



# NEW TECHNOLOGIES & DISRUPTIVE MODELS

Leesa Watego

# STRONG BUSINESS NEED STRONG FOUNDATIONS

Strong Women | Strong Business  
Indigenous Business Australia  
1 - 3 May 2018, Glenelg, Adelaide



Stay standing if you have ever -

**USED THE SAME PASSWORD ON  
A DIFFERENT ACCOUNTS.**

Stay standing if you have -  
**WRITTEN PASSWORDS ON A  
PIECE OF PAPER OR SAVED IT  
ON A WORD DOCUMENT OR  
EXCEL SPREADSHEET  
SOMEWHERE ON THEIR  
COMPUTER.**

Stay standing if you have -

**PASSWORDS THAT A JUST  
NUMBERS AND/OR LETTERS**

Stay standing if you have -

**PASSWORDS THAT ARE JUST A  
MINIMUM NUMBER OF  
CHARACTERS**

**If you are standing you  
need to think about how  
much risk you are  
placing your business in.**


# Top 25 passwords of 2017

- 123456
- Password
- 12345678
- qwerty
- 12345
- 123456789
- letmein
- 1234567
- football
- iloveyou
- admin
- Welcome
- Monkey
- login
- Abc123
- starwars
- 123123
- dragon
- passw0rd
- master
- hello
- freedom
- whatever
- qazwsx
- Trustno1
- 654321
- jordan23
- harley
- password1
- 1234
- Robert
- Matthew
- jordan
- daniel

# Top 25 passwords of 2017

- 123456
- Password
- 12345
- qwerty
- 12345
- 12345
- letmein
- 12345
- footba
- iloveyc
- admin
- Welcome
- Monkey
- Trustno1
- 54321
- Jordan23
- Harley
- Password1
- 234
- Robert
- Matthew
- Jordan
- whatever
- daniel
- qazwsx

**How many Aboriginal  
people will have  
“deadly” as a  
password?**



# 4 best practices for securing your business

# 1. Build good password practices for your team

- Never use the same password twice for anything
- Never use passwords that have some kind of association with you such as birthdays, wedding days or names
- Always use the maximum password length if specified
- If there is no maximum length, then 50 characters is a pretty good starting point
- Always use a mix of lower and upper case
- Always use numbers and special characters when possible.
- Never store passwords in an insecure manner, No plain text files on your computer, no notebook in your drawer




## 2. Use a password manager

- Every password should be unique
- Password manager allows you to only have to remember one password
- Allows for easy logins even when you have multiple accounts for one platform
- If you're going to use 2-step authentication on anything this is the platform that needs it most

LastPass...|





3. Never share  
passwords via  
SMS, Email or  
Facebook

# 4. Write & implement a technology policy that reflects the needs of your business



**Trust in your  
ability to learn &  
adapt.**





**Iscariot**  
Media

[www.iscariotmedia.com/a-strong-business-needs-strong-foundation-keeping-your-business-secure](http://www.iscariotmedia.com/a-strong-business-needs-strong-foundation-keeping-your-business-secure)

