Multi-Factor Authentication

As part of Christopher Newport’s ongoing effort to further secure our information technology resources, Information Technology Services is implementing Multi-Factor Authentication (MFA).

What is Multi-Factor Authentication?

> *Multi-Factor Authentication (MFA) is quite simple, and organizations are focusing more than ever on creating a smooth user experience. In fact, you probably already use it in some form. For example, you’ve used MFA if you’ve:*
>
> - *swiped your bank card at the ATM and then entered your PIN (personal ID number).*
> - *logged into a website that sent a numeric code to your phone, which you then entered to gain access to your account.*
>
> *MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.*

– Source: "Back to basics: Multi-factor authentication (MFA)", NIST.gov

How do I install Duo?

Duo Two-Factor Authentication Client Setup

How do I set up Microsoft?

Microsoft Two-Factor Authentication Setup

When do I need MFA?

- When accessing Google Workspaces (email, calendar, drive, etc) via a web browser
- When connecting to the VPN
- When accessing a server with an administrative account via Remote Desktop Protocol (RDP) or Secure Shell (SSH)