5 TIPS TO PROTECT CUSTOMER DATA FOR HOME BASED PROFESSIONALS

Protecting your customers' data is as important for home-based professionals as it is for multi-million pound companies.

When considered, the chances are your computer has a significant amount of confidential customer data on it. Business plans, financial accounts and even payment details stored on your devices could cause serious problems for your client if they fell into the wrong hands.

Here are 5 tips for home-based professionals on how to protect customer data.

1. Safe payment
If you allow customers to pay their bill online, or are considering implementing it, it is vital to use an established payment platform to securely handle the entire transaction, as well as the storage of credit card details.

Failure to meet the Payment Card Industry Data Security Standards (PCI DSS) can result in a data breach, which not only leaves your customers vulnerable to fraud, but can lead to eye-wateringly high fines for your company.

More and more businesses are choosing to use solutions that are hosted on secure third party servers (PayPal being a prime example of this) that already comply with PCI DSS standards.

2. Encrypt
Encryption comes in many different forms and offers protection under different circumstances.

For your IT equipment, you can use full disk encryption which means all data on the computer is encrypted You can encrypt individual files when they are being transmitted to a third party.

Some software offers password protection to stop people making changes to data but you need to be aware that this may not stop a person reading the data.

A more secure alternative is to encrypt the data itself; and although many believe that only large companies need their files encrypted, you can never be too safe when it comes to protecting sensitive customer information, and can rely on this when defending a potential claim.

Consider re-evaluating your data encryption process; and seek out information form software and IT service providers.

The encryption standards today are a lot higher than they were five years ago.

3. Security lock down
Securing your data is vital; you do not want to be caught out by a virus or malware infecting your PC and gaining access to everything you own.

Make sure your computer has up-to-date anti-virus and firewall protection, and routinely patched; these basics are no different to locking and alarming your premises.

Ensure that your home WiFi connection is secured using WPA2/PSK encryption and uses a strong password.

Although most routers already have this enabled, some older routers may use the inferior WPA or WEP standards, or have default passwords which can leave your network vulnerable. Verify security with your broadband provider to ensure you are not caught out.

4. Back up
As well as customer data being stolen, you must also think about how to avoid losing it. Lost customer data can cripple a business, so ensure you back up regularly - either to an

external hard drive that is physically separate from your IT or by using cloud-based services.

There are endless options out there, including free and 'pro' versions – best-suited to your home-based business.

5. People-proof
Once you have your IT equipment secure with updated programs, encryption and back-ups, the final thing to think about is protecting it from other people.

Passwords are advised, but industry advice is mixed on storing multiple passwords and frequency of changing them; the best philosophy is to ensure suitable priority given the more sensitive or valuable data.

Where employees or sub-contractors use your IT equipment or network, ensuring appropriate permissions and background checks take place.

Lost or stolen IT risks can be mitigated by applications that allow you to remote-lock (or even remote-wipe) in the event it is stolen.

Summary
Increasingly these data and IT security settings are in-built or default options. But a home professional must not take this for granted and balance their typical use with security, and also avoiding weak links where their IT overlaps.