

building websites that **penetrate corporate firewalls**

The web is cluttered with information - lots of it all over the place. Each and every one of us now has the ability to publish our own content through websites and Blogs, or on our favourite social network and technology has played a massive part in making this happen.

Video, Javascript, Flash, Ajax, etc. have left us with web platforms where we can actively take part in the discussion happening online.

But, marketers also want to use this same technology on their business websites with feature rich 'experiences' that engage people, like interactive navigation that pops up when you roll over it and embedded Flash videos - basically wizzy features that use the technology to impress visitors.

But, is that what the user really wants in the business to business environment?

Gatekeepers

One group of people this approach certainly doesn't impress are network administrators who also have an increasingly comprehensive array of tools to counteract the increased drain on bandwidth that this new technology requires. That is on top of the possible virus and spam attacks and the requirements of the HR department looking to reduce wasted hours at work from employees visiting non-work related websites.

The question is, where does your business website stand when it comes to corporate network penetration and your ability to market to, and actually reach, people working in large organisations?

Some local government agencies even have an "off before on" policy, where all websites are black-listed until they are requested, whereupon the website is assessed as to whether it is business related, trusted and safe.

"In a recent conversation I had with a UK government employee I was told that their organisation policy is biased towards the safety of the network over the personal need of that person to access a website that would help them do their job more effectively."

As much as this causes issues for marketers, the approach does make common sense for large companies. On the read/write web, why should corporations and public organisations be forced to accept your b2b website up-front online without any qualification or vetting process, when it could actually be costing their business money or, even worse, be a threat to their network security?

Of course, you will always have variables, such as the quality of the network administrator, the specific policy in place (which differs between companies) but the question is... **How do you create a website that is not only engaging for a user, but also complies with many large company network policies?**

Content rules

The key to remember is that the web is all about content. Yes, this may sometimes involve images and video, but more often than not, the real content - the stuff people need - is just plain old words with the images and 'features' there as icing on the cake. And, does every cake need icing?

Ask Jakob

Jakob Nielsen is one of the foremost authorities on web usability. His website (www.useit.com) is testament to this philosophy of content being the number one 'feature' of a website. His site is

packed with quality information, resource clean and loads very quickly. This reduces bandwidth requirements for the user and therefore is not a large drain on a corporate network.

Compare this with a tool like Facebook: Resource heavy, with plenty of supplementary code - very engaging on a personal level - but a large drain on resources, and probably gets blocked on many counts by organisations large and small. The BBC has just relaunched their new web interface and are facing the same challenges.

Guidelines for building web pages that penetrate corporate firewalls

- The content is the main focus. Make sure it is clean and clear and uses appropriate wording. Automated network gatekeepers may filter your website if it uses words that are recognised as unsavoury. This includes any alt text on images and sometimes takes into consideration the names of the tags in your code (Div tags, classes, etc.).
- Bias all important aspects of your web page to text. This also includes call-to-actions. Some firewalls may load your content, but not images and additional scripts. If the main message can still be understood, with the supplementary 'icing', you still have a chance of penetration.
- Split your website styling from the content by using CSS. This means that your page content is cleaner and more efficient and may still get through.

Alternative websites

If you have a website structure that does not allow for scaled back approach, why not create micro sites that are clean and to-the-point - being careful not to duplicate content from your main site as this may affect your search rankings.

Another more basic, but highly effective, approach is to **simply make your website as useful as it can be to your target market**, especially within vertical markets. If they "need" your website and it doesn't pose a threat, the value should fall in your favour.

The e-mail approach

E-Mail is a good barometer of the future of the web, with opt-in permission being the key to effective e-mail marketing. That, and the user having the control over two key aspects of the relationship:

1. How they receive your information - HTML or Text only (iced or plain)
2. The ability to unsubscribe from your communications

The future

There is much speculation about the future of the Internet and there is already discussion about a two-tiered Internet; one of which is a jungle, the other of which has quality information that you will have to pay for.

With so much general clutter on the web, perhaps it is time **now** to start scaling back on features, cleaning things up and focussing on what people really want - especially when marketing a business to large organisations on the web.

The Escape

Loddon Business Centre, Roentgen Road, Basingstoke, Hampshire RG24 8NG. United Kingdom
t: +44 (0)1256 334567 f: +44 (0)1256 470700 e: ideas@the-escape.co.uk

www.the-escape.co.uk

theESCAPE®