HELPNETSECURITY

Robert C. Johnson, CEO, TeamSupport
March 25, 2020

How to secure customer data for SaaS success

Recently, some of the biggest names in SaaS have experienced customer support data breaches. With data playing an important role in the success of customer support, companies must ensure information security is top of mind to build relationships and develop trust with customers.

But, in addition to being secure, B2B customer support teams need customer information to be easily accessible so they can help resolve tickets quickly and efficiently. In this article, I'll walk through three strategies customer support teams can utilize to improve customer data security.

Equip agents so they can easily and quickly verify customer information

Agents typically spend more time than anyone else working with your customers – which is why they need to be equipped with the best technology and procedures to verify customer information when they're working on a legitimate issue.

When selecting technology solutions, customer support software should include key security features that are built in and easy to work with, letting customer support agents dedicate more of their time and energy on solving the issues at hand. Customers will also have assurance knowing their communications with your team are secure in real-time and will remain secure for as long as your team stores their information.

Features can include SSL user authentication, two-factor authentication, and Service Level Agreement (SLA) management. For example, a simple way to prevent fraudulent logins and impersonations is to require customers to use their mobile device as a part of the support portal login process. When someone tries to login to an account, the mobile number associated with the account will receive a text message containing a security code. This quick form of authentication can be a strong first defense and they can immediately chat or send a ticket once they login.

Control internal and external data access

It can be frustrating when you're locked out of information for which you need access and going through a chain of colleagues to find the right person to give you proper permissions can take time. But, what's just as important as ensuring the proper teams and agents have access to customer information is keeping internal data locked away from those within your organization who don't need access.

Your customer support team has access to a lot of customer information because it's critical to their job, and this data needs to remain safe and secure. To better protect customers and the organizations as a whole, B2B customer support teams must know granting too much access even to internal colleagues can leave data in a vulnerable position. To combat this, companies must enforce practices to ensure data is kept in the hands of those who truly need access to it.

The same code of ethics for customer information should definitely be followed when working with an external vendor who might be involved in a support ticket. For example, if a support agent is working with a customer and their third-party vendor, it might seem only natural to give both parties access to all information and communication regarding the ticket. However, the vendor should be removed from any communications sharing personal information such as a product ID code or confirmation number that could potentially convey sensitive customer information.

Just because a vendor is “green lit” to act on behalf of the customer doesn’t mean you have a relationship in place to share personal information about the customer with the vendor. Tread carefully here and check your contract if necessary.

Collaborate with development teams in a secure manner

Customer support should be a part of the development process since they understand customer frustrations the most, but the two teams must collaborate on a secure platform, especially when sharing customer information.

Many teams rely on inexpensive or free collaborative platforms to communicate because the upfront cost of building their own collaborative environment can be expensive. However, a well-built environment fully integrated with your existing systems is a worthwhile investment considering the risk you and your customers face with their sensitive information when using less secure platforms.

SaaS customer support can be a secure channel for your customers, but you should consider what customer information your agents and employees can access. By properly training your B2B support agents and equipping them with software built to encourage and enforce security best practices, you and your customers will be safer.