

Introduction

For small businesses, having a secure website is not just about maintaining a professional image - it is essential for protecting your business and your customers. With cyber threats evolving, it is important to ensure your website is protected against attacks that could compromise sensitive information, damage your business reputation, or lead to financial loss.

Guidance note:

This fact sheet provides general advice and guidance about protecting some of the more common web platforms available (such as WordPress, Shopify, Wix etc.). Prior to making any changes, we recommend backing up your website to ensure that if something goes wrong, you can revert to a previous version. Before implementing any addons, plugins, or extensions to your website, it is best to ensure that you do some research on what you are installing and whether it is reputable and compatible. *Please note that IDCARE does not have any financial interest in these organisations, and they are recommended solely in the interests of supporting your businesses' cyber resilience.*

Securing your website:

Securing your business website is crucial, regardless of the platform you use. Whether your site is built with WordPress, Wix, Shopify, or custom code, the following best practices can help protect your business, data, and customers.

1. Securing your website management login:

Make sure your website login details are complex and unique, as this will reduce the risk of unauthorised access.

Our advice:

Implement a long, sophisticated and unique password.

- ☐ The **length and sophistication of a password** will assist in reducing the likelihood of scammers breaching your website management software.
- ☐ The **uniqueness of a password** will protect your website if non-related data breaches reveal passwords that aren't similar or the same to your website login.
- ☐ For more information, please refer to our [Password Manager Fact Sheet](#)

- ☐ **Enabling multi-factor authenticator** (MFA) on all accounts when possible. If you can, enable multi-factor authenticator on your admin login.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

2. Regularly backup your website

Backing up your website means storing copies of your site's files and database so you can restore it if it's compromised. If you use a website builder (such as those listed below), exploring the settings or admin panel may let you set these up automatically.

Our advice:

- ☐ Use a backup service offered by your hosting provider or a third-party plugin/tool. Ensure backups are automatic and stored separately from your live site.

Specific advice regarding common platforms:

WordPress:

- ☐
 - Backup Plugins: use plugins like 'UpdraftPlus', 'All-in-One WP', or 'BackWPup' to automate regular backups. Store backups offsite, such as in cloud storage.
 - More information can be found on the [WordPress developer webpage](#).

Shopify, Wix, Squarespace:

- ☐
 - Automatic Backups: some platforms provide automatic backup options – check under your site's settings. Alternatively, use third-party apps like Rewind for Shopify
 - For more information – see online content for [Shopify](#), [Wix](#) and [Squarespace](#) in relation to website backup procedures. Note that in the Wix page, it is clearly stated that backups occur automatically, while for Squarespace, the only option is to keep a duplicated copy of the site.

3. Use HTTPS and an SSL certificate

HTTPS ensures that data transmitted between your website and users is encrypted, protecting sensitive information like passwords and payment details.

Our advice:

- ☐ Purchase and install an SSL certificate from a trusted provider or check if your web host offers it for free. This will automatically upgrade your site to HTTPS.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Specific advice regarding common platforms:

WordPress:

- ☐
 - **Free SSL certificates:** Many hosting providers offer free SSL certificates via **Let's Encrypt**. You can also use plugins like **Really Simple SSL** to enforce HTTPS across your site.

Shopify, Wix, Squarespace:

- ☐
 - **Automatic SSL:** SSL is automatically provided with your plan. Make sure your site settings enforce HTTPS and check your dashboard for any certificate errors.

Custom-built websites

- ☐
 - **Install SSL via hosting provider:** Acquire and install an SSL certificate through your hosting provider's control panel (e.g., cPanel). Update your .htaccess or server configuration to force HTTPS.certificate errors.

4. Keep software, plugins, and themes updated

Outdated software, plugins, or themes can create vulnerabilities that cybercriminals exploit. It is important to keep plugins and software up to date with the latest security and enable automatic updates where possible.

Our advice:

General Best Practices – Keeping Plugins up to date

- ☐
 - **Regular Monitoring:** Set a schedule to check for updates, either weekly or bi-weekly, depending on the complexity of your site and the number of plugins.
 - **Use Security Plugins:** Install security plugins (e.g., Wordfence for WordPress) that monitor your site for outdated plugins and alert you when updates are needed.
 - **Backup Before Updating:** Always back up your site before performing any updates, especially for critical plugins or apps, to ensure you can restore it if anything goes wrong.
- ☐ Use malware scanning tools or services available through your web host or install security plugins that provide scanning features.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Specific advice regarding common platforms:

WordPress:

- **Dashboard updates:** Go to **Dashboard > Updates**. WordPress will show you if any of your plugins have updates available. You can select all and update them in bulk or individually.
- **Plugin page:** Navigate to **Plugins > Installed Plugins**. Each plugin that needs an update will display a notification. Click on Update Now next to each one.
- **Automatic updates:** Enable automatic updates for plugins to keep them current without manual intervention. In the plugin list, click **Enable Auto-Updates** next to the plugins you want to keep automatically updated.

Shopify:

- **App updates:** Shopify apps (plugins) update automatically in most cases. However, some apps may notify you if manual updates are needed. Check the **Apps** section in your admin dashboard for any update alerts or messages.
- **App developer support:** If an app doesn't update automatically, contact the app developer through the **Apps** section for guidance. It's also a good idea to check if the app is still supported and maintained regularly.

5. Limit access and permissions

Controlling who has access to your website's backend and limiting their permissions can reduce the risk of unauthorised changes or data breaches.

Our advice:

- Assign roles carefully (e.g., admin, editor, viewer) and only give access to those who need it, this is called the Principle of Least Privilege. A person should only have enough access to do their job, nothing more. Regularly review this and ensure you have revoked access for former employees or unused accounts.

WordPress:

- **User Roles and permissions:** Use the built-in **User Roles** feature to assign minimum necessary permissions. Install plugins like **User Role Editor** for more granular control.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Shopify, Wix, Squarespace:

- ☐ **Admin and staff permissions:** Platforms allow user roles with varying permissions. Adjust these under **Settings > Staff/Users** to limit access to sensitive functions.

Custom-built websites

- ☐ **Access control:** Implement role-based access control (RBAC) in your application. Set permissions in your server environment (e.g., SSH, FTP) to restrict file access.

6. Install a firewall and use security monitoring tools

A web application firewall (WAF) helps block malicious traffic, while security monitoring tools scan for vulnerabilities or suspicious activity.

Our advice:

- ☐ Many hosting providers offer WAF services, or you can use third-party solutions. For further information, please contact your provider. Additionally, install security plugins or monitoring tools specific to your platform to receive alerts and reports.

Specific advice regarding common platforms:

WordPress:

- ☐ **Firewall plugins:** Plugins like **Wordfence** or **Sucuri Security** offer firewall functionality. Install and configure them to monitor and block malicious traffic. Additionally, Cloudflare have some great content on [improving WordPress security](#).

Shopify, Wix, Squarespace:

- ☐ **Third-party services:** Use services like **Cloudflare** for firewall and monitoring protection. These services operate independently of platform constraints and monitor traffic and vulnerabilities.

Custom-built websites

- ☐ **WAF integration:** Services like **Cloudflare** or **Sucuri** can be integrated with your site. You may also install and configure a firewall directly via your server's control panel (e.g., cPanel, Plesk).

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

7. Additional information

Keeping yourself and your business up to date with the latest advice and scam techniques. Here are some resources you can use:



- Australian Cyber Security Centre ([ACSC](#))
- IDCARE's [Cyber Sushi](#)

The ACSC also has some guidance surrounding:



- TLS, HTTPS and encrypting web and email traffic. View their guideline [here](#).
- DNS and Security. View their guideline [here](#).
- Preparing and responding to DDOS attacks. View their guideline [here](#).
- ACSC's guide on how to [secure your website](#).

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.