Australian Government

Australian Signals Directorate

ACSC Australian Cyber Security Centre

Quick Wins

For your Website

Small businesses account for over 95% of all businesses in Australia and 72% of them have a website. However, in a world in which websites are increasingly being targeted by cyber criminals, only 36% check for updates every week. For those small businesses with a website, or that are considering one, these three quick wins will help you protect your money, data and reputation.

cyber.gov.au

Website Wins

Win #1

Use HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is used to send data between a web browser (Chrome, Firefox or Safari) and a website. It uses encryption to increase the security and privacy of data transfers.

HTTPS also improves your Google search ranking – a reward for adding security.

Soon, some web browsers will mark non-HTTPS websites as "not secure" in the URL bar, marking the URL red.

You might explore and set up HTTPS yourself via free and automatic options, such as **Let's Encrypt**, or direct your website developer to our **PROTECT** publication Implementing Certificates, TLS and HTTPS guidance (available at **cyber.gov.au**) and ask them to set up HTTPS.

Win #2

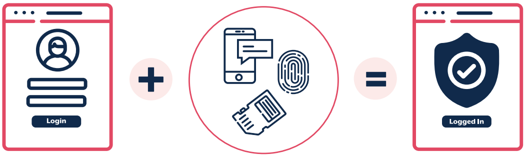
Update your website's content management systems, plugins and programs

If you are using a web hosting provider, contact your provider to make sure they are keeping your content management system and any plugins up to date. They should also send email notifications detailing any website security issues.

Win #3

Secure your access to your website – Multi-factor Authentication and Passphrases

Ideally, your web hosting provider should offer multi-factor authentication to significantly increase the security of your access to a website (refer to the **Step-by-Step Guide to Turning on Multi-Factor Authentication**, available at **cyber.gov.au**).



Using only strong passphrases for your server and website administration areas is an easy, quick win. Wondering what a strong passphrase looks like? See the table below:

PASSWORD/ PASSPHRASE	DIFFICULTY TO BREAK	EASY TO REMEMBER	COMMENTS
password123	Very easy (too easy)	Very easy (too easy)	One of the most commonly used passwords on the planet.
5paghetti95	Easy	Somewhat easy	Not too much more complexity than above with character substitution, and still short length. Easy to remember, but easy to crack.
I don't like pineapple on my pizza!	Hard	Easy	Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very difficult to crack.

For more on creating secure passphrases, refer to the ACSC's **Small Business Cyber Security Guide** https://www.cyber.gov.au/publications/small-business-cyber-security-guide.

ACSC Australian **Cyber Security** Centre

For more information, or to report a cyber security incident, contact us

cyber.gov.au

☎ **call 1300 CYBER1 (1300 292 371)**