T2025_18 Why Enabling Multi-Factor Authentication Is Critical (September 24th, 2025)

Multi-Factor Authentication (MFA) is one of the most effective defenses against account takeover. Even if a password is leaked or phished, requiring a second factor such as a code from an authenticator app, biometric confirmation, or hardware token adds a strong barrier. MFA significantly reduces the risk of unauthorized access, protects sensitive data, and improves overall account security.

Some MFA methods (e.g. SMS) are vulnerable to interception or SIM-swapping, so using more secure alternatives (authenticator apps, hardware tokens) or phishing-resistant methods is preferable.

References

- CISA, More than a Password. CISA. https://www.cisa.gov/MFA?

- CIO, The Importance of Multifactor Authentication. (October 26th, 2022). Retrieved from CIO. https://www.cio.gov/2022-10-26-importance-multifactor-authentication/