Os sistemas de pagamentos online têm crescido cada vez mais nas últimas décadas devido à crescente disseminação de bancos e compras através da internet.

À medida que o mundo avança mais com o desenvolvimento da tecnologia, é possível perceber o surgimento de sistemas de **pagamentos online** e dispositivos de processamento de pagamentos.

Os sistemas de pagamentos online permitem que os clientes paguem pelos serviços por meio de métodos eletrônicos.

Dessa forma, pagamento eletrônico é feito via débito, crédito, cheques eletrônicos, dentre outros métodos alternativos de transações eletrônicas, como carteiras eletrônicas, bitcoin e criptomoedas.

A escolha por esse método de pagamento, tem relação com a rapidez e facilidade da transação, além da segurança que os sistemas oferecem.

Todavia, para que a realização dos pagamentos seja ainda mais segura, é necessário que sejam adotadas normas e regulamentos de segurança de dados nos escritórios e empresas que utilizam do método.

SEGURANÇA DO SISTEMA ONLINE

Em primeiro lugar, certifique-se de que o sistema integrado online que aceita pagamentos em nome de sua empresa esteja hospedado em um ambiente seguro.

Nesse ponto, grandes e pequenas empresas devem tomar os mesmos cuidados, uma vez que ambas podem ser alvos de ataques de segurança.

Desse modo, certifique-se de que o provedor de hospedagem para o sistema tenha as práticas e salvaguardas corretas em vigor.

FATORES HUMANOS

Para incorporar plenamente a cultura de **transações financeiras** digitais em sua empresa ou organização, é necessário educar todos os funcionários.

Principalmente e especialmente os responsáveis por lidar com pagamentos em relação às medidas de segurança necessárias.

Nesse sentido, deverão ser adotadas ações como:

- Proteção de dispositivos por senha
- Uso de um software seguro e atualizado
- Uso de VPNs
- Proteção contra vírus
- Dispositivos com uso exclusivamente profissional

AUTENTICAÇÃO DE DOIS FATORES

A autenticação de dois fatores é a melhor prática recomendada para ser usada por ambas as partes ao efetuar pagamentos.

Isso porque seu uso protege contra perdas de dados e transações fraudulentas causadas por roubo de identidade.

Sendo assim, os clientes precisam garantir que suas transações financeiras digitais e móveis sejam sobre o uso da autenticação de dois fatores.

PROTEÇÃO DE DADOS DO CLIENTE

Com relação aos proventos econômicos da empresa, não há necessidade real de armazenar informações da conta do cliente ou detalhes do cartão a longo prazo.

Nesse caso, a melhor maneira de proteger os dados do cliente é não armazená-los em casos em que não sejam necessários.

Por outro lado, em situações em que precisa ser armazenado, ele deve ser criptografado e armazenado em uma rede privada com acesso limitado para pessoal autorizado.

Sendo assim, poderá ser contratado um parceiro de pagamento de terceiros confiável para garantir a segurança na coleta e transferência de transações financeiras, bem como o armazenamento dos **dados necessários**.

CONCLUSÃO

Nota-se que em qualquer negócio orientado para o cliente, é certamente benéfico pensar nas necessidades dos clientes primeiro.

Dessa forma, os pagamentos digitais em todas as suas formas, sejam por cartões ou pagamentos online, fornecem uma alternativa conveniente para que os clientes realizem as transações financeiras de seu negócio.

Todavia, o ônus de garantir a segurança da implementação do sistema de pagamento se estabelece na empresa a qual adota o sistema.

Portanto, recomenda-se usar práticas indicadas e testadas conforme listado acima ao implementar a mais recente tecnologia de pagamento digital em sua empresa.

Em conclusão, estas são as principais noções acerca das práticas de segurança nos **pagamentos online**. Continue acompanhando nosso blog e siga nosso Instagram para mais conteúdos.