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 for that purpose and is reprinted with permission from the Privacy Rights Clearinghouse (www.privacyrights.org).

Passwords aren't enough! Why you should consider using two-factor authentication

Passwords are dead. Or so we keep hearing. On their own, passwords clearly aren't the best way to protect our important information and accounts. However, for better or worse passwords are still very much alive until the next solution comes along and is widely adopted.

We have been preaching good password hygiene for many years, and we still think it is important. But unfortunately data breaches occur quite often and cybercriminals can be quite savvy. If you want to learn more, the 2014 Verizon Data Breach Investigations Report contains information on attacker methods and patterns over the past decade.

You can never assure perfect security, but fortunately you can take some steps to avoid being the low-hanging fruit. One way to do this is to look for and enable two-factor authentication in your online accounts.

What is two-factor authentication? In short, the concept is that instead of just needing something you know (such as a password) to access an account, you add a layer of security by also requiring information from something you have in your possession (like your mobile device). Use it when you can, and encourage any sites that don't have it to adopt it. It's not new a new concept or tool, but most people we talk with have no idea it exists until someone hacks one of their accounts.

How does two-factor authentication work? Typically, you will enter your password and then a code will be sent to your device—often your mobile phone—to enter before you can access the account. How and when you receive the code will depend on the service you use and/or your personal preference. For example, for some accounts you can download an app to generate codes. Alternatively, you may opt to receive the code in a text message or via a phone call. For those of you worried about convenience, look for an option to forgo the need for a code when you log in from a trusted computer or device.

How do you know if a site offers two-factor authentication? Twofactorauth.org has an extensive list of sites and information about whether and how they support two-factor authentication. You can also typically find out if a service you use offers it by looking on the security settings page of their site.

What can you do if you have more questions? Contact us at privacyrights.org and we will help point you in the right direction!

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