Top 10 Reasons You Need SSL

1. **Meet the New Industry Requirements**—Browsers now display "Not Secure" warnings on all unencrypted connections. The CA Security Council reports only 2% would proceed past untrusted connection warnings and only 3% would give credit card information without the padlock icon. According to an Ipsos Group 2018 study, 87% of users won't complete transaction if they see a browser warning. 58% will go to a competitor to complete their purchase.

2. **Gain Visitor Trust & Confidence**—Online, your brand reputation is everything. SSL shows visitors their safety is your priority and provides visual trust indicators that create instant trust.

3. **Maximize Conversions**—With abandonment rates as high as 75%, you need to do everything you can to gain visitor confidence. HubSpot reports 84% of people won't make a purchase on an unsecured website.

4. **Boost Search Ranking & Traffic**—Top visibility on search engine results pages is the first step to gaining new visitors. As of August 2014, Google gives sites with SSL certificates as much as a 5% boost in ranking.

5. **Unlock Popular Mobile Features**—Salesforce reports 71% of companies believe mobile is core to their business. Mobile's most popular features—geolocation, motion orientation, microphone, full screen and camera access—require HTTPS to be enabled by most browsers.

6. **Speed Up Site Performance**—HTTP is being replaced by a newer, faster version, HTTP/2. Encrypted connections are required to unlock the latest speed and security features.

7. **Satisfy GDPR Compliance**—GDPR went into effect May 25, 2018, and breach penalties are steep at €20 million or 4% of annual turnover, which is higher. Plus, there may be additional fines based on type of breach, data exposed, response, etc. And that doesn't include damage to reputation or legal fees. Some of the requirements in this 99-article regulation can only be accomplished with SSL certificates.

8. **Satisfy PCI Compliance**—SSL certificates play an important role in meeting PCI requirements. Here are just a few SSL-related issues that can cause you to fail a PCI compliance scan if they're not resolved:
   - Using expired SSL certificates
   - Using non-publicly trusted SSL certificates in the wrong areas
   - Using lower than 256-bit encryption
   - Using outdated TLS protocol

9. **Protect Against Phishing Attacks**—According to PhishLabs Q3 2018 report, nearly half (49%) of phishing sites appear safe to visitors because they use Domain Validation (DV) certificates. PhishLabs reports sites protected by premium certificates (Organization Validation/OV and Extended Validation/EV) are 93 – 97% safer than encryption-only DV sites.

10. **Minimize Data Breaches**—According to the 2018 Global Threat Report, 70% of company's report suffering at least one data breach. The first half of 2018 saw 4.5B records stolen (291 every second) and only 1% were encrypted. Verizon's Data Breach Investigation Report cites lack of encryption and security when handling confidential information among the top causes of breaches. If you suffered a breach, wouldn't you at least want to make sure the data couldn't be decrypted? Not having an SSL certificate increases your risk of a data breach.

3220 Executive Ridge Drive, Suite 101, Vista CA 92081