Here are some simple ways to protect your business from ransomware attacks.

What is ransomware?

It’s software.

Cybercriminals trick you into downloading it.

Once in your network, it encrypts your files, locking you out of your own system.

Criminals hold your data and files hostage.

If you pay the ransom, they give you the key to unlock the files.

If you don’t… goodbye data.

Or worse: Your data (and your customers’) gets sold on the dark web. That can lead to lawsuits, competitors getting the edge on you, or even going out of business.

Who should worry about ransomware?

How does my system get infected?

Are you a business with at least one employee – even if you’re the sole employee?

Then you should be worried.

In fact, smaller businesses can be extra-attractive targets. Criminals think, “Maybe this small or medium business hasn’t had the time or resources to set up a solid defense. Easy pickings.”

Have you ever… opened an email? …downloaded an attachment? …visited a website?

No matter how innocent and legit it looks, any of these could deliver ransomware into your network.

Why is ransomware such a common attack?

Simple. It works.

One click. And they’re in.

Powerful. When your business suddenly stops, revenue stops, and you might be desperate enough to pay whatever it takes to liberate your network.

ROI. Cybercrime is a business, too. And the criminals want a return on their investment (ROI) – which they can often get.

How can I protect my business?

Here are some simple ways to protect your business from ransomware attacks.

Fast Facts: Ransomware

No business is too small for a ransomware attack.

Facts:

Here are some facts you don’t want to know about ransomware: a growing business in all sizes, and nearly any industry. It’s so easy for a cybercriminal to compromise a company’s data that it can seriously impact the business.

Myth: Ransomware attacks only happen to big businesses.

What is ransomware?

Ransomware attacks are too.