**Password Boss Email Templates for MSPs:**

**Password Boss: Email #1**

**SUBJECT LINE:** What if you lost your biggest customer?

Hi [Customer Name],

81% of security incidents come from weak or stolen passwords.

Companies without password managers risk losing their biggest revenue streams when their business must be shut down to recover from an attack or when word gets out that you were hacked.

Yet, it’s not uncommon for most business owners to let employees use the same passwords at the peril of compromising the systems that hold their most sensitive data.

If you’re interested in adding a password manager to your current services, you can reach us at:

[Sign Off/ MSP Contact Info]

**Password Boss: Email #2**

**SUBJECT LINE:** This mistake could ruin your business

Hi [Customer Name],

Cybercrime is rising at unprecedented rates and your biggest risk is human error.

In fact, 82% of data breaches involve a human element—**this includes the use of stolen login credentials.** It’s not a matter of *if* you will get hacked or targeted, but *when.*

Using a password manager can save you thousands to millions of dollars more than if you try to get by without one. Many times, security incidents will even put owners out of business because the cost is too great to recover from.

If you want to help your employees secure personal and business passwords, we can help you get started with Password Boss’ password manager. Learn more about password management in the attached e-book: *Everything You Need to Know About Password Management for Your Business.*

[Sign Off/ MSP Contact Info]

**Password Boss: Email #3**

**SUBJECT LINE:** Your reputation is at risk

Hi [Customer Name],

55% of security breach victims are small businesses.

These attacks can cost businesses millions of dollars and *if* your business survives, can present long-last challenges like trying to rebuild your public reputation.

When private customer information is stolen, it costs you more than money. It costs you your client’s trust, the public’s trust, and even employee trust in your business. Knowing this, are you prepared to recover from a malware attack?

If you’re looking to protect your business and its sensitive information with Password Boss’ password manager, you can reach us at:

[Sign-Off/ MSP Contact Info]

**Password Boss: Email #4**

**SUBJECT LINE:** Losing Revenue

Hi [Customer Name],

Did you know that over 81% of security incidents come from weak or stolen passwords?

Yet, it’s not uncommon for most business owners to let employees use the same passwords at the peril of compromising the systems that hold their most sensitive data.

Too often businesses like yours risk their sensitive data by keeping and sharing passwords in the wrong place. Or, worse, using the same or similar passwords for many accounts.

That’s why password managers are the best option for accessing your company’s accounts. To learn more about password management, check out the e-book we attached to this email.

If you’re interested in adding a password manager to your current services, you can reach us at:

[Sign Off/ MSP Contact Info]

**Password Boss: Email #5**

**SUBJECT LINE:** Password Management Solution

Hi [Customer Name],

Cybercrime is rising at unprecedented rates. Which means it's more important than ever to be aware of the risks your business faces daily. Surprisingly, the biggest risk isn’t a hacker reaching your server or firewalls, it’s human error.

In fact, 82% of data breaches involve a human element—**this includes the use of stolen login credentials.**

Unfortunately, the human element of cybersecurity is also the hardest to control.

That’s why we recommend adding a password manager to your cybersecurity strategy. The password manager we use and install for our clients is Password Boss. It's a password manager that allows employees to separate personal and work passwords.

If you want to help your employees secure personal and business passwords, we can help you get started with Password Boss’ password manager.

[Sign Off/ MSP Contact Info]

**Password Boss: Email #6**

**SUBJECT LINE**: Security Risks are Increasing

Hi [Customer Name],

Did you know that **55% of security breach victims are small businesses?**

Fortunately, you can make big changes by implementing simple solutions, such as using a trusted password manager. The password manager we use and install for our clients is Password Boss. It's an easy-to-use solution that allows you to manage and share credentials securely.

If you’re looking to protect your business and its sensitive information with Password Boss’ password manager, you can reach us at:

[Sign-Off/ MSP Contact Info]

**Password Boss: Email #7**

**SUBJECT LINE**: How to mitigate security incidents

Hi [Customer Name],

Did you know that over 81% of security breaches come from weak or stolen passwords?

Despite this information, about 60% of small business employees use the exact same password for everything they access.

Every day, businesses like yours risk their sensitive data with seemingly harmless actions, like keeping and sharing passwords in compromising locations or using the same or similar passwords for multiple accounts.

To mitigate the risks associated with poor password management, the FBI suggests to “Create a strong and unique passphrase for each online account you hold and change them regularly. Using the same passphrase across several accounts makes you more vulnerable if one account is breached.”

We know it’s hard remembering different strong passwords for every account, especially when they look something like this: v^C1U7jpJR!A5F90tU+$—so we don’t expect you to.

That’s why password manager tools are the best option for managing access to your company’s accounts and programs. Not only can you safely share and store complex passwords but they can also:

* Streamline your workday by storing every username and password to auto-log you into every account
* Offer a mobile app for access to your work and personal logins on the go
* Help you find out if your email or passwords have been leaked on the Dark Web with a comprehensive security dashboard

If you’re sharing or storing passwords on sticky notes, through email, Excel, or even chat tools like Microsoft Teams or Slack, you’re at risk of those passwords being found and abused by cybercriminals. You can learn more about where your employees could be sharing their passwords (and *shouldn’t* be) in the e-book attached to this email.

Protecting yourself from bad password sharing habits is easy when you implement a password manager tool like Password Boss. If you’re interested in adding Password Boss to your current services, you can reach us at:

[MSP Contact Info]

**Password Boss: Email #8**

**SUBJECT LINE:** Cybersecurity benefit for employees

Hi [Customer Name],

As the foundation of your business operations, your employees are the key to your company’s cybersecurity. In fact, 82% of data breaches involve the human element, which includes the use of stolen login credentials.

Unfortunately, the human element of cybersecurity is also the hardest to control.

That’s why when you add a password manager to your cybersecurity defense, we also encourage you to use it personally. Getting in the habit of following Cybersecurity Best Practices in and outside of the office is what helps cultivate a strong cybersecurity awareness culture.

By offering a password manager that includes separate personal and work folders it not only helps your business stay protected but can also be offered as a cybersecurity benefit to your employees at no additional cost.

As an employer you won’t have access to personal passwords, so your employee’s personal data remains private, while helping them get into good password habits by giving them a greater individual incentive to consistently use the password manager.

Even the US Cybersecurity and Infrastructure Security Agency explicitly recommends “The most secure way to store all your unique passwords is by using a password manager. With just one password, a computer can create and save passwords for every account that you have – protecting your online information, including credit card numbers and their three-digit codes, answers to security questions, and more.”

Offering a cybersecurity benefits like password management demonstrates a comprehensive approach to benefit offerings while safeguarding your business’s information.

If identity and information protection is something you’d like to offer your employees through the Password Boss password manager, you can reach us at:

[MSP Contact Info]