Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

QUICK WINS FOR YOUR WEBSITE

cyber.gov.au

Having an online presence is important for many businesses. With so much commerce now taking place online, websites are critical – making them a prime target for a cyber attack. Protect your website from cybercriminals with these three cyber security wins.

Website Wins

Win #1

Use HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is used to send encrypted data between a web browser (e.g. Chrome, Firefox, Edge or Safari) and a website. This encryption provides security for sensitive information such as passwords and credit card details, as well as privacy of the content you visit online.

HTTPS improves your website's ranking in Google searches – a reward for being secure.

To check if your website is using HTTPS, look for 'https' at the start of the URL:

- ✓ https://www.example.com
- × http://www.example.com

For websites that don't use HTTPS, many web browsers now tell users that the website is "not secure" and will warn them not to enter any sensitive information.

You can explore and set up HTTPS yourself via free and automatic options, such as **Let's Encrypt**, or direct your website developer to our publication *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* (available at **cyber.gov.au**) and ask them to set up HTTPS and renew certificates automatically before they expire.

Win #2

Secure your website's content management systems and plugins.

Ensure that your website's content management systems and any plugins are updated regularly to address security vulnerabilities. If your website is managed by a third-party or external provider, contact them to discuss regular patching and updates.

Win #3

Secure access to your website using multi-factor authentication (MFA)

Ideally, your web hosting provider or content management system should offer multi-factor authentication (MFA) to increase your website's security and protect it from unauthorised access.

Enable MFA for your website administration accounts and servers, where possible.

If MFA is not available, use a passphrase to secure website administration accounts. A passphrase uses four or more random words as your password, e.g. "crystal onion clay pretzel". Passphrases are hard for cybercriminals to guess, but easy for you to remember. Make sure your passphrase is unique – do not reuse it elsewhere.

For more information about **MFA and passphrases**, or cyber security advice for your business, visit **cyber.gov.au**

Securing e-commerce websites

Any Australian business that accepts card payments needs to comply with the Payment Card Industry Data Security Standards (PCI DSS), regardless of business size.

If your website is an e-commerce website that accepts card payments, ensure your business is PCI compliant.

If your e-commerce website uses a payment gateway provider to process transactions, ensure they are also PCI compliant.

Meeting these cyber security standards will help you protect your data and customers' information from breaches and theft.

For more information visit **business.gov.au**.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2023
With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371).

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre