September 2016
Volume 11, Issue 9

Two-Factor Authentication

NH Department of Information Technology
www.nh.gov/doit/cybersecurity

Phones, computers, and appliances all store vital information. Passwords are one of the first steps to protecting that information – digital keys to our online kingdoms. But you can make login information more secure by pairing the password - something you know (knowledge) - with another factor, such as something you have (possession) or something you are (inherence). Something you have might be a smartphone, and you can prove you have the phone by reporting back the PIN code that was sent to it in a text message. Something you are could include your fingerprint or other biometric data. When two of these factors are combined to secure an account it is called two-factor authentication.

Why Shoud I Use Two-Factor Authentication?

Two-factor authentication is an important layer of defense beyond your password. It decreases your risk of falling victim to a compromise because criminals need access to two separate items to compromise your account – for instance your password and your smartphone (to receive the PIN code). Cyber criminals regularly "leak" (release) login credentials from compromised websites. They then use these leaked login names, email addresses, and passwords to find other accounts using the same credentials. This allows them to easily impersonate you online, gain access to work and personal accounts, sign online service agreements or contracts, engage in financial transactions, or change account information. Enabling two-factor authentication makes it more difficult for criminals to use this technique against you because a password would not be sufficient to gain access.

Turning on Two-Factor Authentication

Turning on two-factor authentication is really important on websites that process financial transactions (banks), contain sensitive information (Facebook), or could be used to impersonate you (Twitter). You can usually enable two-factor authentication through the security settings and directions to enable two-factor authentication are available in the help section of each website (It may be called "login verification" on some websites). If you can't find the directions on how to enable two-factor authentication on a specific website, an Internet search for "enabling two-factor authentication on" and the name of the website will usually get you the directions.

To be more cyber secure, turn on two-factor authentication and pair it with a strong, unique password.

Password Managers

One of the most common components of two-factor authentication is a strong password. Typically this means making the password long, complicated, and unique. But remembering all those passwords can be a challenge. So while you're implementing two-factor authentication on your accounts, you might also consider choosing a password manager.

A password manager is a password-protected application that can run on a computer, smartphone, or in the cloud that securely tracks and stores other passwords. This means you only have to remember one password! Most password managers can also generate strong, random passwords for each account. As long as the password to access the password manager is very strong and unique, and the location of the password manager data is protected, this technique can be effective at securing login credentials. When choosing a password manager, ensure it is from a known, trustworthy company with a good reputation. Only use a password manager that stores the information on the device and use it on devices you trust and can keep secure.

Further Information

More information on the role of strong passwords in enterprise defense is available in the CIS Critical Security Controls: https://www.cisecurity.org/critical-controls.cfm

Further advice on passwords is available in the MS-ISAC Security Primer available at: http://msisac.cisecurity.org/whitepaper/documents/Security Primer - Securing Login Credentials.pdf

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.