EFF’s HTTPS Everywhere Added to ExpressVPN Chrome Extension, Offering More Secure Browsing

Extension provides users with greater online security by ensuring connections to sites are encrypted

TORLOTA, British Virgin Islands (PRWEB) June 19, 2018 -- ExpressVPN, a leading international consumer VPN provider, today announced that it is adding functionality from the Electronic Frontier Foundation (EFF) HTTPS Everywhere to the company’s VPN Chrome extension. With this latest update, the ExpressVPN extension will provide users with stronger protection against having their online activity and data monitored, tampered with, or hacked.

Nine in 10 Americans worry about online privacy and data security, particularly identity theft (54 percent) and credit card fraud (16 percent), according to a survey of 1,000 U.S. adults age 18+, conducted online by Propeller Insights on behalf of ExpressVPN in April 2018. However, many internet users find protecting themselves online to be complicated and confusing. The ExpressVPN Chrome extension provides them with multiple layers of privacy and security protection, including HTTPS Everywhere and VPN connectivity, in one easy-to-use package.

Developed by EFF, a leading non-profit that defends digital privacy and free speech, HTTPS Everywhere automatically redirects browser traffic to the HTTPS version of thousands of major websites, encrypting the connection with those sites and providing significantly more security than the standard HTTP.

“With news of privacy violations and data breaches on the rise, it’s clear that online privacy and security have never been more important and that strong encryption is critical. Together, HTTPS Everywhere and ExpressVPN provide users with greater confidence that their internet activity and personal data are encrypted and protected,” said Harold Li, vice president, ExpressVPN. “As long-standing supporters of EFF and their fight for digital rights, we’re proud to be able to bring the benefits of its HTTPS Everywhere project to our users.”

HTTPS provides users with the confidence that the traffic between them and the site they are visiting is encrypted and that the site is really the one that they intended to connect to. While the HTTPS protocol is decades old, many sites and internet users alike are still relying on the less secure HTTP. ExpressVPN is among several major internet companies working to ensure broader adoption of the standard. As of July, Google Chrome will prominently label all HTTP pages as “not secure.”

Connecting to a VPN in addition to using HTTPS further enhances a user’s privacy and security by channeling all traffic through a secure tunnel. This helps guarantee that online activity is protected by encryption even if a site does not fully support HTTPS. It also prevents hackers or internet service providers from seeing what sites the user is visiting, which HTTPS alone does not conceal—particularly relevant in the post-net-neutrality world.

About ExpressVPN
One of the world’s largest providers of VPN services, ExpressVPN enables users worldwide to protect their privacy and security online with just a few clicks. The company's award-winning apps for Windows, Mac, iOS, Android, Linux, routers, and browsers secure user information and identities with best-in-class encryption and
leak-proofing. With 2,000+ servers across 94 countries and new servers added each week, ExpressVPN provides a fast connection wherever you are and offers uncensored access to sites and services from across the globe. ExpressVPN is based in the British Virgin Islands and has been operating since 2009.

A vocal advocate for internet freedom and privacy, ExpressVPN is a proud financial supporter of non-profit organizations fighting to protect digital rights, including the Electronic Frontier Foundation, the Internet Defense League and OpenMedia.

To learn more about ExpressVPN’s privacy and security solutions, visit expressvpn.com.
Contact Information
Alessandra Nagy
Bospar
+1 (714) 310-4439

Online Web 2.0 Version
You can read the online version of this press release here.