/ Information Technology / Why Do Multi-factor Authentication?

WHY IS THE COLLEGE PROMOTING MULTI-FACTOR AUTHENTICATION FOR EMAIL ACCESS?

This is a valid question, and one that deserves a thorough explanation. For the sake of this document, multi-factor or two-factor authentication will be referred to as MFA.

First, the definition of multi-factor or two-factor authentication is important. A more basic question is, “what is a factor?”.

A factor is a method used to authenticate a user. There are three different basic factors:

- Something you know – a password, a PIN, or a passphrase.
- Something you have – a physical key, a smartphone, or even just an identification card.
- Something you are – a fingerprint, a retina scan, your face, or your voice

MFA uses at least two of these three factors, making it much harder for someone to access your account.

So why push MFA now?

Aside from multiple external security assessments recommending the practice, here is a quick list of reasons. Each one will be explained below.

- Email is the easiest method of attacking users and trying to trick them into giving up their passwords.
- Phishing emails continue to get better, more believable, and more frequent. It is only a matter of time before they become almost indistinguishable from valid emails.
- The impact of an account breach is more than just email. The same username and password most likely also allows for login to a computer. When a user connects to Office365 for email, this also grants them access to OneDrive, Sharepoint, and other Microsoft services.
- The Office for Information Technology (OIT) is already implementing single-sign-on, or SSO. This will consolidate even more services under the one username and password used for email. MFA is essential for SSO to succeed.
- Attackers only need to succeed once.

Email is the easiest method of attack for criminals. Email is how things get done within organizations and between organizations. Emails are given “the benefit of the doubt” by perimeter security tools like firewalls and intrusion prevention systems. That is why they are the most effective way to try and compromise a user or an entire organization.

Phishing emails continue to get better. Attackers refine the text of their emails to make them more believable. Where spam emails tend to gear their messages to the more susceptible, phishing emails are usually targeted at more experienced users or toward users with more responsibilities in the organization, i.e, those who have access to money. It is only a matter of time before it will be very difficult to tell the difference between a phishing attempt and a valid email. Fraudulent emails sent from within an organization, such as when another user’s account has been breached, make it even harder to tell the difference.

The impact of a breach of email credentials, which are actually Office365 credentials, is greater than just a few sensitive emails read by an unauthorized user. Not only can an attacker read emails they are not authorized to see, they can also delete them, or even worse, impersonate the victim to other users.

These same credentials allow access to OneDrive, Sharepoint, and other Office365 services. Since we now synchronize passwords between Office365 and our local authentication for workstations, Active Directory (AD), those same credentials could allow access to a user’s computer, if the attacker is on campus. Users with VPN access are at greater risk, as those same credentials allow access to the VPN (*OIT will be mitigating this issue in the future, stay tuned for more information*).

OIT is currently working to provide single-sign-on (SSO) capability for most web-based applications used by faculty, staff and students. While this is a great and useful tool to help ease the burden of remembering what username and password to use with what service, it absolutely must be coupled with multi-factor authentication to be successful. Imagine the damage that could be done if SSO was not protected by MFA.

Finally, attackers only have to succeed once. It only takes one user responding to a phishing email, not protected by MFA, to potentially cause a near-apocalyptic amount of damage to the college and to employees and students. MFA substantially strengthens the college’s security stance and makes it much harder for attackers to penetrate our defenses.