpetrator cannot be identified, suggest to a line manager that a reminder is circulated to the department.

WHAT KIND OF SECURITY AGENT ARE YOU?

5. What would you do if you noticed a colleague had posted something on social media that related to a sensitive work project (i.e. information which you know should not be shared outside the organisation)?

A – Contact your colleague and inform them that they have breached security policy by disclosing information that isn't publically available, and request they delete the post immediately.

B – Look into whether you can delete, hide or amend the post yourself. Then contact your colleague to let them know the post has been amended, or that they need to take it down, and why.

C – Look elsewhere on the site to see if your colleague or others working on the project have disclosed further sensitive information. Then share your observations with your line manager or the project lead.

D – Speak to your colleague and explain what you saw, why the information poses a security risk to the organisation, and why it shouldn't be shared on social media.

6. You notice that a colleague is unusually quiet at work, and frequently ignores basic security procedures (e.g. they send sensitive information inappropriately to a supplier over email). What would you do?

A – Let your colleague know they've been breaking security protocol and brief them on how to handle sensitive information on email.

B – Check the current security policy to ensure your colleague is deviating from this. If so, send them and others concerned a reminder of the policy. Offer to help if they are unclear what to do with certain information.

C – Keep an eye on your colleague and share your observations about their change in character and recent security lapses with a line manager. Together you can discuss a way forward.

D – Invite your colleague for an informal catch-up to ask how they are. Use this as an opportunity to also tactfully let them know that you've noticed they're not following security policy, and remind them that it's important to do so.

WHAT KIND OF SECURITY AGENT ARE YOU?

7. What would you do if you saw an important-looking visitor walking around the workplace unescorted, without a pass?

A – Approach the visitor immediately and let them know that they can't be unescorted in the office. Then, follow up with the member of staff responsible for the visitor to inform them that leaving any visitor (however important) unescorted and without a pass is in breach of security policy.

B – Approach the visitor, find out where they are going, then either escort them there or stay with them until the member of staff responsible for the visitor re-appears.

C – Keep an eye on the visitor and their movements, all the while asking around the office which of your colleagues or managers is responsible for them.

D – Ask the visitor who in your organisation they are here to see and whether they have been issued a security pass. Then, liaise with the person responsible and after the visitor has left, tactfully remind them why their actions could cause a security breach.

IF YOU ANSWERED MOSTLY...

A – YOU ARE AN ENFORCER

You know what the security policy is and have no trouble approaching and confronting someone who isn't following the rules. You are firm, but fair, and believe strongly in the need for everyone in the organisation to adhere to the security policy to help keep you all safe and secure.

While some of your colleagues may feel a bit uncomfortable stopping someone in the corridor, for example, to ask them to wear their security pass, you are happy to handle any type of confrontation regarding security. You offer a valuable helping hand to others such as Observers, who are good at spotting security breaches, but would rather not confront others about the matter themselves.

However, there may be times when your approach requires a softer touch, perhaps in the case that a VIP visits your offices and is seen to disobey a fundamental security rule; they need a reminder, but might take issue with being told what to do. In these situations, call upon one of your colleagues – a Diplomat perhaps – to lead the discussion, with your support. Your firmer approach may still be required if the person continues to demonstrate inappropriate security behaviour.

B – YOU ARE A FIXER

You're someone who takes it upon themselves to sort stuff out, whether you're responsible for it or not. You are the organisational backbone within your team or department, in most instances, but especially when it comes to behaving in a security-conscious way.

You're always the person that finds they're clearing away confidential material left lying around. This frustrates you, as you think about all those times when you're not in the office to cover everyone else. You're also often the one that has practical ideas for how to resolve a security matter or prevent breaches from reoccurring.

You need to make a stern point about the security lapses taking place in your work area, but you're not fond of confrontation. You might want to let an Enforcer or Diplomat help you get your point across.

IF YOU ANSWERED MOSTLY...

C – YOU ARE AN OBSERVER

You have eyes in the back of your head and are forever curious. When something doesn't look right or someone's behaving abnormally, you're the first to ask questions or follow the situation more closely.

Others are often interested to hear about your comments and thoughts regarding security in the workplace because you notice when and how often security policy is being flouted. You're not perhaps the most vocal person, but you inspire hushed confidence in everybody around you.

When you do spot a trend in security lapses, you might want to call upon a Fixer to help you implement a plan, or an Enforcer or Diplomat to ensure staff members are made fully aware of proper security policy.

And let's face it, once you do, you'll be quietly checking back to make sure they follow it.

D – YOU ARE A DIPLOMAT

You are a natural collaborator that uses charm and wit to encourage colleagues to work together, without being imposing or forthright. You have a very pleasant manner with your contemporaries and can explain the benefits of following the security policies in place, 'bringing people with you' using your warmth and diplomacy. You are also skilled in winning over upper management to implement policies, and in tactfully handling sensitive security matters with senior people.

You may find, however, that you've approached someone about their security behaviour and since discovered that the problem is more endemic. You may need to call upon an Observer to find out exactly how extensive the problem is, or where the biggest lapses lie, as well as a Fixer to help you implement an action plan.

THANK YOU

INTRODUCTION TO SECURITY

CPNI
Centre for the Protection of National Infrastructure