



Avoiding the perils of public computers

INTERNET GATEWAY MANAGEMENT SERVICE

– WHAT TO LOOK FOR

- The service provides a full suite of functionality, including content filtering, firewall, virus blocking and isolation.
- Usage reporting can be carried out at any time and according to desired parameters
- The interface is easily understood by non-expert staff and changes to filters etc. Can then be made with a few clicks
- The service can be provided through a periodic subscription rather than via a very costly start-up price
- The service is 'plug and play' and does not require major overhauls and reprogramming of existing IT systems

Offering Internet access in a library to members of the public has its challenges. Whilst the obvious dangers of inappropriate material can to some extent be controlled by off-the-shelf content filters, there are a host of other ways in which public computers can be abused and all of them place extra burdens on library staff who may not be IT professionals. But there are a range of products/services available that offer simple and easily maintained solutions to some of the more common issues.

The first thing to understand when it comes to public computer use is that 'dangerous' content is not always sexual or illegal. What is increasingly more likely today is that a user will visit a website that exposes the computer to a virus or other form of malware. Whether this is done accidentally or deliberately is irrelevant, the result is the same – an infected machine. And since most library computers are networked, the problem can spread rapidly. This may necessitate the shutting down of all computers on the network in order to isolate the virus. Added to this is the cost of an emergency call out to specialist IT maintenance personnel.

The chance of infection becomes even higher when storage devices like USB sticks are inserted into public machines. Library users and even staff can quite innocently be carrying malware upon these devices picked up from other machines or in turn have their home computer infected by a virus they obtained from a library PC.

Another problematic issue for providers of public computers is selfish use. Downloading large media files (for example movies and music) will rob other users of connection speed (particularly in a Wi-Fi environment) as well as potentially increasing the bandwidth costs of the library. The legal risk of exposing the institution to copyright infringement is also real if they are providing the means for illegal file sharing.

The standard approach to these issues is usually piecemeal. Some site filtering software (often quite out of date and easily avoided), some anti-virus software (ditto) and a wary eye cast over suspicious customers (but with little chance of proving anything).

‘dangerous’ content is not always sexual or illegal. What is increasingly more likely today is that a user will visit a website that exposes the computer to a virus or other form of malware

When a virus is detected through a website or inserted hardware, a Internet Gateway Management Service should be able to isolate that machine instantly, to prevent the infection spreading and to keep other computers operational, allowing IT staff to work on just the problem PC without the urgency of a major network outage.

A better way of solving these sorts of problems is to use a Internet Gateway Management Service (IGMS). The best of these services can combine firewall, web filtering, email sanitization, infection isolation and reporting features into a single service. They work by combining some simple equipment on site that interfaces with a remote Network Operations Centre (NOC) – similar to the way that a pay TV box connects a home to the provider.

To solve the problem of inappropriate content, a good IGMS will use a blocking list that is much more dynamic than standard filter settings and is updated at least daily to keep informed of new threats. Staff should be able to set the service according to a selection of keywords or specific needs, since blanket bans on some types of content or words are not always practical.

When a virus is detected through a website or inserted hardware, a IGMS should be able to isolate that machine instantly, to prevent the infection spreading and to keep other computers operational, allowing IT staff to work on just the problem PC without the urgency of a major network outage.

Reporting functions on the service should allow the examination of activity on individual computers. This means that staff can check to see if a user is draining a lot of bandwidth with large downloads and what sort of sites this is happening through. Aside from the policing of selfish activity, this can also lead to identifying savings in Internet costs.

Overall, using a IGMS is an increasingly effective way of offering safe Internet connectivity to patrons. Best of all, it removes the need to saddle busy staff with the extra roles of police officer and technical support.