THE 2017 NUMBERS:
CYBER ATTACKS ON AUSTRALIAN SMALL BUSINESS

OVER 1 IN 9 SMBs HAVE BEEN AFFECTED BY A RANSOMWARE ATTACK

MORE THAN 1 IN 3 SMBs DON'T THINK THEY'D LAST A WEEK WITHOUT CRITICAL BUSINESS INFORMATION

MORE COMPANY DEVICES BECAME PASSWORD PROTECTED IN 2017:

CYBERCRIMINALS STUCK TO TRIED AND TESTED METHODS IN 2017

AUSTRALIAN SMALL BUSINESSES CONTINUE TO EXPERIENCE THE SAME TYPE OF CYBER ATTACKS

OF THE BUSINESSES WHO HAD EXPERIENCED A CYBER ATTACK:

54% HAD FALLEN TO AN EMAIL OR PHISHING SCAM

28% WERE THE VICTIM OF A RANSOMWARE ATTACK

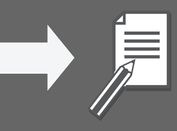
MAIN IMPACT OF CYBERCRIME:

- **39%** DOWNTIME
- **27%** INCONVENIENCE
- **25%** EXPENSE FOR RE-DOING WORK
- **14%** PRIVACY BREACH
- **13%** DATA LOSS
- **11%** FINANCIAL LOSS

BACK UP & RECOVERY

1 IN 5 SMALL BUSINESSES BACK UP THEIR BUSINESS DATA NO MORE THAN ONCE A MONTH

33% ARE RETRIEVING LOST DATA ON AT LEAST A MONTHLY BASIS



INTERNET SECURITY SOLUTION SIGN-UPS INCREASE FROM...

68% IN 2016 TO **87%** IN 2017

13% OF AUSTRALIAN SMBs ARE UNPROTECTED FROM CYBER THREATS

PUBLIC Wi-Fi SECURITY

40% OF BUSINESSES HAVE EMPLOYEES THAT ARE REQUIRED TO TRAVEL OR WORK REMOTELY

26% DON'T TAKE ANY SAFETY PRECAUTIONS WHEN CONNECTING TO PUBLIC Wi-Fi

FROM THE EXPERTS: SECURITY TIPS AND TRICKS

Don't wait until it's too late to know your business

Don't wait until you've been hit by a cyber attack to think about what you should do to help secure your information. Learn the risks, review your business practices and identify security gaps that you can start to address before it's too late.

Invest in security and backup

To reduce the risk of being hit by a cyber attack, implement comprehensive security software such as Norton Security for Professionals or Norton Small Business, and use backup solutions regularly to help safeguard business critical data.

Keep up-to-date

Ensure all your company devices, routers, operating systems, software and applications are always up to date with the latest versions and patches to reduce the risk of being exposed to security vulnerabilities.

Get employees involved

All employees should be vigilant and know how to spot phishing scams, ransomware attacks and be aware of which sites they can visit on their work devices. Small businesses should invest in mandatory training or formal policies to help educate employees so they become your best line of defence against cyber attacks, not your weakest link.

Use strong passwords

Use unique passwords for all your devices, accounts and Wi-Fi networks and routers, change them every three months and don't reuse them. Consider using an online password manager like Norton Identity Safe as an added layer of protection.

To help protect your business, visit **au.norton.com/small-business** today

Norton by Symantec

Source: Norton Australian SMB Cybersecurity Survey, 2017