The padlock may not mean the site you are using is secure - see below:

When you visit a website in a browser, it’s long been advised that you check for the green padlock icon next to the web address in the URL bar to indicate that you’re visiting a secure site. However, as cybercriminals and hackers are also using security features — for the nefarious purpose of tricking you — that security advice no longer holds true.

Cybersecurity researchers at [PhishLabs](https://www.phishtank.com/) reported that nearly half of all fraudulent websites are also using the green padlock symbol in the URL bar, with the hope that you’ll be fooled into thinking that you’re in fact visiting a legitimate and secure site. And because many web surfers have been trained into believing that the green padlock logo indicates that a site is safe, the number of fraudulent websites adopting the padlock has increased from 24 percent in 2017 to nearly 50 percent in 2018.

When a browser shows the green padlock in the browser bar, it means that a site is sending information over an encrypted connection. That doesn’t mean that only legitimate sites will have access to the padlock logo, but it does mean that you should not enter private information — like credit card or Social Security numbers — on a site lacking that logo. However, given that hackers are getting more sophisticated, you should also do more research and make sure you’re actually on a legitimate website even when you do see a green padlock.

When you’re visiting a fraudulent website with a green padlock, it means that the information you’ve entered will be transmitted over an encrypted connection. But instead of going to your favourite e-commerce site to make your purchase, your credit card details will be transmitted securely to a hacker phishing for your information.

Researchers cite cheaper access to encrypted connections as one reason for the rise in fraudulent websites with the green padlock. “Criminals can now easily obtain certificates that enable the padlock to show up and encryption to take place, and they can do it without revealing very much about who they are,” [CNET](https://www.cnet.com/news/scam-websites-are-using-that-green-https-padlock-to-fool-you/) reported.

The increased use of the green padlock may also stem from publicity around the feature. Popular browsers like [Google’s Chrome](https://www.digitaltrends.com/computing/https-google-chrome/) or Mozilla’s Firefox began flashing red warnings to users when they visited an unsecured site, which is often noted with an HTTP rather than an HTTPS prefix.