



SECURING YOUR PUBLIC WI-FI

Introduction

Wi-Fi availability or wireless access is listed as the number one amenity expected by travellers today. In this extremely competitive market, it's no surprise then that 90 per cent of hotels and bed and breakfasts (B&B) today have a wireless network installed so guests can connect to the Internet.

Suddenly it's possible for anyone to go out and buy a cheap Wi-Fi kit in their lunch break and install it themselves. This is great news for B&B or Self Catering Accommodation providers who are looking to add value to their business quickly with limited disruptions, however, it also illustrates the threat wireless connections could pose to the tourism industry if more and more people are in control of a technology they don't have the first idea about securing, let alone managing.

One of the first high profile cases of hotel security being compromised was back in 2007 when a London branch of the Novotel chain was found to have effectively no security on its wireless network. The website claimed that their hotels feature "top-speed, high security wireless internet access in all our hotels" but it was found to be running a security-free wireless network including VoIP, which meant that the hotel's entire booking and customer information system was effectively open to access by all those with internet connections.

The fact that such a major security breach was allowed to happen with an international hotel chain suggests that many hotels are attempting to employ internet-based communication systems, primarily for cost reasons, while failing to understand the security implications that are associated with such an approach.

Wi-Fi threats

As the world becomes dependant upon wireless and VoIP communication systems, so the risk and dangers of such an approach continue to rise. Wi-Fi technology now has the potential to bypass almost all existing IT security systems and open the door to hackers, unauthorised entry and just about every other security nightmare you can think.

If your B&B or hotel has an alarm system in place to deter burglars, then the same measures need to be put in place with your wireless network. According to researchers, the weakest link in any hotel's network is its wireless network, as signals between the access point and a computer can be compromised easily. Even though a router does offer advanced security features, it still does not mean the guests or hotel's personal/confidential information is being protected.



SECURING YOUR PUBLIC WI-FI



This guide is designed to help owners of hotels and B&Bs to understand the security risks, and to provide practical advice on tightening up security measures to minimise the risk of breaches that can carry high costs to the business, both financially and in reputation terms.

“It won’t happen to me”

If you own a B&B and you have the attitude “it won’t happen to me because I’m out in the sticks and only have two to three guests at a time”, then think again, as breaches of wireless networks can happen anywhere and to anyone.

Our research shows 90 per cent of B&Bs in Wales that offer Wi-Fi as a value added service leave their networks wide open i.e. without a password for guests to use. This potentially leaves the systems wide open to hackers, with potential embarrassing consequences for the guests and the B&Bs concerned.

Gaining unauthorised access to a wireless network is a simple process for a hacker if the correct methods to negate these risks are not taken by the hotel or B&B manager/owner. The risks could include accessing your business network and data, using your network to commit a crime, stealing copyright material via file sharing, or something as severe as downloading child abuse images.

The Digital Economy Act 2010

The Digital Economy Act requires OFCOM to implement regulations placing the responsibility of illegal activity such as copyright theft squarely at the feet of the network owners. If you don’t take reasonable steps to protect your network, identify who has access to your network at any given time and warn against illegal activity, at any given time, you could be liable for your visitors’ crimes.

What makes a good password?

- Needn’t be a word at all. It can be a combination of letters, numbers and keyboard symbols.
- Is at least eight characters long. Longer passwords are harder to guess or break.
- Does not contain your user name, real name, or company name.
- Contains a mix of upper and lower case letters, numbers and keyboard symbols (i.e. `~!@#\$%^&*()_+-=|[]:”;’<>?. , . /).
- Is changed regularly.

Minimum Equipment Recommendations

Ensure you use the following equipment and settings on your public wireless access:

- Ensure your Wi-Fi access point is a wireless router with VLAN (virtual local area network) capabilities. This will enable you to separate your business’s network and data from your visitors’. Examples of suitable routers to use are available at www.ecrimewales.com/products. If you use a standard domestic Wi-Fi router your entire private business network will be accessible to all of your visitors.
- Use WPA2 (Wi-Fi Protected Access 2) with AES (Advanced Encryption Standard) encryption on your access point. WPA2 is the latest security standard introduced by the global, non-profit industry association, the Wi-Fi Alliance. Some older equipment may not work with WPA2; however do not use encryption standards less than WPA. Older WEP (Wired Equivalent Privacy) encryption is simply not secure enough; our experts have been able to hack WEP encryption in less than 3 minutes!
- Keep a log of when visitors request access to your wireless connection. Ensure they sign a terms and conditions document before you give them the wireless access key (password) to allow them to access your connection.
- Make sure your wireless access key is an alphanumeric password of at least 8 characters using both upper and lower case letters. We suggest you change your wireless access key monthly.
- Consider filtering access to P2P (peer to peer) data on your network. This will offer you some protection against illegal file sharing of copyrighted material. Some routers will allow you to set filters to block all types of data transmission and file types, thus allowing you to choose what activity visitors can undertake on your connection.
- Disable VPN (virtual private network) access on the router settings if you don’t require it. If you don’t know if you need it or not, you probably don’t!
- Some routers will also let you restrict access at certain times of day. You may want to consider this.
- Data logging provides evidence of all data traffic and activity on your network. If the worst happens, this may prove crucial in proving your innocence.

You may consider implementing a separate telephone line and broadband connection to completely separate your business network from your guests. If you go down this route we still recommend you implement all of the above advice to offer yourself and your business the maximum level of protection.

If you are unsure about any of the above we suggest you use your IT support provider to help you install the equipment. For a list of suppliers in Wales, visit www.ecrimewales.com/suppliers



SECURING YOUR PUBLIC WI-FI

Terms and conditions

Technology alone can never give you 100 per cent protection, and the roaming nature of Wi-Fi means user education in this area is of particular importance. It is absolutely essential that hotels or B&Bs implement a rigorously enforced set of terms and conditions so everyone is educated about the requirements for security. By getting your guests to sign and agree to the terms and conditions you will also go a long way to ensuring that your business is covered for any inappropriate or illegal activity that your guests may carry out when roaming on your wireless network. It will also in most cases deter any criminals trying to compromise the network if they know their personal details are on record.

With this factsheet we have included a template Terms and Conditions document for your Wi-Fi serviceⁱ. This template policy is also available to download and personalise at www.ecrimewales.com/tourism

The implementation of the Digital Economy Act is likely to alter further the requirements on those who provide wireless internet access. You should periodically check the e-Crime Wales website to ensure that your policy is up to date.

Be safe

If you want to run a safe and successful Wi-Fi service within your hotel/B&B, think of every possible 'door' a hacker can enter because if given half a chance, they will take it. As you have seen above, implementing Wi-Fi security isn't rocket science - if you have taken the time to weigh up the benefits, purchase the kit and install it, then you have time to secure it.

For further information on wireless security, please visit www.ecrimewales.com

ⁱ This policy is prepared to provide general advice on the issues which a business will need to include in considering a wi-fi policy. The policy should not be considered as an alternative to taking advice on the structure and content of a policy (or on specific situations where the policy may have been breached) suitable to the specific needs of your organisation. As a result neither the Welsh Assembly Government nor Morgan Cole accept any liability arising from the use of this policy and should the user choose to use the policy for implementation in their own business without specific legal advice they do so entirely at their own risk.