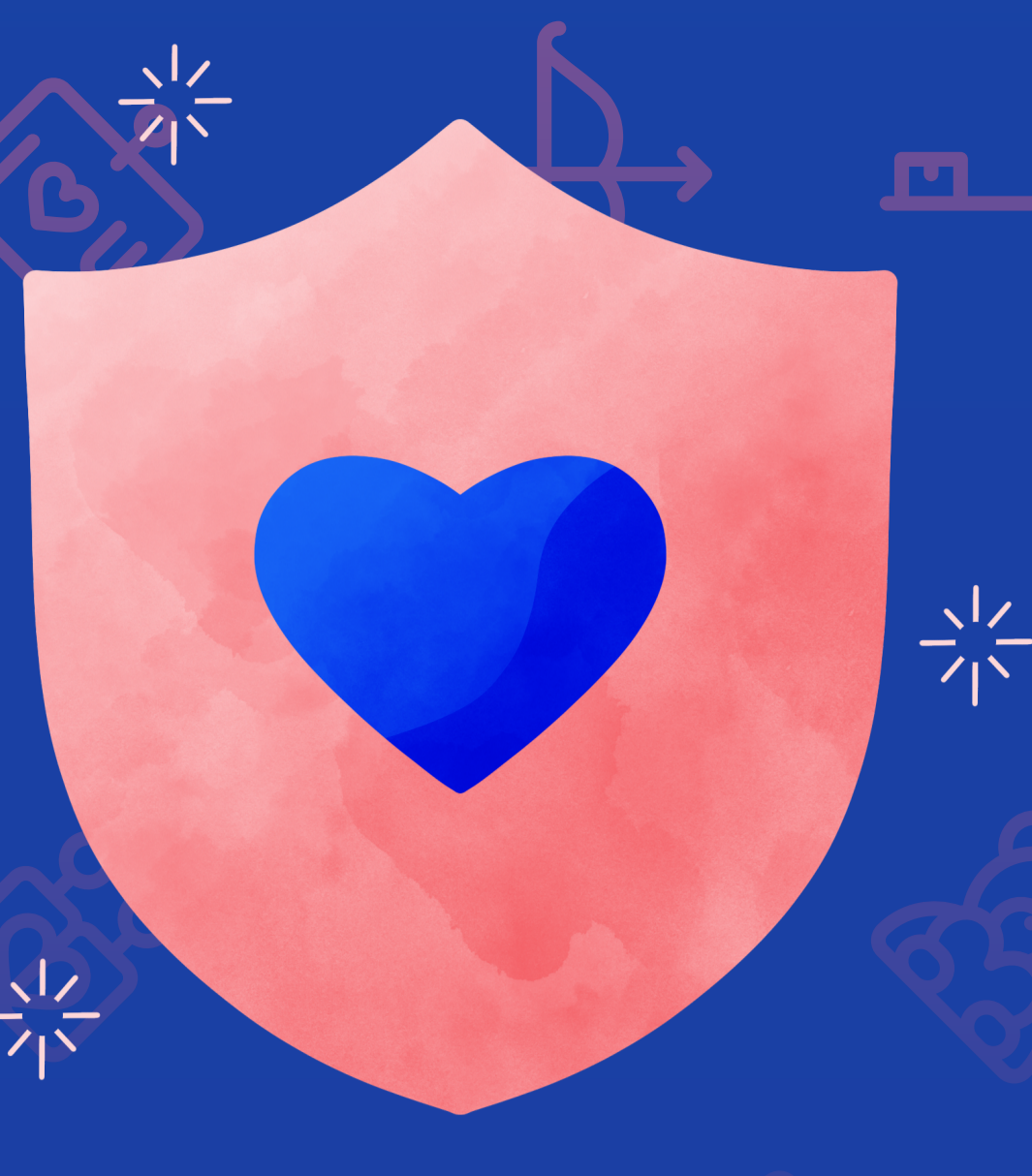


Love means putting safety first

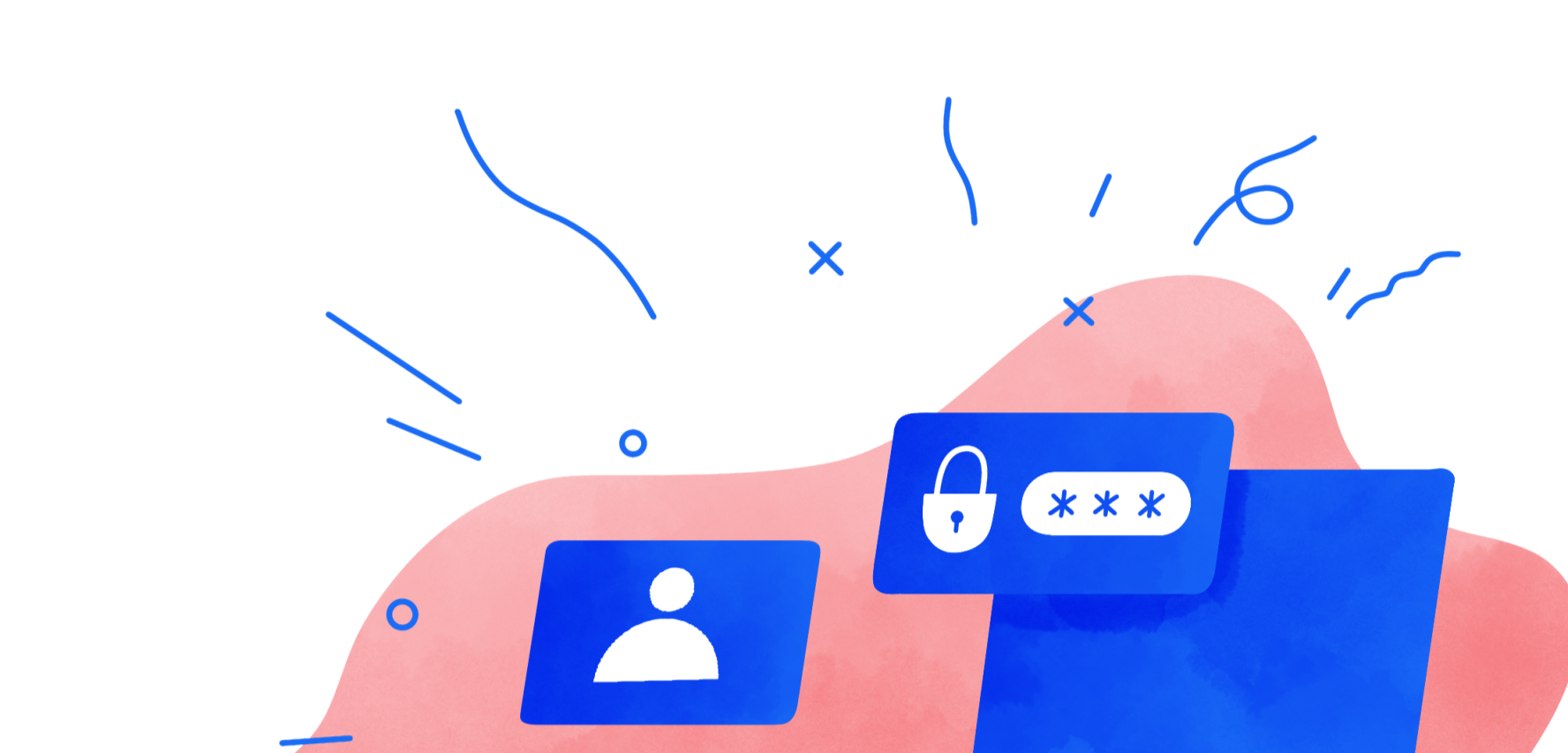


Many website owners still neglect basic safety measures because they think that hacker attacks will never happen to them. And this is a huge mistake.

60% of websites were vulnerable to malicious attacks in 2019, which is 4% more than in 2018



Taking precautionary measures will help you ensure the only thing transmitted through your website is encrypted data—not viruses. And so it will prevent hackers—aka the third wheel—from ruining your relationships with your partners.



Encourage prevention



We all know that using complex passwords is a simple yet important preventive measure—doing otherwise means basically inviting hackers to break into your account. To keep your users' accounts safe, ask them to create strong passwords like eight characters with uppercase letters and numbers. And make sure you store them as hashed values.

Make your connections safe



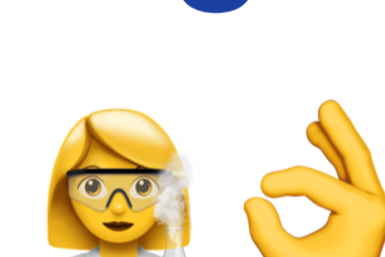
Getting an SSL certificate will let you switch to HTTPS, which is more secure. The combination of an SSL certificate and HTTPS ensures that all the data transmitted between your server and users' browsers is securely encrypted. You may already have the secure mode icon next to your website, as it is now the industry standard. If not, don't lag behind and get one ASAP.

Always carry barrier protection



Consider using a website firewall not to stay up at night worrying about the most common attack types including SQL injections and cross-site scripting. A website firewall works like a shield, warding off hacker attacks, by constantly monitoring and analyzing all the traffic coming in and out of your website server.

Get tested regularly



Taking precautions doesn't mean you're 100% safe. You still need to regularly test your website's health using a combination of automated detection tools and manual reviews. And if you have no clue how cross-site scripting is different from cross-site request forgery, don't feel ashamed and ask for professional help.

Gotta stay fit



Keep your website clean and your software up-to-date. Hackers often target popular web software aiming to find a security flaw and take down thousands of websites at a time. When a software update is released, it often fixes some security lapses. So make sure to install it immediately so that your website isn't vulnerable to attacks.

Always have a backup plan



The final precaution you need to consider is regularly backing up all the data, both on-site and off-site. That way, if your website gets infected in spite of all the preventive measures, recent backups will help you recover.

Keep an eye on the expiry date



To make your partnerships last, you'll have to remember important dates. Like your partners' business anniversaries or the date your domain expires. Luckily, this problem is easily solved via reminders.

If you truly cherish your customers and want to build partnerships based on trust, keeping your website clean is the only way to go. With strong protection in place, hackers won't be able to penetrate your website and get their hands on your customers' sensitive data.