Lock Down Your Login

READY WISCONSIN

There is a lot to do when preparing for the holidays – buying gifts, planning travel, decorating the house, and preparing for festive holiday meals. The majority of these tasks require at least some sort of shopping and most consumers will do this shopping online. According to the National Retail Federation's 2016 study, more than half (56.5%) of holiday shoppers this season will be making their purchases online.

When shopping online, it's important for consumers to take steps to protect their identity and finances. Just as consumers have migrated towards online shopping, credit card thieves have started shifting their efforts online as well. During the holidays, deeply discounted products look appealing and shoppers make quick purchasing decisions without always taking into consideration the online purchasing risks that can be present. Millions of Americans have had their online accounts hacked and personal information compromised because of stolen credentials or weak logins. As hackers get more resourceful, usernames and passwords – which have been the fundamental account security mechanism – are no longer a sufficient solution to secure accounts. Luckily, there is a simple way to secure your online accounts and better protect yourself against online crime: strong authentication.

Enabling a strong authentication, sometimes called multi-factor or two-factor authentication, goes beyond just a username and password and is a useful way to lock down your login.
The Department of Homeland Security's Stop.Think.Connect.™ Campaign encourages you to enable a strong authentication on your sensitive online accounts such as your email, banking, and social media accounts today.

Taking advantage of the strong authentication – such as a unique one-time code through an app on your mobile device, biometrics, or security keys – that are offered by the majority of popular websites and services can go a long way in protecting your personal information online. The White House recently launched the "Lock Down Your Login" campaign to encourage all Americans to protect themselves online with strong authentication.

For more information on strong authentication and the new campaign, please visit www.LockDownYourLogin.com. You'll find specific advice on how to turn on strong authentication on a variety of websites and services that Americans use each day.
For more tips and information on how to stay safe online, please visit www.dhs.gov/stopthinkconnect.

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.
Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.