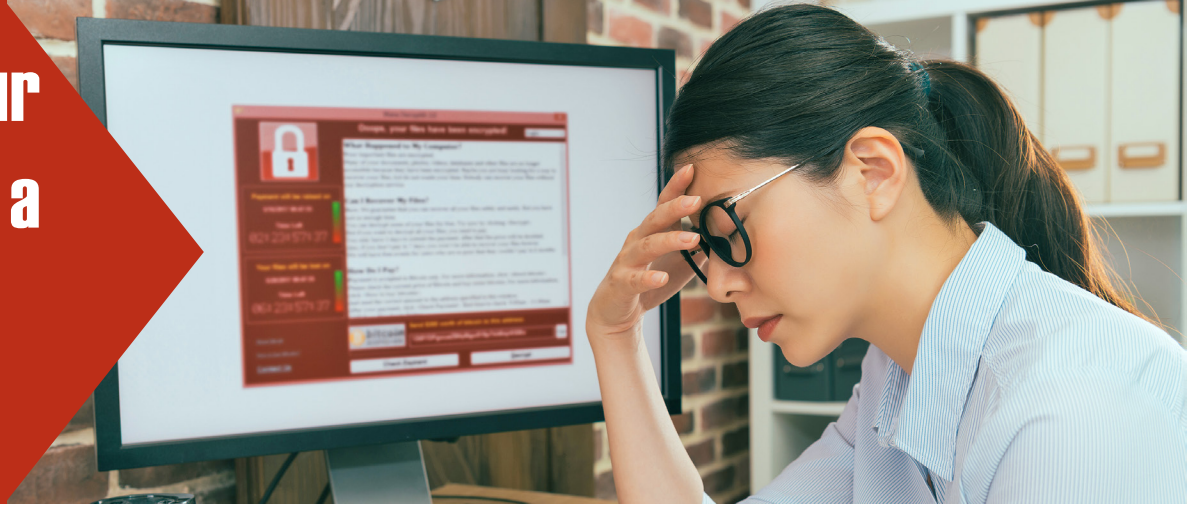
Protecting Your Business From a Ransomware Attack



Over the last few years, ransomware attacks have become more frequent, as criminals have been targeting businesses and organizations in order to obtain user information. The goal is to monetize user information and force companies to pay a fee for their vital data through infiltrating a database and building an encrypted wall between the business and internal data.

When this first started becoming a popular tactic with criminals, it was mostly happening to larger companies, such as hospitals, where there is mass amounts of data and information. Over the years, ransomware attacks have been made on businesses large and small, and many are not sure how these attacks happen or how to prevent them.

As a local business owner, knowing where to start is the first step in protecting your customer data. Here are some answers about ransomware and how you can protect your business against an attack.

How Does a Ransomware Attack Happen?

Typically, ransomware attacks happen due to one of two reasons: opening encrypted attachments in emails and downloading from unprotected websites. While unsuspecting, these are the two main vehicles that criminals use to infiltrate your database.

When it comes to websites, there are many ways that an attack can take place. You or someone in your company could be using a company device to download items from an unfamiliar website or you could be downloading items from a website of a trusted source that has already been infiltrated by cybercriminals. By downloading a document or other digital items, hackers can easily access your database and customer information.

Fraudsters and scammers have long used email as a way to manipulate people into giving out personal information, and ransomware is no exception. Cybercriminals planning a ransomware attack via email usually pose as a familiar person or company and prompt users to open an attachment filled with ransomware. Opening attachments is a way that criminals can infiltrate a computer system, as it automatically downloads attachments onto your device, a clear path into your database.

Both ways are used and should be monitored, as many people do not know that criminals who want to access company data are waiting for you to make one wrong click.

How Can I Prevent a Ransomware Attack?

One of the best ways you can prevent a ransomware attack is to educate your employees. No one intends to visit a website that is filled with ransomware or open an attachment from an untrusted source, however, it happens every day. Inform your employees about what to look out for and how to navigate situations that they may come across. This will significantly decrease your chances of becoming a cybercrime victim.

Some ways you can engage and educate your employees are:

- Having a Q & A with your IT department
- Finding a reliable source of articles or blogs about the topic and printing them out for employees
- Having a third party employ tests for employees, to demonstrate how easy it is for people to get into your database.

Additionally, there are some cybersecurity procedures that you should implement business-wide to protect your business from being attacked. Procedures to implement include:

- Never opening attachments or clicking on links from an untrusted source
- Never downloading items from an unfamiliar website
- Updating devices immediately when security updates are available

These are simple ways you can ensure safety of your company and your data. Protecting your company from a ransomware attack is everyone's responsibility, and ensuring that your employees are aware of how attacks happen, as well as implementing safety precautions, will lessen the chances of your business being attacked.

Here at Blackhawk Bank, we want to ensure that you have peace of mind while helping customers day by day. Want to learn more about Blackhawk Bank? Contact us today!