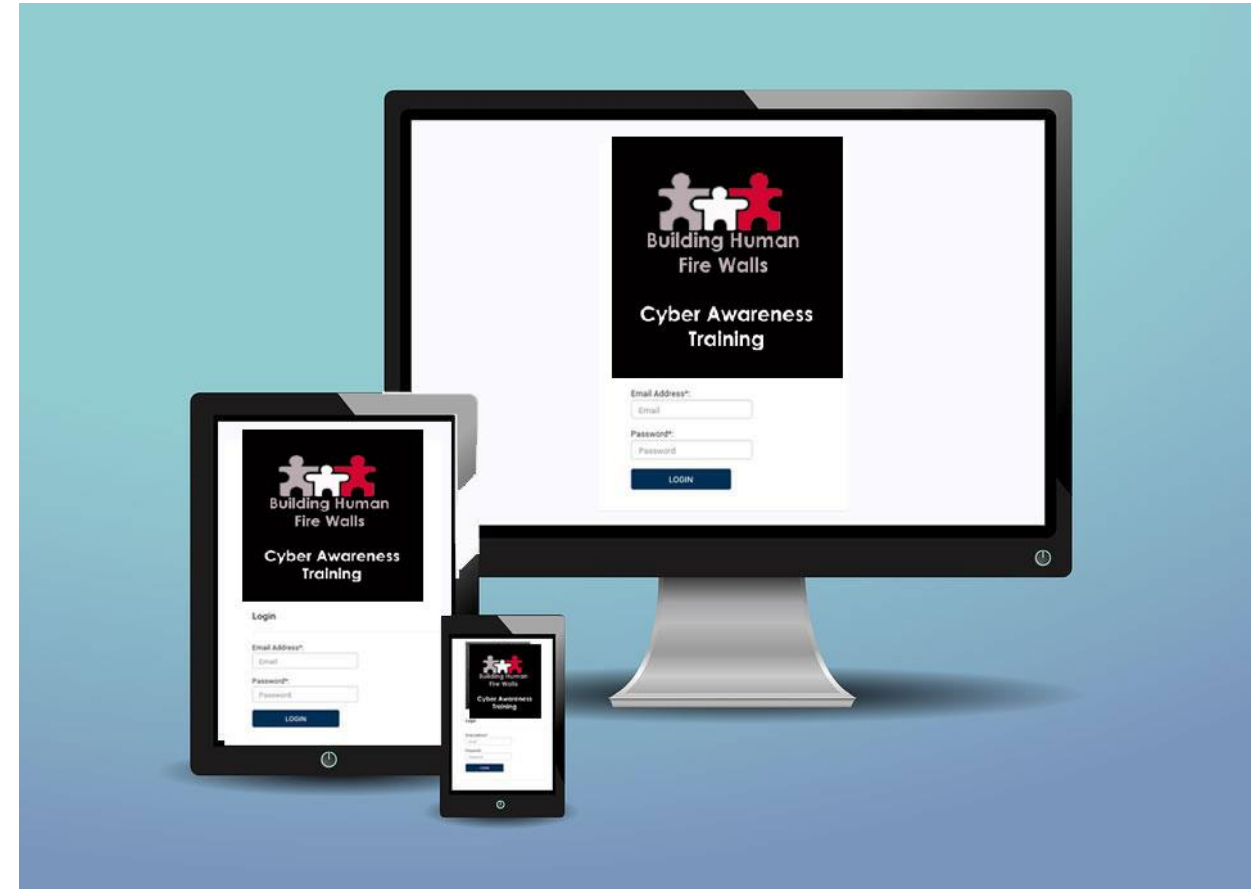


# CYBER AWARE LAB

## A Cyber Awareness Training Programme for General Staff



# Today's Situation

- Although the “technical hack” still occurs (Equifax) security researchers agree most attacks start with individuals being targeted in their email. Many of these attacks cannot be caught by even the most advanced email filters.
- For certain types of cyberattacks, the end user is the only layer of defense. In many organisations, however, the prevailing view among leaders and employees is that IT security is the sole domain of the technology staff.
- Sometimes referred to as the human firewall, a motivated and cyber-aware workforce is as important as any technological defense to the overall organisation staff



- Our aim is to help organisations adopt cyber best practices, encourage confidence in the use of information technology and ultimately, enhance the strength of their human firewall
- Manage your people risk: Up-to-date technology is critical, but it can all be for nothing if companies fail to recognize and control the risk posed by their people. People can make mistakes, fall prey to social engineering attacks, or simply act out of malice. More often than not, it's human error that lies at the heart of major security breaches. Educating your staff on their responsibilities, and on the dangers they face is key.



# THE APP.

- Online web based best practice cyber awareness App for general staff
- An Awareness training program, not technical
- Simple and easy to use
- Training time < 20 minutes
- Progress through course by answering review questions at end of each section
- User can print off Certificate at completion of Course.
- Could be done annually as a refresher.
- Could be reference material

## TRAINING MENU

INTRODUCTION TO COURSE

11/08/2017

EMAIL SAFETY

10/08/2017

THREATS- MALWARE

11/08/2017

THREATS - PHISHING

11/08/2017

BROWSING WEB SAFELY

11/08/2017

PASSWORDS

11/08/2017

PRINT CERTIFICATE

# Training Menu

- Email Safety
- Threats - Malware
- Threats – Phishing
- Browsing Safely
- Passwords Management



## TRAINING MENU

INTRODUCTION TO COURSE

11/08/2017

EMAIL SAFETY

10/08/2017

THREATS- MALWARE

11/08/2017

THREATS - PHISHING

11/08/2017

BROWSING WEB SAFELY

11/08/2017

PASSWORDS

11/08/2017

PRINT CERTIFICATE

# Course Material Updating

- Course material constantly updated
- Identifying the latest hacks and threats



## spam

*Electronic junk mail is commonly known as spam. These are electronic messages you haven't asked for that are sent to your email account, mobile phone number, or instant messaging account.*

*The content of spam messages varies. Some messages promote legitimate products or services, while others will attempt to trick you into following a link to a scam website where you will be asked to enter your bank account or credit card details.*

*The best way to protect yourself from malicious email is to stop it from reaching you. That way, there's no chance it can influence you into doing something you might regret.*



- *Don't share your email address online unless you need to and consider setting up a separate email address just to use for online forms or shopping.*



- *As much as possible, have separate email accounts for personal and business use.*
- *Use a spam filter to catch these messages before they*

# Sample Pages from Course

Back <

Next >



## What you will learn in this Section

Arguably the first step in understanding cyber security is to understand the threats and to do this we need to learn the meaning of several terms that may be foreign to us.

When you have completed this section you will learn what the terms mean and how cyber attacks takes place



## Malware



# Contact Us

Bob Anderson  
Sales Manager  
Business Risk Management Services

M. 0423819663

E. [bob@brmservices.com.au](mailto:bob@brmservices.com.au)

W. [www.brmservices.com.au](http://www.brmservices.com.au)

