WV Executive Branch Privacy Tip

As you know, the Privacy Office occasionally issues tips for the purpose of assisting you in making informed decisions in your "away from work" life. The following tip is reprinted with permission from the Privacy Rights Clearinghouse (www.privacyrights.org).

Get Your Digital House In Order!

Posted January 28, 2015

Now is a good time to take a moment to make sure you are doing what you can to help minimize data privacy and security risks with regard to your digital accounts.

1. Take inventory of your online accounts. Make a list all of the online accounts you have, and determine which ones you no longer use or need. This may include old email accounts, social media accounts, financial and banking accounts, shopping accounts that retain your credit card information, accounts containing personal health information, and others.

2. Examine your password practices. Do you use the same passwords for multiple accounts containing sensitive information? Do you use common words or phrases as passwords? If the answer to either of those is yes, create a new strategy and change your passwords. This could involve using a password manager, enabling multi-factor authentication (which we highly recommend), or (at minimum) changing and strengthening your passwords.

3. Navigate privacy and security settings. Determine which accounts contain information you consider most sensitive, and focus on those accounts first. Note that you may want to check shopping sites with which you have accounts, to see if they store your financial information in a way that anyone could get if they gain your log-in credentials.

Often privacy and security settings are located separately, and you may need to contact the service provider to help walk you through them. For apps or social media sites, you may want to reevaluate who you share information with and change permissions where possible.

4. Stay aware of current scams. Even if you do everything in your power to keep your information safe, you can't prevent a company you do business with from having a data breach. In addition, a lot of information is publicly available, and it is difficult to prevent a fraudster from finding it and using it to target you with a scam.

The Federal Trade Commission publishes resources for consumers which are helpful to read on a regular basis, but you should always keep your guard up. Don't click on links or download blindly, and never email your personal information – in particular your Social Security number— to anyone claiming they need it. Even if it looks legitimate, call the person or business yourself (a number you know is legitimate) to find out if it is a scam.

5. Ask questions and complain. Contact us with your privacy-related questions and complaints. We can help you navigate privacy and security-related resources, and we use complaints to help us advocate for consumer privacy rights.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.