Two-Factor Authentication

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 (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

Currently Suffolk is using Two-Factor Authentication for limited users and applications such as Workday.

	Suffolk has implemented Duo Two Factor authentication for Workday.

How It Works

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. You add multiple services to allow you to authenticate with Duo, such as using SMS, voice call, one-time passcode, the Duo Mobile smartphone app, and so on.

No mobile phone? You can also use a landline or tablet, or ask your administrator for a hardware token. Duo lets you link multiple devices to your account, so you can use your mobile phone and a landline, a landline and a hardware token, two different mobile devices, etc.

Why Do I Need This?

Passwords are increasingly easy to compromise. They can often be stolen, guessed, or hacked — you might not even know someone is accessing your account.

Two-factor authentication adds a second layer of security, keeping your account secure even if your password is compromised. With Duo, you'll be alerted right away (on your phone) if someone is trying to log in as you.

This second factor of authentication is separate and independent from your username and password — Duo never sees your password.

How Do I use Duo Two-factor Authentication?

Visit Using Suffolk Duo Two-Factor Authentication

Supported Devices

Click your device to learn more:

- iPhone & iPad
- Android Phones & Tablets
- BlackBerry Phones & Tablets
- Windows Phones & Tablets
- Cell Phones & Landlines
- Hardware Token

Reminders

- Never share your passwords with anyone
- Suffolk University, Information Technology Services (ITS) and ITS third-party service providers will NEVER ask for your account passwords
- If in doubt about a web link don't click, instead type it in the web address yourself and make sure it is a valid web address / URL that you are browsing to.

You should never circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software, except for University email, which is password secured by the overlaying operating system on University User workstations or smart devices.

Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device. Smart devices such as smart phones should be set to auto lock and require a password or pin to unlock. Laptops and personal smart devices should always be under your control and should be secured when not being used.

If you suspect or have reason to know that the security of a password may be compromised, the password must be changed immediately. Under such circumstances, you should immediately report the discovery to the Suffolk University ITS Service Desk (617) 557-2000.

Need Additional Assistance

Please contact the Service Desk
Email us at
servicedesk@suffolk.edu

or call 617-557-2000
(2000 on campus)

For information about Walk-in Support, http://www.suffolk.edu/explore/60186.php.