Coming Soon to a Call Centre Near You: More Fraudsters (apparently)

By **PAUL FISHER**

Musing through the myriad number of email security newsletters I subscribe to, a headline from a recent addition caught my eye: “Call centre fraud: how to respond”.

According to specialist security website BankinfoSecurity, in 2014, the call centre is likely to find itself the object of misplaced affection from more fraudsters than is frankly desirable.

Shirley Inscoe, a financial fraud analyst at Aite, is quoted as saying malware and call centre fraud are the two big threats to financial institutions, and the call centres of the largest financials are being targeted by organised gangs at “unprecedented” levels.

Well, maybe. Perhaps there is another way of looking at this. Obviously hackers and criminals will target call centres, same way they target banks or indeed any organisation that stores or processes personal data. I think though that our Shirley is being a little alarmist. It’s not as if call centre management aren’t aware of the risks and threats they face from criminal organisations.

One thing about the UK, we may not be the global power we once were but we do some things very well, and one is call centres. I like to think that we have some of the best, most advanced in the world, staffed by people who are empathetic and well-trained. Yes, really - I know because I’ve used them.

But I digress. The other good reason for call centres ensuring they don’t fall victim to criminals and fraudsters is a thing called PCI-DSS. This ugly acronym (actually most acronyms are ugly these days, especially in the tech world) stands for Payment Card Industry Data Security Standard, set up by the payment card industry to ensure that any organisation that processes credit and debit cards, does so securely. Failure to comply can lead to big fines, or worse, losing merchant status altogether.

To any call centre organisation, losing merchant status would pretty much render it useless, not to mention commercial ruin for its owners.

Because call centres deal with personal data when at its most vulnerable, via voice, they take security so seriously - probably more acutely than other payment card processors. Security software can do much, but none can prevent eavesdropping or human error such as notes left on desks or in the trash, for example. Again, this is why call centre management train and retrain their staff in the fine and essential art of keeping a secret.

Unless staff are totally on their game and have been taught to recognise and stop social engineering tactics by criminals, the defence against them is as thin as the human breath that accompanies the fatal words down the line.

As Jonathan Gale, CEO of New Voice Media told Call Center Helper, “One of the biggest issues you will face in making your call centre PCI compliant is managing the people involved. The more you can limit the number of agents that are exposed to sensitive data and reduce the amount of data they can see, the safer it will be. The best way to do this is to make sure that your staff are only given access to the information they need to do their job." I couldn't put it better myself.

Given that the lifeblood of any call centre is the storage and processing of consumer data –whether by voice or electronic means, it's no surprise that the industry takes security and industry initiatives like PCI-DSS so seriously. It has to. And why scary predictions like Shirley's should be taken with not so much a pinch of salt, more perhaps a useful and timely reminder of the threats out there.

Please fill out the form and we will be in touch with you shortly.

1.844.324.0340