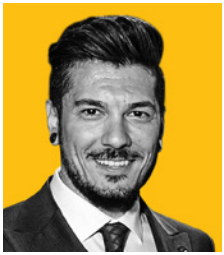

FELIX ZEVKLI, *Founder, Social Force*
LinkedIn https://www.linkedin.com/in/felixzevkli/

Felix has led an impressive career as a digital marketer and a young entrepreneur that spans over 10 years. In 2019, his company Social Force was nominated for the Best Marketing Agency in Australian Small Business Champions Award 2020 & 2021. He was recently WA winner for Australian Achiever Awards 2021 in the Advertising, Marketing & Public Relations Services category. Felix is a big believer in supporting the community.

TIP 1. PROTECTING YOUR WEBSITE

Every interactive element on your page – filling out forms or uploading files – is a potential security breach and requires additional technical protection. If the public can talk back to you, you have to be sure that they are not giving instructions to your computers. To combat this, consider requiring your customers/users to sign in with a password and multi-factor authentication.

TIP 2. BACKUP YOUR SITE REGULARLY

Backing up your site, routinely, is a safety precaution that will make your life easier if hackers do find their way into your site. By having a recent copy of your site, you'll be able to easily restore your content before it was compromised and won't be stuck in the position of trying to figure out what to do next.

TIP 3. AUTHENTICATE YOUR EMAIL

Some web host providers let you set up your company's business email using your domain name (that's part of your URL, and what you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. If you don't have email authentication, scammers can impersonate that domain name and send emails that look like they're from your business. When your business email is set up using your company's domain name, make sure that your web host can give you these three email authentication tools:

- Sender Policy Framework (SPF).
- Domain Keys Identified Mail (DKIM).
- Domain-based Message Authentication, Reporting & Conformance (DMARC).

TIP 4. DON'T USE NULLED MODULES

Avoid using modules, extensions, themes and scripts, downloaded from non-official sites and torrents. In almost all cases, such scripts contain backdoors and malicious code. Always download the extensions and the templates for your sites only from the official developer sites.

TIP 5. SECURE YOUR LOCAL COMPUTER

If your computer is infected with a virus, or malware software, a potential attacker can gain access to your login details and make a valid login to your site, bypassing all the measures you've taken before. This is why it is very important to have an up-to-date antivirus program and keep the overall security of all computers you use to access your website on a high level.

For this purpose, use reliable updated antivirus software such as:
Norton Internet Security, offering Antivirus, Antispyware, Two-way firewall, Antiphishing, etc.
or Bitdefender Antivirus Plus, which is the Bitdefender's entry-level antivirus software offering, making it ideal for home users without technical skills and anyone who wants basic defence against threats.

TIP 6. KEEP THEMES, PLUGINS, AND WORDPRESS UPDATED

Updates can be a pain to keep up with, especially if you have lots of plugins installed on your WordPress site. But it's critical that you try. Themes and plugins can occasionally have security vulnerabilities, which are patched by the developer as soon as they're discovered. It's important to update regularly because many malicious bots specifically search for out-of-date plugins and themes with known vulnerabilities. Plus, updates often patch other bugs and enhance usability, so it's a win all around!

TIP 7. UNINSTALL INACTIVE PLUGINS AND THEMES

Even deactivated plugins and themes can have vulnerabilities and, for that matter, can still take up your server's resources. It's best to simply uninstall any plugins or themes that aren't consistently active. If this idea stresses you out, just remember: You can always reinstall themes or plugins later if you need to.

TIP 8. ADD CATPCHA TO YOUR WEBSITE

There are several variants of Captcha out there, but the idea is the same between plugins and methods: force any site visitor who tries to fill out a form to first prove they're human. While it was once a troublesome and inconvenient option, Captcha has improved greatly in recent years. Plus it protects all kinds of forms on your site, so it does double duty by helping to stop hackers and prevent spam.

TIP 9. USE TWO-FACTOR AUTHENTICATION

Another way to prevent brute-force login attempts is by setting up two-factor authentication.
This method requires two verifications – a password and an authorisation code sent to your phone or email – to log in. While it takes a little more time for people you trust to log in, it also makes it a whole lot harder for people you don't trust to gain access to your site. You can add two-factor authentication to your website login, and some hosts offer it for your hosting account as well. Two-factor authentication takes a little time to get used to it, but it's worth it in the long-run!

TIP 10. USE CLOUDFLARE CDN

This is more of an advanced option, and certainly not one that everyone needs, but CloudFlare is an external service that acts as a sort of "filter" between your servers and your users. CloudFlare offers many security and performance options, several of which are available on their free plan. While most sites don't need to worry about DDOS attacks, CloudFlare is excellent at preventing those, since your server's IP address will be effectively masked. CloudFlare also offers a variety of other security options, including blocking IP addresses or specific regions.