CPNI
Centre for the Protection of National Infrastructure

Security Minded Communications Guidance for Virtual Tours

PUBLISH DATE: May 2020

CLASSIFICATION: Official

The aim of this guidance

This document supplements the existing Security Minded Communications guidance and highlights the key protective security points to consider when creating virtual tours of your facilities.

Overview

Virtual tours are a great way of helping attract people to your site and/or plan their visit. During the COVID-19 lockdown restrictions virtual tours can help maintain interest of potential visitors and keep them mindful of the site as a place to visit once Government advice allows.

Whilst helpful for potential visitors, virtual tours can be incredibly useful for another audience – those considering malicious acts against your site or visitors. This can range from petty criminality (e.g. pickpockets) to terrorists.

This short guidance shows you how you can create virtual tours that are attractive and useful for your normal site visitor, but less useful to those with malicious intent, who are also known as a 'hostile'

It also shows how you can further deter these individuals with some key messages about security placed on your website

Background

The Centre for the Protection of National Infrastructure (CPNI) defines a hostile as 'a person who wants to attack or disrupt an organisation for profit or to make a political or ideological point'. Research shows that there are three stages in a hostile's attack planning: target identification; detailed planning; and action. A key part of the first two stages is hostile reconnaissance. CPNI defines hostile reconnaissance as 'purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target'.

A hostile doesn't necessarily have to physically visit a site to obtain the information they require. They can use online resources to gather useful and current information from credible sources. Your communications can provide a potentially very effective layer of protective security, at little or no additional cost. By adopting a security minded approach to your communications and online content you can deny the hostile the valuable information they require in the attack planning stage.

How to create virtual tours….

Step 1- What would a hostile want to know about my site?

A hostile will be looking to obtain information that helps them to select a target, choose an attack time and understand what method of attack is likely to be most successful and fits with their motivation. They will be looking for information on the protective security measures at your site and will be seeking to understand where there are vulnerabilities in your protective security.

Step 2- How would a hostile obtain that information?

CPNI
Centre for the Protection of National Infrastructure

Security Minded Communications
Guidance for Virtual Tours

PUBLISH DATE: May 2020

CLASSIFICATION: Official

A hostile will undertake online hostile reconnaissance as well as onsite hostile reconnaissance to inform their decision making. They may also seek to gain information from current or former members of staff, contractors or volunteers.

Step 3- How can I create virtual tours without giving away information that may be of use to a hostile?

When creating website content, press releases or any other communication, you should consider the follow points:

- What do I **need** to communicate?
- How can I use this opportunity to **seed** messages that would deter a hostile?
- How can I ensure I provide information **without giving away details** that would be potentially useful to a hostile?
- If I need to put out details, how can I **counter** any vulnerability created by promoting the protective security measures in place?

When considering virtual tours of your site there are some specific things you can do to limit the amount of useful information a hostile can obtain from the tour, whilst still ensuring that the tour is informative and fun for your target audience.

How to deter a hostile:

- Ensure your website has a robust and up to date cookies page and privacy statement so that a hostile will know that you record details about their use of your website, such as their IP address.
- Ensure your website includes a dedicated safety and security page that highlights the range of security measures that are in place at your venue (without giving away details that could be useful to a hostile).
- Audit the content on your website and make sure you are not accidently giving away information that might be useful to a hostile.
- Staff featured in the tour are wearing security passes with the detail blurred so that a hostile could not replicate the pass or identify the full name of the staff member.
- Consider a tour by room or key feature, rather than a walk-through tour which provides more information to a hostile on your site's layout.
- If your virtual tour takes the form of a walk-through, consider what other information you could include on your website to promote the protective security measures you have in place. For example, promoting collaboration with neighbouring business or law enforcement partners might suggest to a hostile that those working on your behalf looking for suspicious activity extend beyond your perimeter.
- Flag that security is in place at your site but do not reveal detail that would be beneficial to a hostile. For example, "Here we take the safety and security of our visitors seriously but to

ensure you get the most from your virtual experience we have removed certain security features from the tour. To find out how we keep you safe when you visit our venue please visit our Security page."

- If there is a chat function, or area for visitor comments on the virtual tour, be proactive about monitoring these comments and responding.

Things to avoid that may give a hostile valuable information:

- Virtual tours of entrances/exits that show exactly what search or screening is in place at your site. Also avoid showing doorways and corridors that help a hostile to understand the floor plan but add little enjoyment or information for your target audience.
- Showing the location and type of CCTV installed at your site.
- Showing the locations of security staff or information that will reveal security shift or patrol patterns.
- Showing emergency evacuation or muster points on maps that may appear around the site (particularly by exits).
- Providing information about staff passes, so if staff are featured in the tour blur out pass information.
- Providing accurate to-scale maps / floor plans of your site
- Sharing information about exact visitor numbers or busy and quiet times.

Further Guidance

If you would like further information, or access to the Security Minded Communications or Deterrence Communications guidance, please contact detercomms@cpni.gov.uk or your local CTSA.

Understanding Hostile Reconnaissance

Understanding Hostile Reconnaissance and countering the threat

Disrupting Hostile Reconnaissance

NaCTSO Crowded Places Guidance

Action Counters Terrorism

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 favouring by CPNI. The views and opinions of authors expressed within this document shall not be used or 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

CPNI
Centre for the Protection of National Infrastructure

Security Minded Communications Guidance for Virtual Tours

PUBLISH DATE: May 2020

CLASSIFICATION: Official

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 judgement as regards use of this document and seek independent professional advice on your particular circumstances.

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without written consent from the Centre for the Protection of National Infrastructure (CPNI).