SMALL ACTIONS, BIG CONSEQUENCES:

YOUR GUIDE TO BEING SECURITY SAVVY

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.

INTRODUCTION

This booklet is for employees within organisations that hold sensitive assets – assets which may be vulnerable to security risks, such as theft, cyber-attack, espionage and terrorism. These assets could be organisational systems, processes, technology, designs, equipment, materials, public or employee data, research projects, intellectual property and/or intelligence. As employees, you can play a vital role in helping to protect these assets and keep the organisation safe and secure.

HOW YOU CAN HELP

Small actions you can take inside and outside of the workplace can make a big difference in helping to reduce the likelihood of a successful attack. These actions can be as simple as shredding sensitive documents, ensuring visitors are always escorted in protected work areas, reporting suspicious behaviour to security or taking care over what organisational information is shared with outsiders.

USING THIS BOOKLET

This booklet provides examples of the behaviours you can demonstrate to help keep your organisation secure. It highlights security scenarios you might encounter in your day-to-day life, and actions you can take to help reduce vulnerability to a threat. This booklet also illustrates the kind of behaviours to avoid that can have adverse effects for security.

You are advised to read the booklet and to think about how these behaviours apply to your role and organisation. For further information on the specific security practices in your organisation, please contact your local security representative or team.

The booklet covers the following scenarios:

1. Entering and leaving secure sites
2. In and around the workplace
3. Managing visitors
4. Using corporate IT
5. Representing your organisation online
6. Handling queries from customers, suppliers, partners or the public
7. Living life outside of work
8. Being a security advocate as a line manager
9. Being a security advocate as a senior leader

ENTERING AND LEAVING SECURE SITES

Entrances and exits to sites are the first and last points of protection for the organisation. As an employee, you can play a key role by being alert and vigilant to any unusual or suspicious activity (e.g. suspicious individuals or unattended bags) by identifying and reporting this immediately to security. You can also minimise potential security risks to you personally by adopting sensible and practical security behaviours.

Some example do's and don'ts regarding your security behaviour when entering or leaving sites are provided below.

DO

- ✓ Look alert and be vigilant when entering or leaving a site – your behaviour can deter someone with hostile intent from planning an attack.
- ✓ Report anything unusual or suspicious immediately to security, following the correct process (e.g. make sure you have the phone number for security to hand).
- ✓ Avoid having the same routines every day for when you enter or leave a site (e.g. vary which entrances/exits you use and times you use them).
- ✓ Follow the correct entry and exit procedures for passing through gates, vehicle barriers, doors and so forth (e.g. swiping your pass or signing in and out).

DON'T

- ✗ Appear distracted or unaware of your surroundings at the entry or exit points (e.g. by being on your mobile phone or wearing headphones); this can give the impression that you, or the organisation, might be an easy target for an attack.
- ✗ Ignore suspicious activity because you feel it's not your responsibility or you don't know the reporting process.
- ✗ Draw attention to where you work by smoking or loitering near the entrances or exits of your site, or having your pass on display in a public place.
- ✗ Feel awkward when asking other staff members to follow the correct entry and exit procedures, for instance asking them to swipe in rather than holding a door open for them.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

IN AND AROUND THE WORKPLACE

Good security behaviour in the workplace ensures that all employees act in a security conscious and professional way. This helps to minimise the chance of accidental breaches occurring and increases the likelihood of any malicious activity being spotted.

Some example do's and don'ts regarding your security behaviour in the workplace are provided below.

DO

- ✓ Wear your security pass in the workplace, ensuring it is clearly visible.
- ✓ Discuss sensitive subjects or projects in an appropriate location, like a meeting room, with only those who need to be present.
- ✓ Dispose of sensitive information appropriately, for example by using a shredder for paper documents.
- ✓ Ensure your desk is clear of any sensitive information at the end of the day – where necessary, lock it away.
- ✓ Allow yourself time to adhere to security policy when transferring sensitive information, whether that's sending emails or transferring printed documents securely.
- ✓ Immediately report any lost organisational items, like laptops, phones or papers.
- ✓ Lead by example and demonstrate good security practice in front of colleagues, visitors, and the public.

DON'T

- ✗ Obscure your security pass under a jacket or in a pocket while onsite.
- ✗ Feel embarrassed to approach anyone who isn't clearly displaying a security pass onsite.
- ✗ Take offence if a colleague is kind enough to remind you to display your pass or adhere to a particular security procedure – they are just trying to be helpful.
- ✗ Discuss sensitive subjects or display sensitive information in areas where visitors are likely to be, such as the lift.
- ✗ Delay reporting a lost item because you think it won't matter or assume it will turn up.
- ✗ Assume you know what information can and can't be shared with others without asking the owner of the information or checking the security policy.

MANAGING VISITORS

When receiving a visitor, check they are who they say they are: ask for identification before bringing them onsite and sharing sensitive information with them. Remember also that it is your responsibility to manage your visitor. Take time to explain any security procedures or protocols to them so that they don't inadvertently put your organisation at risk.

Some example do's and don'ts regarding your security behaviour when managing visitors are provided below.

DO

- ✓ Ensure your visitors are signed in and out, and that reception knows ahead of time who's coming and when they will arrive.
- ✓ Ensure the relevant identity and clearance checks have been made well in advance of visits, and that you verify the identity of your visitor when they arrive.
- ✓ Check that your visitors are wearing the appropriate pass when onsite and make sure they return their passes when they leave.
- ✓ Brief your visitors on any relevant security procedures, such as the requirement that they are escorted at all times.
- ✓ Take responsibility for your visitors when they are onsite.
- ✓ Keep visitors away from sensitive areas, where they may not be authorised to go, when onsite.

DON'T

- ✗ Bypass security if you've forgotten to sign in your visitor or to register their IT equipment – the consequences could be severe.
- ✗ Assume that visitors will be aware of the security procedures in your place of work. Help them out by sending them a reminder in advance regarding any IT restrictions or a requirement to show photo identification.
- ✗ Allow visitors who haven't had a precautionary identity or clearance check into sensitive meetings.
- ✗ Take short-cuts through sensitive areas of the site or make your colleagues uncomfortable about where you are escorting your visitor.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

USING CORPORATE IT

Corporate IT systems and devices frequently hold a wealth of sensitive information. This means they can often be the target of attack. Using devices responsibly and securely helps to ensure sensitive information is not accessed by those who may wish to cause harm. Know your organisation's IT policy and stick to it. Good security behaviour when using IT is vital to ensure that you and the organisation stay protected.

Some example do's and don'ts regarding your security behaviour when using corporate IT are provided below.

DO

- ✓ Lock your device or computer terminal when leaving it unattended.
- ✓ Wait until instructed by IT to upgrade your device or install new software.
- ✓ Connect only sanctioned devices and media to the organisation's network, such as authorised USB sticks or mobile phones.
- ✓ Store only the essential information you need on portable devices or mobile phones, especially when going overseas, in case they are lost or stolen.
- ✓ Avoid using work devices and work email for personal use – you could be putting yourself, and those you contact, at risk.
- ✓ Adhere to good practice and policy for information management by ensuring all your work is stored on your organisation's IT systems.
- ✓ Use your IT devices appropriately and in line with policy, for example only visiting the social media sites you are allowed to.

DON'T

- ✗ Store passwords with the associated device – if you lose the device then anyone can gain access to it.
- ✗ Download apps onto work devices unless they have been authorised by IT – you could be putting the organisation at risk.
- ✗ Install new software or carry out software upgrades unless instructed to by IT.
- ✗ Connect unauthorised IT devices or media (e.g. USB sticks or CDs) to the IT network without going through the proper channels.
- ✗ Connect personal mobile devices to corporate devices (e.g. charging personal mobiles on work laptops) unless authorised to do so; you may inadvertently pass on malware.
- ✗ Use public Wi-Fi on IT devices you have received from the organisation.
- ✗ Lose track of what corporate IT devices are in your possession and where they are.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

REPRESENTING YOUR ORGANISATION ONLINE

In an increasingly digital world, organisations are conducting a number of activities online, such as recruitment, marketing, corporate communications, and the delivery of services. However, an increased digital presence can present an increased security risk if the information posted online is not managed carefully.

Some example do's and don'ts regarding your security behaviour when being asked to represent your organisation online are provided below.

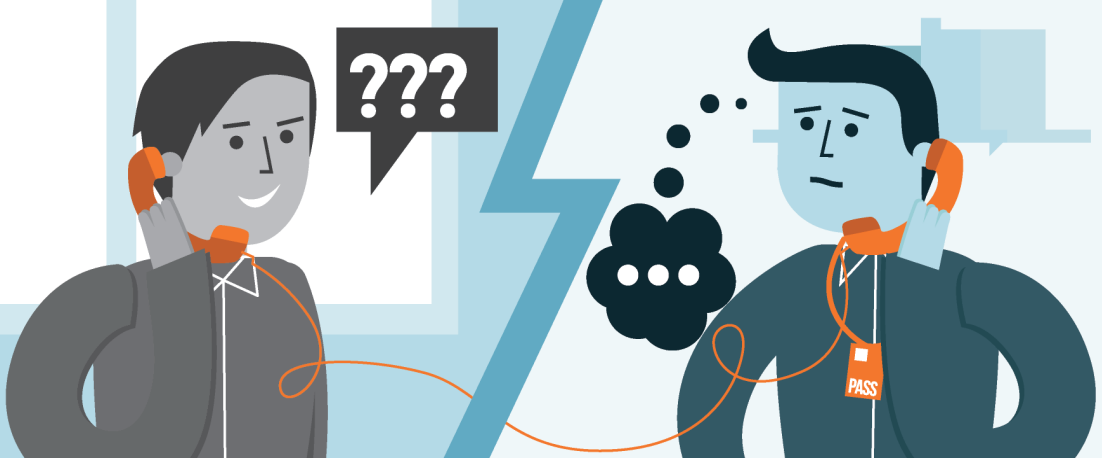
DO

- ✓ Gain official approval if you're blogging, publishing or commenting online as a representative of the organisation.
- ✓ Think carefully about what you publish online from a security perspective – limit any potentially sensitive information where possible to avoid creating a security risk (e.g. employee details or sensitive project details).
- ✓ Ask the security department to review any sensitive information that is being made public to ensure it is appropriate to do so.
- ✓ Take account of the security implications for you if you are linking yourself with your organisation online – for instance, you might like to reduce your personal profile online if your work profile is being raised (e.g. by tightening personal social media settings).

DON'T

- ✗ Publish anything online that reveals sensitive information about the organisation.
- ✗ Be naïve about online security risks, for example by assuming that the information you share will go no further than its original recipient.
- ✗ Be unprofessional when representing the organisation online by getting drawn into inappropriate discussions.
- ✗ Assume a more relaxed stance to security applies online than it does offline – the same security principles apply.

HANDLING QUERIES
FROM CUSTOMERS, SUPPLIERS, PARTNERS OR THE PUBLIC



If you deal with customers, partners, suppliers or other industry professionals on a regular basis you must remain vigilant about security, even if you know the person well. For example, when answering questions over the telephone or sharing information with them, make sure you keep security in mind.

Some example do's and don'ts regarding your security behaviour when handling queries are provided below.

DO

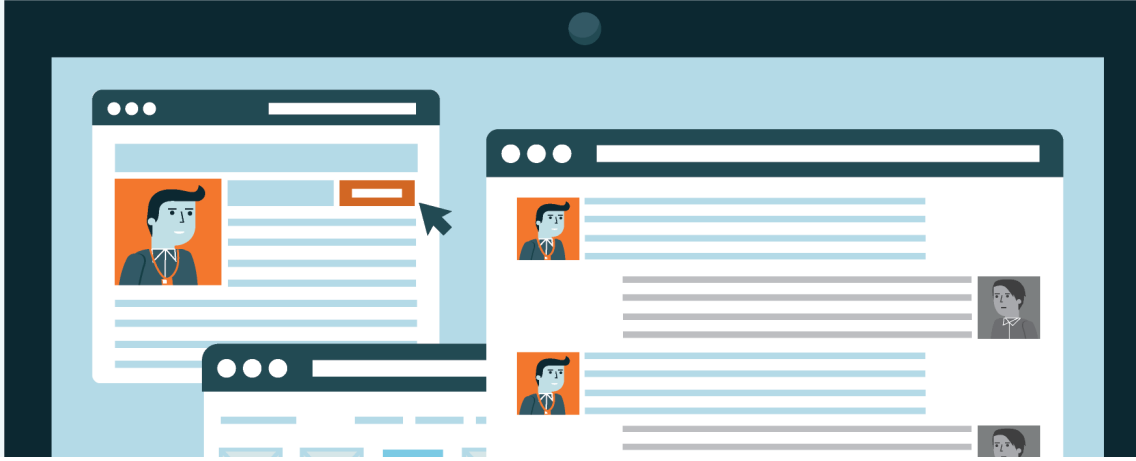
- ✓ Verify the identity of partners and customers before sharing information or working with them.
- ✓ Understand what information can and cannot be shared with anyone outside of the organisation.
- ✓ Be aware of the social engineering tactics that could be used to get you to accidentally release sensitive information, such as phishing emails or bogus phone calls.
- ✓ Only send sensitive information to external contacts when appropriate and in line with the security policy.
- ✓ Develop tactics to handle questions from external contacts politely and without revealing sensitive information.
- ✓ Take the time to double check whether information can or can't be shared if you are unsure.

DON'T

- ✗ Take any customer or partner at face value (e.g. by making assumptions about their legitimacy or credentials).
- ✗ Assume you know what information can or cannot be shared with an external party.
- ✗ Assume that social engineering tactics that manipulate you into sharing sensitive information won't happen to you – they just might.
- ✗ Give away too much information when requested by an external party just to show yourself as helpful – ask yourself "Do they really need to know this?"
- ✗ Be put on the spot and feel pressured to respond to a question immediately – you can always take their name and call them back.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

LIVING LIFE OUTSIDE OF WORK



There are aspects of work life that will inevitably spill over into our personal lives, such as when out in social situations or when interacting online. However, sometimes it is these situations that can put us at risk. Keep applying those small actions that keep us secure at work to your personal life.

Some example do's and don'ts regarding your security behaviour when you are living life outside of work are provided below.

DO

- ✓ Only reveal minimal details about the sensitive work you do, socially and online.
- ✓ Regularly monitor your digital footprint to ensure your online profile is not leaving you or your organisation vulnerable.
- ✓ Use social media sites responsibly and only share information that does not compromise the reputation or security of your organisation.
- ✓ Advise friends and family not to share certain information about you or your work, when in social situations or online.
- ✓ Keep your personal and work lives online as separate as possible.
- ✓ Seek advice on how to describe careers in sensitive roles, such as on a CV or social media profile. Promote your skills, but don't compromise security.

DON'T

- ✗ Assume you won't be targeted by someone with malicious intent outside of work or offsite.
- ✗ Draw attention to sensitive aspects of your work, or the fact that you work with sensitive information.
- ✗ Assume the default settings on your devices and on social media will keep the content of your messages secure.
- ✗ Make yourself a target by openly linking aspects of your work to your private profile.
- ✗ Write detailed accounts of sensitive aspects of work when describing your career history, such as on your CV or when speaking to a recruitment agency.
- ✗ Assume you are not vulnerable to a security breach outside of work – report any suspicious incidents that make you feel uncomfortable to security.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

BEING A SECURITY ADVOCATE AS A LINE MANAGER

Leading by example is vital to maintaining security, particularly within teams that often deal with sensitive information. If you are a line manager, you need to be especially vigilant when it comes to security behaviours. You also have a responsibility to ensure your team is fully briefed on the relevant protocols.

Some example do's and don'ts regarding your security behaviour as a line manager are provided below.

DO

- ✓ Ensure your team is fully briefed on the potential security threats they may face.
- ✓ Explain the security rules and guidelines to your team and check everyone understands them.
- ✓ Personalise security messages, making them meaningful to your team, with tangible examples.
- ✓ Assess security knowledge levels within your team and provide additional training where needed.
- ✓ Encourage two-way conversations with staff about security and provide feedback on their behaviour where you can.
- ✓ Keep note of who in your staff has access rights to certain systems or devices, closing down that access when they move roles.
- ✓ Develop an environment where your staff, including contractors, see good security practice as part of their personal responsibilities.

DON'T

- ✗ Assume your team knows about security or understands what their responsibilities are.
- ✗ Leave security briefings to the training team or security department, or forget to check that staff are clear on policy.
- ✗ Trivialise or belittle security messages in front of your team, giving the impression that security is not important.
- ✗ Ignore the security risks when making business decisions.
- ✗ Allow staff (or contractors) to leave roles with access to privileged information that is no longer needed.
- ✗ Expect staff to get security right all of the time. Acknowledge that mistakes happen, but ensure there is appropriate learning and reflection afterwards.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

BEING A SECURITY ADVOCATE AS A SENIOR LEADER

Good security practice starts at the top of the organisation. If you're a senior leader, you are key in not only demonstrating that senior management are acting in a security conscious way, but also in ensuring the organisation has the right systems, practices and guidance in place to ensure it develops and maintains a security savvy workforce.

Some example do's and don'ts regarding your security behaviour as a senior leader are provided below.

DO

- ✓ Keep up to date on security threats facing the organisation and the wider industry.
- ✓ Ensure there is accountability for security at a senior level, such as by nominating a senior risk owner.
- ✓ Develop partnerships with security functions in the organisation to keep abreast of issues and updates.
- ✓ Keep security implications in mind when making strategic decisions.
- ✓ Develop organisational systems and processes that make it easy for staff to follow good security behaviour.
- ✓ Monitor the security performance of the organisation regularly and ensure proportionate protective security mitigations are in place.
- ✓ Equip the organisation with the resources it needs to instil a strong security culture and a security savvy workforce.

DON'T

- ✗ Assume you are up to date on the current security threats and risks facing the organisation – ensure you receive regular briefings.
- ✗ Presume that security is the responsibility of others and not of senior management. This can have a significant negative impact on the organisation's security culture.
- ✗ Ignore the value of building good strategic relationships with the security functions within the organisation.
- ✗ Take account of security as an afterthought when making strategic decisions.
- ✗ Assume third parties that hold your data and/or assets have appropriately secure systems and procedures in place.
- ✗ Rely on the right security culture developing organically over time – your strategic direction and leadership is key.

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy

AND FINALLY...

By applying the good security practice set out in this booklet, we can all play our part.

Remember: small actions can have big consequences. By taking these steps you can keep yourself, your colleagues and your organisation secure.

If you have any questions about the security practices in your organisation, contact your local security representative or team. You can keep a record of their contact details in the space provided on the next page.

NAME	
ROLE	
CONTACT DETAILS	

© Crown Copyright 2016 | Small actions, big consequences: Your guide to being security savvy