MAXIMUM SECURITY

BY **TIM**KELLY | @MOTORCLAIMGURU

It's Monday morning. You've gone into work fully expecting an invoice to have been paid and to find £30,000 sitting in your account. The insurer told you it was going through Friday and would be in your bank after the weekend. But this time, it's not the insurer playing games, and that money you're owed is still missing.

I ask myself, why is it that as a general rule the vehicle body repair industry is in the dark ages when it comes to running the business, especially surrounding cyber security?

If your email address is something like "paint&body@hotmail/yahoo/gmail/bt.com", then you need to be giving your heads a wobble. I bet you have not changed your password this month either. What? Not in the last 10 years? And you don't have two-stage verification set up, or use a server, or have encrypted email?

I hope the above truly terrifies you because that is my intention. I get asked to assist with a lot of things, and three times in the past few months, this has happened to a bodyshop just like yours.

The Christmas period is a perfect time to attack vulnerable businesses.

Do you have Wi-Fi via a router connected at work? Did you turn it off over Christmas? Or any time when you are not there? In fact, do you turn your router off every night? Do you have your plugs on a timer switch to physically stop power going to your computers? This is simple stuff.

One in five businesses go bust after a cyber-attack, and 48% of UK businesses reported at least one cyber-attack in the past 12 months.

SECURE YOUR SYSTEMS

Because you handle your clients' data, you will be registered with the Information Commissioner's Office – **https://ico.org.uk/for-organisations/advice-for-small-organisations/**. You are registered aren't you?

The risk attached to losing that data and any criminal use of it, can make you liable. Names, addresses, bank and credit card details – think about it.

Do you have secure firewalls on your IT systems? Intrusion detection systems? are you paying for up-to-date antivirus software? You cannot afford not to have it, and you can claim it back as a business expense.

A good starting point to learn about all this can be found here: **https://www.ncsc.gov.uk/collection/small-business-guide**. Don't put it off, you need to know it now.

How secure is your internet connection, your Wi-Fi? Are you still using the password it came with? Or "bodyshop123"? Are you encrypting your data? Your emails and financial transactions?

Are you using a remote server? My website and emails are "hosted". I pay for a company to protect me and anyone who communicates with me. I have in the past, a long time ago, been hacked and someone gained access to my emails. Only one email was read, forwarded on and used as it was not intended. It caused me huge headaches, including threats of legal action against me. It was an active attempt to undermine my credibility.

Never again. There is no such thing as "un-hackable", but there is much you can do to protect yourself.

Any email is vulnerable, some more than others. Change your passwords regularly, use two-stage verification, have a trusted person as back up verification. Set up a proper domain for your website and attach your email to that so your emails are encrypted.

Your password should be at least 16 characters long and a mixture of random letters, numbers and symbols that don't spell a word.

COMMON THREATS

1. **Malware:** Malicious software, ransomware and spyware can infiltrate systems and cause huge amounts of damage.
2. **Phishing attacks:** Designed to deceive to make you download software.
3. **Social engineering:** Using human vulnerabilities to manipulate you into giving sensitive information to gain access.
4. **Insider threats:** Employers and contractors with malicious intent, or it could be leaving your mobile phone unattended. If you are a one-man band, is your office locked when you are working on a vehicle?

What about that business with the missing money? The insurer says they have paid the bodyshop, however the bank details had been changed on the invoice so the insurer actually paid somebody else. The invoice the insurer received came from the bodyshop's email address, "allegedly".

Current status? Stalemate. The insurer has advised they are not paying again and blame the bodyshop. The bodyshop can find nothing wrong their end and believe it is down to the insurer. What we do know is someone got into the system somewhere and made those bank changes.

Next step? Legal action, and all the hassle that goes with it.