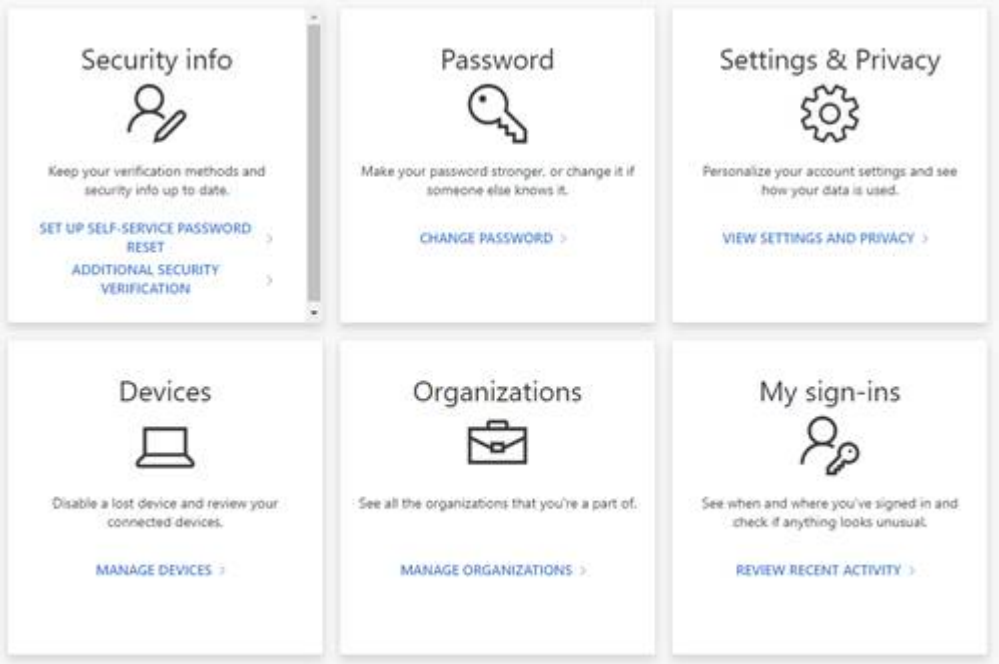
Keeping your account safe and secure: We all understand the importance of keeping our account secure, even more so with the reliance on telework and remote services. With the start of the fall semester, now may be the perfect time to review your account privacy and security settings. You may not even be aware of the new portal Microsoft has made available to help you monitor your account activity. Here are some basic hygiene steps you can perform on your account as the semester kicks off. Your account settings can be accessed from a web browser using this link: https://myaccount.microsoft.com/?ref=MeControl. After you log in, you'll see several tiles to perform such actions as: configure your password recovery options, enabling multi-factor authentication, and view sign-in activity. Take a moment to confirm your password recovery options so you do not lose access to your account. Configuring additional security verification is the best method for protecting your account from unauthorized access. In the event risky activities are detected on your account, multi-factor authentication will force an additional layer of protection when logging in. The "My sign-ins" portal was recently enabled and allows users to review attempted sign-in activity on their account.



Personal Account Protection: The Equifax data breach feels like it happened decades ago given our new normal, but attackers are still exploiting identities that were disclosed. You should always review your credit reports on a regular basis for anomalies. In addition to periodic review if you feel you are at greater risk you may want to look at the option of implementing a Credit Freeze. Also known as a security freeze, this free tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. If you'd like more information regarding this tool please visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

If you have questions or concerns about this newsletter, please contact Information Security.