"Fake" colleges

There has been a resurgence of "fake" websites that infringe upon the intellectual property of our customers. Their name and brand may be misused, the design of their site may have been copied, or the website may be trying to masquerade as them. In some cases the legitimacy of the organisation running the site may be in question.

When dealing with theses sites it is useful to break them down into several groups. This helps decide which approach will be most effective at resolving any issues. This is not meant as proscriptive and the sites can fall into several of these groups. Mixed approaches are often most successful.

1. Sites that pose immediate operational threats

These sites undisputedly masquerade as another institution and are used as part of a technical attack. They may also be used to gather personal information from prospective students, phish existing students and staff, spread malware and manipulate search results.

Responsible ISPs are not keen to be seen to host these sites, and many domain registries have policies prohibiting the registration of deliberately confusing domains. An e-mail or phone call to the host and domain registry concerned will usually result in the site being taken down as the companies act to protect their own reputation.

Whilst waiting for the site to be taken down you may want to consider blocking the hosting IP address or DNS resolution as a temporary measure. You could redirect users to another page informing them of the situation and providing material to help them protect themselves against future attacks. Whilst this will protect local users from falling for a phishing attack they may still be at risk when using other networks.

If you believe that a crime has taken place, report the incident to your local police force.

2. Sites infringing upon copyright or trademarks

These sites don't pose a technical threat to an institution but have copied large amounts of material without permission or are falsely claiming associations with an institution's brand. The most common case is that the site has copied an institution's web design without permission.

If the issue is only one of intellectual property infringement then a legal route is most appropriate. A carefully worded take down notice should usually result in the offending content being taken down promptly, but be prepared to follow through if necessary. The process can become quite lengthy and complex, especially where content is hosted abroad. Seek qualified legal advice. JISC provides a factsheet on Take Down Policy and Procedures that contains useful examples of how take down notices may be worded (http://www.jisc.ac.uk/media/documents/themes/content/sca/templatenoticetakedown.pdf [1])

3. Other sites

Websites are encountered that simply do not appear to be quite right. Perhaps they claim to be in an area you know well but you've never heard of them, or there is just something odd that sticks in your mind. Warning signs include:

- Over emphasis on association with other organisations such as AQA, IIP and BIS.
- Many pages on visa and immigration processes in comparison to information on departments, staff and courses offered.
- Published address is a serviced office or mailbox and the telephone number is incorrect or goes unanswered.
- Large volumes of text copied verbatim from other websites.

Neither one or all of these signs is conclusive proof that an institution is not legitimate but we should be aware that fraudulent websites do exist. Fraudulent websites could be involved in:

- Student visa scams. Although many of these schemes have been closed down in recent years, stories of institutions selling false documentation for visa applications are common.
- Advance fee fraud in relation to visa applications. Offers of paid assistance with visa application paperwork appear to be quite common, but it's not clear if this is a legitimate service or not.
- Degree mill. The institution may be offering qualifications for sale (and usually without accreditation). Such scams used to be commonly advertised through spam.
- Information and identity theft from prospective applicants. In some cases it's clear that an institution does not actually exist but there is also no obvious fraud taking place. It is possible that the site is simply gathering personal information, documentation and fees from prospective applicants.

If you believe you have encountered such a site please contact us for further advice. If you believe that an immigration related crime has taken place it can be reported to the UK Border Agency at http://www.ukba.homeoffice.gov.uk/aboutus/contact/report-crime/ [2]

Protected terms

Under the Further and Higher Education Act 1992, only institutions granted permission by the Privy Council may award degrees or use the word university or 'university college' in their title. As a result fake universities are comparatively easy to detect and most fraudulent sites claim to be further education colleges. The term college by itself has no protection. The Skills Funding Agency maintains a Register of Training Organisations which lists institutions eligible for public funding.

The UK Border Agency has a list of educational institutions registered as Tier 4 sponsors, i.e., licensed to recruit non-European Union students. If a college is not on that list it is extremely unlikely that it is able to recruit international students (http://www.ukba.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/pointsbasedsystem/r [3]).

.ac domains

Many legitimate learning institutions are not publicly funded and eligible to register .ac.uk domains. Some are eligible for an .ac.uk domain but are unable to register the .ac.uk domain they desire. In many cases these organisations have used .ac (Ascension Island) domains instead. A minority of fraudulent sites have also been attracted to these domains.

The .ac registry NIC.AC is based in the UK and has always been extremely helpful in assisting Janet to shut down fraudulent registrations where possible. They are heavily involved in efforts to secure the DNS including DNSSEC.

Links
[1] http://www.jisc.ac.uk/media/documents/themes/content/sca/templatenoticetakedown.pdf
[2] http://www.ukba.homeoffice.gov.uk/aboutus/contact/report-crime/
[3] http://www.ukba.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/pointsbasedsystem/registerofspo