LastPass •••|

enterprise

Your Business Should Invest in Password Management

Advanced Kiosks uses LastPass Enterprise for their password and security management.

Cybercrime is not something we take lightly at Advanced Kiosks. We work with many government and healthcare organizations, so protecting their data is not just fundamental, it's non-negotiable. We go to great lengths to secure our products. Why wouldn't we do the same to protect our workplace computers?

It's Not Just Big Brands Under Attack

A recent study showed that the average total cost of a single data breach was a staggering $3.79 million US dollars. 1 in 40 small businesses are at risk of becoming a target for cyber criminals. Symantec's "Internet Security Threat Report 2016" revealed that small businesses should worry about the less advanced attacks

The Cost of an Attack vs. the Cost of Preventing One

There are three main types of costs associated with not protecting your business from malicious cybercriminals:

Financial: Loss of revenue, loss of potential revenue from new deals.

Time: Contacting law enforcement, financial institutions, creditors, vendors, and customers as well as identifying the cause of the breach and resetting passwords.

Creditability: Damage to your brand, loss of job, business, customers, and employees.

Advanced Kiosks chose LastPass Enterprise because we recognized that preventing potential attacks is worth the nominal investment.

Why Aren't Businesses Protecting Themselves Against Cybercrime?

1. They believe they aren't a valuable enough target. Cyber criminals are opportunistic, targeting their victims at random and looking for easy access to money. Small businesses make easy targets. According to Small Business Trends, "These phishing attacks target employees largely responsible for the finances of a small business."

2. They think finding the right solution is going to take too much time.

Employers trust their employees. However, you can't know for sure until you have a system in place to confirm if employees are following best practices. The first question to ask is: Do I know what the best password practices are for protecting our data and are my employees equipped to follow those best practices?

LastPass Enterprise solves the problem of not knowing if your employees are taking the proper password security measures. LastPass is also a self-service solution, can be up and running quickly, and scales well, so you're able to start small and deploy across your organization.

Why Advanced Kiosks Chose LastPass Enterprise

• We are a self-service technology company started by an engineer who firmly believes in mitigating risk.

• **Price:** The pricing is flexible and budget-friendly for an SMB.

• **Educational Resources**: Our team members appreciate having access to educational resources, from the LastPass Blog to the Screencasts to other helpful support options.

• **Easy to use:** The vault's interface is user-friendly and makes managing passwords easy.

• **Password Sharing:** In the vault, we're able to grant shared access to various software platforms without disclosing the passwords. If someone leaves their position, we can revoke access to passwords and change them.

• **Centralized admin dashboard:** We are able to onboard new employees by granting them access in just a few minutes. You can also preload employee vaults so they have the logins they need to get them up and running with LastPass.

• **Security:** LastPass uses leading encryption algorithms, doesn't store passwords on any of their servers and offers two-factor authentication.

A small investment in cyber security is worth protecting against the upwards of millions of dollars in potential damages. A recent report from Security Intelligence shared that cybercrime will become a $2.1 trillion problem by 2019. Now is the time protect your business with a small investment for what is priceless: your peace of mind.
Take action today.

This article was written by Nancy Deol, Marketing Manager at Advanced Kiosks, a LastPass Enterprise customer.