Important Information for Schools – Technical Guidance

SSL Search in Schools

For some while now search service providers (including Google) have provided search results behind SSL encryption. This means that all search results are served using 'https' (with the secure padlock shown in web browsers).

Search service providers such as Google state they do this in order to make searching the web more secure by preventing search terms, results and login information from being intercepted by others. Encrypting all transactions between search services and their users ensures they cannot easily be accessed by other individuals and organisations.

WHAT DOES THIS MEAN FOR SEARCHING THE INTERNET IN SCHOOLS?

Whilst making searching more secure, it can impact on the ability of schools and other organisations with a duty of care in relation to children's access to the internet to filter web content and search terms effectively in order to block access to inappropriate and harmful content.

In some cases this could present a safeguarding issue, as it means it is now more likely that inappropriate material could appear in search results. Whilst there has always been the possibility of this occurring (as no filtering system can ever be 100% effective 100% of the time), this change means that the possibility of inappropriate content bypassing filters has increased.

WHAT CAN SCHOOLS DO?

In summary there are four options that schools can consider in response to this issue:

1. Continue to use and access SSL search services such as Google without any changes to filtering solutions. Schools choosing this option should be aware that access to inappropriate material may be accessed by staff and students.
2. Change primary search service provider to Microsoft Bing www.bing.com which doesn't use SSL (https). This may offer a seemingly simpler short-term solution, though it is important to acknowledge that more and more websites move to SSL (https) and as such in the longer term it may not be an effective solution.
3. If Google is your school's primary search tool, ensure that Google's SafeSearch is applied to search results. This could be enabled by either your filtering solution or through Group policy (Windows domain joined computers). It is important to recognise that SafeSearch does not offer the same level of granularity and control over filtering. This therefore increases the risk of inappropriate search results, including images, being returned and displayed to learners.
4. Approach your web filtering/proxy service provider to request adding or activating 'SSL inspection' functionality to filtering solution (the filtering solution can intercept, decrypt and filter search results). In order to perform 'SSL interception', schools typically need to deploy a certificate (as it needs to decrypt, analyse, and then re-encrypt all traffic using a security certificate). This certificate needs to be deployed to all computers and devices that browse via the school's filtered internet connection.

Schools considering options 1 and/or 2 are advised to discuss the issue amongst key stakeholders within the school to ensure that the risks are fully understood and any additional training or other measures required are put in place. This will most likely require the update and refresh of school IT acceptable use policies and user education practices.

Schools considering options 3 and/or 4 should, in the first instance, contact their filtering solution provider and ascertain what capabilities the solution may have.

Some additional points which schools may wish to consider and raise with filtering solution, broadband service or technical support providers include:

- In schools where SSL inspection is selected as the best option, the process should be discussed with the technical support team to ensure everyone is aware of the steps to be taken to ensure the continuing protection of learners and staff.
- In schools where SSL inspection is deployed, the school's technical support/team may need to resolve issues with Apps which use https traffic in the background, generally this is where the Apps traffic is inspected and filtered, whereas previously the traffic wasn't inspected and filtered (examples of this are Youtube for Kids, where such apps do include advertising, in this instance the school would need to review the educational value and appropriateness of an App that includes advertising)
- Schools may also want to make parents aware of the general issue and also the school's chosen option; this provides transparency and demonstrates that schools are exercising their duty of care

Recommendation:

Using web filtering solutions that have Advanced SSL inspection technologies provide schools the ability to filter on https search queries, results and web pages accessed, reduces the risk of inappropriate search results being returned and improve reporting/monitoring capabilities.

If you would like further information or assistance in checking whether your school has implemented Advanced SSL inspection on the web filtering service please complete the following form:

https://goo.gl/forms/29s8kXkZJikxeaAx2

Reference to original article published at:

http://www.nen.gov.uk/advice/ssl-search-in-schools