

Security is Everyone's Business

By: Laurie Ellwood, Network Administrator

The Court was sharply reminded last month of just how vulnerable it is to data security threats. Some of our staff received the dreaded letter and have taken appropriate steps to protect themselves from further exposure. However, don't wait to be the next target. Examine your position in terms of risk to your own identity, credit, and financial information. While the OPM continues to investigate, being pro-active in data security will reduce the likelihood of exposure of your personal or professional information.

The precautions you take now can prevent you from becoming a victim. It cannot be stated enough, so we will restate a few of the actions you can take here. Monitor your financial and credit accounts and report anything suspicious immediately. Get your free credit reports from www.AnnualCreditReport.com. Place fraud alerts on your credit files, or place credit freezes to prevent opening or reviewing credit accounts without your consent www.consumer.ftc.gov/articles/0497-credit-freeze-faqs. Be aware of unsolicited emails or phone calls asking for personal or professional information. Be mindful of language and links in email and the security of the websites you visit (https:). **Install anti-virus software and keep it updated.**

Change passwords and create stronger ones. Most of all, stay informed. Use the resources available to you to better understand your risk. Here are a few that have been mentioned previously but of course worth mentioning again, www.Identitytheft.gov, www.us-cert.gov/ncas/tips, www.antiphishing.org, and www.ic3.gov.