HOW TO KEEP YOUR SAAS BUSINESS SAFE

5 MISTAKES TO AVOID

Skipping multifactor authentication

Multifactor authentication is one of the most powerful security tools out there. By not offering at least two-factor authentication to verify employee and customer information before login, you're putting both customer accounts and internal data at risk.

Moving your data unencrypted

Encryption is one of your strongest allies in the ongoing fight to keep data safe and secure. Make sure to encrypt your data both when it's at rest (in storage) and in transit (being sent), decreasing the fallout from any data interception that may inadvertently occur.

Not properly training your employees

Employee training is a fundamental part of any company's security program. It's vital that employees understand the security tools at their disposal and how to use them, as well as what their responsibilities are when it comes to protecting customer data.

Not using the latest technology

Many sophisticated antivirus scanners and cloud access security brokers are available to help you secure data for your SaaS business. Make sure to set up these security tools correctly and audit them regularly to ensure they are still protecting you as expected.

Not segmenting and storing data appropriately

Sensitive business data should be kept on separate servers that are physically secure. Data for individual customer accounts should be stored separately so their details are harder to compromise. To make this happen, be sure to create and follow clear rules for where data is stored and who can access it.

2checkout

www.2checkout.com