IMPROVING SECURITY MEASURES ON YOUR PORTAL

Introducing Two-Factor Authentication

What is two-factor authentication and why the change?

Two-factor authentication adds extra security to your account by requiring a second factor, such as a code sent to a mobile device or email. This helps prevent unauthorized access and protects against security breaches.

Your data security is our top priority, and we utilize robust data protection measures to safeguard your information.

1 **Reduce Risk of Unauthorized Access**

2 **Added Layer of Security = Peace of Mind**

Instructions

The next time you use your portal, you will be prompted to use a second form of authentication.

You will be prompted to use two-factor authentication when logging into your portal, registering for an account, updating a password, or selecting 'Forgot Password'.

When registering, you will need to enter your cell phone number and an email address where the two-factor authentication code can be sent.

To continue, you must enable Two-Factor Authentication.

What does this mean? This means that a unique code will be required to log in from now on. You can choose to receive this code via email or cell phone.

Please select your preferred mode of contact, and you will be sent an authentication code right away. Once received, enter the code as generated on your mobile device or browser.

When you can expect to be prompted:

Logging In

Updating a Password

'Forgot Password'