MVCDC Support

Multi-Factor Authentication (MFA) Update

2023-07-24 - Richard Woolf - General

Greetings from IT!

To better protect our organization, we will be enabling Multi-Factor Authentication on some of your accounts during the month of August:

There is no immediate action required yet, but we wanted to let you know what changes are coming, and how they will affect you. We will be sending out an additional email in a few days with more information on what you will have to do. At this point in time, the Multi-Factor Authentication will not apply to classroom computers. We will continue the current arrangement where teachers are only able to connect to their email accounts when on computers connected to the agency network. So, classroom computers and tablets will be exempt from this for the time being.

The Big Problem

You are probably wondering, **"Why are we doing this? What is Multi-Factor Authentication, and why do I care?"**

Sometimes mistakes happen, like putting your username and password into a misleading website. Sometimes your credentials get stolen from another site that you frequent. Once hackers get a hold of your username and password, they have full access to your accounts.

The good news: There's an easy way to better protect your data. It's called Multi-Factor Authentication (MFA), and we are adding it to your account.

What is Multi-Factor Authentication (MFA)?

MFA might sound complicated, but it's a pretty simple concept.

Right now, your username and password is what you use to access your account. This is considered **one factor**. It's something only you know which is why it works pretty well for ensuring only you can use your account. But if your credentials get stolen, someone can impersonate you. Remember, as far as your account is concerned, whoever enters your password is you.

If we add in a **second factor**, even if someone steals your password, they will not be able to login since they are missing the second factor. So what's a second factor? It's something you are or something you have. In this case,

your something you have will be your phone, because what else do you have with you more than your phone these days?

Now when you log in with your credentials, your account sends you a text with a code. You'll enter this code along with your password which tells your account It knows that only you should know your password and only you would also have your phone. Now your account can verify that the person signing in is actually you and not a hacker who stole your password.

Is this extra hassle really worth it?

The short answer: **YES**

Microsoft reports that using **MFA can block 99.9 percent of account compromise attempts**. You may think that there's nothing of value inside your email account, but the truth is every account has value. Think about all of the sensitive information that may be contained in your emails.

This information can be used, not only to steal from you, but target your colleagues and vendors acting as you.

Together, we'll keep this from happening.

Ryan Hardesty

Director of IT and Data Systems

Phone (937) 226-5664 x 336

Mobile (859) 446-8671

Miami Valley Child Development Centers

215 Horace Street | Dayton, OH 45402

rhardesty@mvcdc.org