IT for CEOs & CFOs is published by House of Words Ltd.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

Keeping Data Safe on the Move

Mark Hickman

Mark Hickman
Chief Operating Officer
WinMagic

Biography

Mark Hickman is the Chief Operating Officer at WinMagic (https://www.winmagic.com), and is responsible for direct and channel sales, marketing, professional services, and global business development.

Joining WinMagic in 2010, Mark brings over 18 years of software sales experience. Mark holds a BA majoring in Economics from Concordia University in Montreal, Quebec.

Based in Mississauga, Ontario, WinMagic provides key management for all encryption needs. With the leading SecureDoc product line, WinMagic continues to provide easy-to-use and robust data security solutions for wherever data is stored, providing enterprise grade encryption and key management policies for all operating systems.

Keywords Enterprise IT, Data breach, Encryption, Mobile
Paper type Opinion

Abstract

Keeping data safe when we are on the move gets increasingly complex as we all work out of the office more than ever before. In this article, the author talks about some of the challenges and offers some advice on how to become a victim of cyber crime or an accidental data breach.

Introduction

More than ever before we all work on the move – technology and connectivity have reached a point where we no longer panic about whether it will be possible where we are heading. It means that the location of data is no longer fixed, so the importance of protecting data across devices and cloud services is much more important.

Data security is probably the last thing on your mind when preparing a business trip, but data is one of the most valuable things you carry, and must be protected. Unfortunately, usually you don't realize how important it is until it has been stolen. A laptop or smartphone is replaceable but the sensitive data that those devices carry is irreplaceable. Once in the wrong hands there is nothing you can do except attempt to deal with the damage that has been done, or may follow.

In today's IoT world we have access to everything and everyone around us from public Wi-Fi in hotels to coffee shops to restaurants to airports. Staying connected is made quite easy for us, but there is a trade-off that comes at the expense of the security of our private data. These free public Wi-Fi spots are attractive to travellers, but they also attract plenty of hackers. From the moment you connect to public Wi-Fi you are connected to the rest of the world and are potentially letting hackers watch your traffic. The way hackers do this is by positioning themselves between you and the connecting point. This way, instead of being connected directly to the network, you are sending your information to the hacker. At this point they have access to all the information on your device such as credit card information, banking information, confidential business emails, and various credentials to your private data.

How can you prevent being the next target?

Well, staying off the public Wi-Fi is the best strategy, but understandably sometimes it cannot be avoided. Here are seven steps you can take to make sure that your information stays safe on your device where it belongs:

1. **Disable your automatic connection to Wi-Fi** – Laptops, tablets and Smartphones typically roam to find the best Wi-Fi connection. By disabling this feature you know when, where and how you are connected.

2. **Update and Patch everything** – Cybercriminals are always looking for security holes, so before you travel make sure that all the latest software and security updates are applied on your devices.

3. **Use a VPN** – It encrypts traffic between the device and the VPN server, making it a lot more difficult for a hacker to access your data.

4. **Only connect to websites that use HTTPS** – Most websites that use https encrypt everything you send and receive from the website making the communication secure. You can tell whether a website uses this by looking at the start of the web address, and you will usually find a padlock displayed in the address bar confirming that the connection is encrypted.

5. **Use a strong firewall and antivirus** – A firewall will not provide complete protection but it's an extra layer that should be enabled for your security. While an antivirus will alert you when your system has been compromised.

6. **Two-Factor Authentication** – Use two pieces of information to log into your accounts. That way even if a hacker can get your password by hacking your Wi -Fi, they will not be able to log into your account because they don't have the second piece of information needed.

7. **Only use legitimate public Wi-Fi** – If you are unsure whether the public Wi-Fi is genuine, ask the hotel, restaurant or café to confirm the correct network name and splash screen you should get when joining the network. This is important because there is no reason that a hacker could not set up a Wi-Fi network from their laptop using the same name to intercept traffic.

In short, whether you are travelling on business or sitting in a café or hotel looking at your emails – be safe, be sure, and be wise.