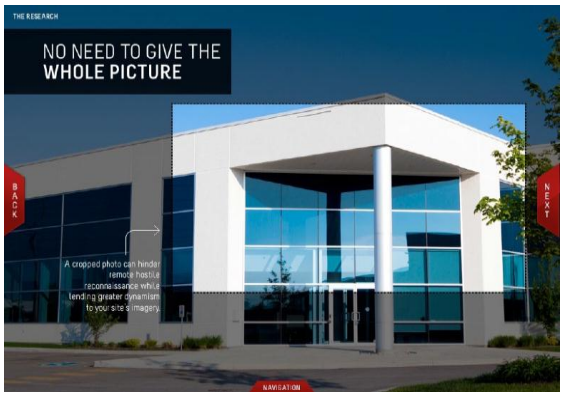
Security-minded comms

BRIEFING NOTE



Overview

This interactive guidance has been designed to help organisations understand the threat from hostile individuals and groups and how online communications can influence their behaviour.

It has been put together by CPNI (Centre for the Protection of National Infrastructure) and is based on specialist research, including the observations of individuals replicating online hostile reconnaissance on a variety of organisations, including ones like yours.

Who are these hostiles? They can be organised criminals, protesters, terrorists, governments or even lone extremists. The guidance provides more information on the types of threat and how they plan their action and also gives case studies of how hostile reconnaissance has been used in the past.

Corporate communications is a relatively untapped but potentially very effective layer of protective security, which can be achieved at little, if any, cost. This guidance shows how corporate communications can help deter those seeking to carry out hostile reconnaissance, especially when they are trying to select their targets. It also shows how corporate communications can enhance and augment the deterrent effect of protective security.

The guidance will help you:

- reduce the risk to your organisation from hostile actors
- understand the connection between communications and security
- deter hostiles without compromising the effectiveness of your communications
- evaluate and amend your existing online content
- produce security-minded communications in the future

The guidance is easy to use, clear of jargon and accessible to everyone in your organisation, not just security professionals. It is accessible as a flash document, as an interactive pdf or in tablet form.

The research

Putting yourself in the position of the hostile can be the most effective way of understanding how they behave. As such, CPNI commissioned research from surveillance specialists who, acting as hostiles and only using open source information, looked at 50 organisations in order to see what they could find and in doing so, whether there would be anything to discourage them.

Out of the 50, only four deterred our 'friendly hostiles' from doing further research, while half were described as easy, or very easy targets.

The research found:

I.T. ENCOURAGED HOSTILES IF:

- Detailed information revealed exploitable weaknesses in security
- Security did not appear to be a priority for the organisation
- There was a lack of evidence of physical security measures
- The website had a bland cookie policy

I.T. DISCOURAGED HOSTILES IF:

- A lack of information meant they could not confirm or deny assumptions
- They could not ascertain detail on organisational structures or personalities
- A lack of imagery prevented a virtual recce of the physical location
- The cookies policy included logging of a user's IP address, pages visited and keywords searched for

Organisations that demonstrated that they had security measures in place, but which did not give too much away in terms of specific detail, were deemed to be the hardest targets. Organisations should ask themselves whether it is absolutely necessary to make content available for their main users; in doing so, they might be able to reduce the amount of information available to hostiles.

The guidance outlines what hostiles look for and what sort of things you can do in terms of both removing sensitive information and introducing deterrence messaging. Communication concepts like 'the power of unpredictability', 'hard words softly spoken' and 'strong policies, smart functionality' can all be utilised to help you reduce the threat.

Next steps

Once you have read the guidance, you are encouraged to undertake a series of exercises to make you think like your adversary. Putting yourself in the position of the hostile will better enable you to assess your communications. The final step in the process is to complete an audit of your online security messages. An audit tool and exercises are available as part of the guidance.

The impact of this guidance is improved when it is used in conjunction with other CPNI guidance, most notably the Communications Toolkit for Managers Responsible for Physical Sites. By combining the techniques in both guides, by 'layering' deterrence messages, you can ensure that hostiles are confronted at every stage of their planning process.

Further information

Please email DETERComms@cpni.gsi.gov.uk