Conquest Wildman

Final Defence

Improving your last line of defence against Cyber threats

When considering how to protect their IT, most companies overlook the area in which they are most vulnerable.

Your business has probably invested in good firewalls, managed anti-virus, anti-malware and e-mail protection, but if your staff are not risk aware then in terms of security they are almost certainly your companies weakest link. Even more concerningly they are probably not even aware of it.

Every day your staff are receiving e-mails and using the web to conduct their work. You are entrusting the safety of your whole IT system to people who may not have been properly trained on how to spot phishing attacks, how to avoid the ransomeware and crypto viruses that are becoming ever more common and increasingly sophisticated. How do you expect them to distinguish between genuine e-mails and those which are very cleverly engineered frauds that will harm your business if handled incorrectly?

In the past it has been fairly easy to spot the poorly written fraudulent e-mails because of the unusual English and bad grammar. But the fraudsters are improving fast, many of the e-mails we have seen recently are almost indistinguishable from genuine correspondence and enquiries your business would expect to receive.

Cyber attacks in general are becoming more sophisticated and affecting our customer base on an almost weekly basis. They are getting harder to protect against when using traditional methods, and becoming much more sophisticated in their nature. Cyber crime has certainly moved from the bedrooms of mischievous teenage hackers to become big international business for organised criminals and you may be surprised to know that organisations like yours present so many opportunities for fraudsters to anonymously benefit if your staff are not properly trained.

Final defence is our solution to cost effectively providing your employees with the knowledge they need to keep your business safe from Cyber Threats on an ongoing basis.

Using a unique program of automated mini online training sessions and quizzes which are delivered directly to your employees inboxes according to a predefined schedule, all IT users in your organisation can soon be made security aware and taught the simple skills they need to keep your business safe. All of the training is delivered in 'bite size' chunks which can easily be incorporated into a normal working day without causing disruption to peoples regular work loads.

Spending just 8 minutes watching the first of our online videos will explain simple methods your staff can use to differentiate between a genuine e-mail enquiry and a dangerous phishing or malware attack. A simple skill that all e-mail users in your organisation should be made aware of.

As a manager, you will receive regular reports that show which staff have viewed which of the training materials and how they have scored in any of the security quizzes that are present at the end of some of our training modules. We use the same information to send reminders to those who do not engage in the training and to offer further resources to anyone who scores poorly on the quizzes.

With threats constantly evolving it is important to keep on top of your staff security training. With our Final Defence Programs you can leave that to us. If good practice security advice changes, then we will update your staff accordingly.

To ensure the training remains effective and to asses your organisations vulnerability, we also occasionally send harmless simulated phishing attack e-mails into your organisation. Any staff 'caught out' are discretely sent additional refresher training and further resources on how to stay safe. This is the ultimate test of your protection.