Appendix 4: Security

No website can ever claim to be 100% unhackable, but we never stop working to ensure the security of your data. Here’s how:

Encryption At Rest

www.theIDRegister.com runs on an encrypted SQL Server database. data is stored in discrete file blocks that are fragmented and encrypted using 256-bit AES. That means that the cipher encrypts and decrypts data in blocks of 128 bits using cryptographic key 256-bits. That would take you more that 1 billion years of supercomputer time to decrypt using brute force. In short, our database is useless to anyone who does not have the encryption key.

Secure Webservice

From the database, your information travels through our web servers and code. These run on the Microsoft Azure platform https://azure.microsoft.com/en-us/support/trust-center/ . Microsoft employs intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the Azure platform. In a landmark ruling on 15th July 2016, the US Supreme Court ruled that the US Government cannot access data held on platforms like Azure when they are hosted overseas. We at the ID Register also penetration test our site annually using independent, ethical hackers for an extra level of assurance. You can find their details on the landing page of our website.

Encrypted Transmission

As the data travels between our web servers and your browser, we encrypt it in an ‘Secure Socket Layer’ (SSL) tunnel. Once your browser connects to our servers, all information passing to and from your browser is scrambled by 256-bit encryption that's virtually unbreakable by hackers. In fact, the least secure part of this journey is the transmission of the data from the screen to your eyes.

GODADDY.COM
VERIFIED & SECURED

The Human Factor

So, our web service is monitored 24/7 to protect against every kind of attack that we can imagine. That is considerably more secure than the equivalent manual process, where information is stored in unsecured PDFs and spreadsheets, certified documents are kept in boxes and filing cabinets and communications are sent by email. Moving this information to an encrypted, protected and continuously monitored service is helping to bring CDD security into the 21st century.