Name: John Lloyd Renzo R. Castillo	**Date:** Oct 26, 2023
Course/Section: BS Computer Engineering	**Instructor:** Dr. Iryll Nungay

The Imperative Need for Two-Factor Authentication in Online Accounts

In the digital age, our online accounts are important for personal and financial information. Protecting these accounts is essential, but with the increasing of cyberattacks, more than traditional passwords are required. Two-factor authentication (2FA) adds an extra layer of security by requiring users to provide two different authentication factors to gain access to an account. This makes it much more difficult for attackers to access accounts, even if they have the user's password.

2FA is effective in securing accounts for several reasons. First, it requires users to provide two separate forms of identification, which makes it much more difficult for attackers to gain access to accounts. Second, 2FA can protect against phishing attacks, which are attempts to trick users into revealing their passwords or other personal information. Third, 2FA can help mitigate credential stuffing attacks, which involve using stolen usernames and passwords to gain access to multiple accounts (Snow, 2023).

The widespread adoption of 2FA would have a significant impact on improving cybersecurity. According to the Verizon Data Breach Investigations Report (DBIR), 81% of data breaches in 2020 involved compromised passwords. This means that the vast majority of data breaches could have been prevented if 2FA had been used.

The DBIR also found that organizations that use 2FA are much less likely to experience data breaches. For example, in 2020, only 10% of organizations that used 2FA experienced a data breach, compared to 25% of organizations that did not use 2FA (*2023 Data Breach Investigations Report*, n.d.). These findings demonstrate the positive impact of 2FA on cybersecurity.

2FA offers some benefits for organizations and individuals. For organizations, 2FA can help to protect sensitive data and reduce the risk of data breaches. 2FA can also help to improve compliance with industry regulations and standards.

For individuals, 2FA can help to protect their personal and financial information from unauthorized access. 2FA can also help to reduce the risk of identity theft and fraud.

In conclusion, 2FA is a critical component of a robust cybersecurity strategy. It is effective in securing accounts and protecting against a wide range of cyberattacks. Organizations and individuals should enable 2FA on all of their online accounts to improve their security and protect their privacy.

References

Cybersecurity Report Series - Download PDFs. (n.d.). Cisco. Retrieved November 5, 2023, from https://www.cisco.com/c/en/us/products/security/security-reports.html

Snow, J. (2023, May 23). *Practical tips for protecting your data while traveling*. National Geographic. Retrieved November 5, 2023, from https://www.nationalgeographic.com/travel/article/practical-tips-for-protecting-your-data-while-traveling

2023 Data Breach Investigations Report. (n.d.). Verizon. Retrieved November 5, 2023, from https://enterprise.verizon.com/resources/reports/dbir/