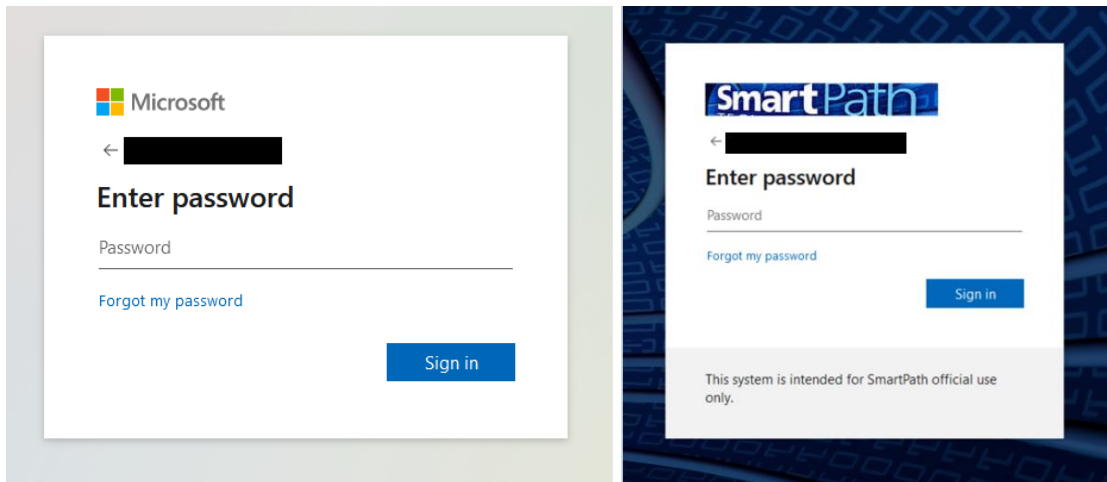


## Microsoft 365 Introduction

Your organization has decided to implement Microsoft 365 services through SmartPath Technologies. This means several things!

- You have the ability to check your email from anywhere using the Outlook Web App. The address is <https://portal.office365.com> Sign in with your full email address and password.
- For added security, your email login page will have custom branding after you enter your username. Do not log into a page that does not have your company branding; it may be a fake/scam website! Sample generic and custom logins are shown below:



- Another layer of protection present is multifactor authentication (MFA). This requires a code or mobile device authentication for login attempts. Setup instructions available at [SmartPathTech.com/resources](https://SmartPathTech.com/resources)
- You can check your email on mobile devices as well. The device must have a PIN of **at least** 6 digits. Setup instructions for iOS and Android are available at [SmartPathTech.com/resources](https://SmartPathTech.com/resources). The mobile device may be wiped automatically if an intruder attempts to log into it unsuccessfully too many times. The device may also be wiped manually if lost or stolen.
- You can encrypt any outgoing message by adding #encrypt or #secure to the subject line. Messages may also be encrypted automatically if sensitive content is detected. The recipient will be required to log in with a Microsoft account to view the message.
- Messages received from outside your organization will have the following banner at the top:

**Caution:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

This can be used to help identify if someone is attempting to impersonate a staff member.

Reach out to SmartPath Technologies if you experience any issues.

