

# What is Two-Factor Authentication?

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (such as your smart phone, landline, hardware token or other mobile device) along with your password prevents anyone but you from logging in, even if they know your password. Please check out the Double Up on Security video and the Guide to Two-Factor Authentication for more information.

Three steps to stronger authentication

1. Enter username and password as usual
2. Use your phone to verify your identity
3. Securely logged in

Once you've enrolled in Duo you're ready to go: You'll login as usual with your username and password, and then use your device to verify that it's you.

More information can be found in this short [video](#).

Short URL to this page: [https://answers.fredonia.edu/x/\\$action.getTinyUrl\(\)](https://answers.fredonia.edu/x/$action.getTinyUrl())

---

## Related articles

- [Fredonia Mail Data Loss Prevention Policy for Credit Card Numbers \(CCN\) and Social Security Numbers \(SSN\)](#)
- [What are my options to enroll in Duo Security?](#)
- [How do I mark or unmark Spam in Gmail?](#)
- [Can I use the Duo Security internationally?](#)
- [Do I need a smartphone to use Duo?](#)