Bitwarden: The Ideal Solution for Password Management

Section A: Blog Post

In recent years, Cyber Security breaches have been increasing drastically at Northern Light Health Medical Center. While there are many factors to building a secure network domain, your advanced security could be undone by a single password breach. With password requirements becoming increasingly stringent, it has become far more common to rely on the old standby: the handwritten password on a yellow sticky note. While this is a significant risk and most certainly breaks the compliance regulations of most corporate office environments, it still does not deter the common user. A slightly better option would be a text file on your device containing passwords and other sensitive information. This is also a risk as an attacker would only need to crack your account password to access that file. In addition, users will often fall back on easy to remember password phrases rather than randomized passwords that are far more secure. The true solution to these dilemmas would be a dedicated password managing software. There are many variations of this type of software, but today I will be discussing the current standard in this field that I would like to implement, Bitwarden.

Bitwarden is a cross-platform application that provides end-to-end encryption for your personal password vault. Once the app is downloaded (on IOS, Android, or Windows), you can store all usernames and passwords in one central location. This personal vault is protected by a master password known only to you. It can’t be recovered through email, nor is it stored on any server where the company can access it. This password library can be accessed across multiple devices if needed including your company cell phone. Password lists can also be organized into folders for convenience.

A poorly secured password manager could create significant problems, which is why Bitwarden uses AES-CBC 256-bit encryption, salted hashing, and PBKDF2 SHA-256 (Bitwarden, n.d). These gold standard encryption algorithms ensure that the data you enter will not be accessible by anyone but you. The algorithms encrypt your master password locally on your device before transmitting to the server and it is then salted with a random cryptographic value before being hashed again for storage (Bitwarden, n.d). The passwords cannot be reverse engineered by anyone at Bitwarden, which also means there is no way an attacker could steal your data in the event of a breach to their servers (Bitwarden, n.d)

Another bonus to this software is the fact that it is Open-Source, meaning the user community can review the application code and see how the software works to suggest improvements or potential vulnerabilities (Gizmondo Advisor Reviews Team, 2021). Bitwarden also includes useful tools in their software in the form of sending secure passwords and browser extensions for all personal and enterprise tiers of their service (Jennings, 2023).

Perhaps one of the most useful tools is a password/passphrase generator. You can select the length of the password and whether it will include special characters or capital letters. These randomly generated passwords will be far more secure than anything users would create currently as most important dates, names and locations can be found easily by attackers searching social media websites.

Implementing this software within our organization will provide employees with a secure password storage solution to avoid potential risks that password breaches present. With the easy-to-use auto-fill features and random password generator it will encourage users to set up more complicated passwords knowing they will be stored securely. This will prevent potential patient health information breaches and avoid non-compliance lawsuits in the future.

Our company would benefit greatly from a password managing application. Bitwarden is a software that has security in mind with every piece of their model, including state of the art encryption algorithms. Allowing users to install this software on their corporate devices will go a long way toward eliminating the risks of handwritten sticky notes or poorly secured text files containing passwords. Securing this data will keep our patient information safe and further minimize the risk to the organization.

Section B: Identify Employee Group

The employee group for this article would be the Information Systems Management team for our organization, Northern Light Health. These would be the Directors and Vice Presidents would make the decisions for which software is allowed by the organization.

B1. Analyzing Business Etiquette

The tone of the article was written to be Urgent. This is a solution that needs to be implemented as soon as possible. Given that the issues addressed are potentially going to cost the organization money and loss of reputation if handled incorrectly, I had to provide multiple reassurances of the security features of this software and why this option would be the best way forward.

Information Systems Management would be comfortable with some technical terminology (encryption algorithms, etc.) used above. The article was intended to be convincing, so I used realistic examples of the current issues with risk and proceeded to provide solutions that this software provides to each of those problems. My word choices were intended to be Semi-Formal while still conveying the seriousness of the need for the software.

Section C: Sources

Bitwarden (n.d.). What Encryption is Used?
https://bitwarden.com/help/what-encryption-is-used/

Jennings, Mike. (August 8, 2023). Bitwarden Review: Pros & Cons, Features, Ratings, Pricing and more.

https://www.techradar.com/reviews/bitwarden

Gizmondo Advisor Reviews Team. (August 12, 2021). Bitwarden vs. LastPass: A Tale of Two Password Managers.
https://gizmodo.com/advisor/password-manager/bitwarden-vs-lastpass//