Court Connection
Volume No. 6 – Issue No. 1
January 2017

IT NEWS AND SECURITY UPDATES

A Renewed Focus on Cyber Security
Submitted by Laurie Ellwood

Although Cyber Security has always been important for the courts, our mission this year is to step up the fight to secure our systems and protect our users and data from ongoing threats. We will become more educated, informed, and aware as the threats and strategies to harm our systems and data change daily. The Judiciary has systems in place to help us provide a more secure environment for our users both internal and external and a top notch security team at the AO that monitors these systems 24/7. They also provide updated and improved systems and support to local courts to help further protect against these threats. FLMB implements and upgrades these systems and continues to update and educate our IT team and our users. Weekly reports, monthly staff reports, and quarterly scans give us an "IT Security Scorecard" that is used to assess the security status of our local court environments. We strive to keep the scorecard complete and updated and we also strive toward constant and consistent improvement.

We saw a variety of Cyber Security threats in 2016 which included ransomware, key loggers, drive by downloads, spoofed emails and social engineering. Not only were these threats internal, but some of our external users suffered as well. Fortunately our Court could block, clean, delete, or remove these threats, and avoid data loss and/or locked files. We could also notify a few of our attorneys of possible threats and infections on their own systems. We could do this because of the Judiciary's vigilance and our educated, informed and aware local court community.

To view Biggest Data Breaches of 2016, So far - https://www.identityforce.com/blog/2016-data-breaches

This year will bring more threats and require even more diligence as we move through 2017. We all have a hand in protecting and securing our systems here and at home. Some familiar tips to keep you more secure include; updating software, operating systems, and browsers, installing a firewall and Anti-virus/Anti-malware programs, and using strong, updated passwords. Maybe more important than all of the above is to remain informed and aware of current trends and past mistakes, to become more prepared and aware for future threats.