Illinois Heartland Library System

IT Update for February 2017 Board Meeting

Security updates

Security is always a high priority for IHLS. Not only do we have the obligation to protect our internal data, but also the data that exists on the servers for the SHARE automation project. We have always tried to err on the side of being too careful, but that can lead to times when it makes other tasks inconvenient for different groups. This report will hopefully give a brief overview of some of the steps we've taken to secure our systems.

There has been much talk on the news about ransomware and other new attacks that hold computers hostage until a price is paid. In fact, St Louis Public Library has been in the news lately for exactly that. IHLS has taken several steps to help minimize these risks.

First, staff of IHLS using PCs are not local administrators on their computers. This means that they don't have the permissions to install new software without IT involvement. This does cause some inconvenience when new legitimate software needs to be installed or updated, but the trade-off in security is worth it.

Second, with the installation of the new firewalls at all the sites, we now have the ability to filter out websites and URLs that are known to participate or be associated with viruses of all kinds and other malicious activity. All computers on our network are forced to go through this filter system to access the Internet. The filtering is provided by a subscription service that is included in our gold level maintenance agreement. It is updated continuously and even blocks some sites that are brand new and haven't been rated yet. This is because a lot of scammers are registering brand new domain names to get around filters that only keep track of bad website names. So far, this hasn't been a hardship to staff at all, and most haven't even noticed it.

As always the biggest threat is malicious emails. We encourage our staff to never click on links contained within emails if they aren't sure of the source of the sender. As long as computers are connected to the Internet there will be a chance for security breaches. However, we are taking every reasonable step to ensure our members and stakeholders that we care about the safety and security of their data.