Small Businesses
Big target for cybercrime

Protect your business before it's too late

Small business owners used to have to watch for thieves who worked at night and carried a crowbar. Today, they are under attack by criminals on computers that are thousands of miles away.

Many attacks on small businesses are done with malware. First, the malicious software lands on a computer at the business. Then it quietly gathers data (such as credit card information) and sends it secretly to thieves over the internet.

Once a thief has the data, he can quickly turn it into cash. He can sell it on the black market, or he can make purchases and phony credit cards. The end result is the same: the business bank accounts are emptied, and the thief never even sees the building.

Your business is a target

The news headlines are filled with cyber attacks on big retailers. But small businesses are far more likely to be hacked. Why? Because most have almost no network security. They are an easy payday for thieves.

Two out of three data breaches last year hit small businesses[1]. An astounding 96% of successful attacks on payment card systems hit small businesses[2]. It's undeniable - small businesses are a prime target for hackers

How can cybercrime hurt your business?

Empty bank accounts – Using malware, phishing emails and other techniques, hackers can empty bank accounts from across the globe. Many small companies hit by this type of attack are forced to close.

Steal credit card data – Criminals can quickly turn a list of credit cards into cash on the black market. When this happens, the business can be hit by massive fines and lose a tremendous amount of trust from customers and partners.

Knockout computer systems – Cyberthreats can even knock your computers offline. How much would it cost your business if the network went down for a day? How about a week?

Secretly take control – Cybercriminals control millions of computers in the U.S. alone. The people who own the computers have no clue. They are used for illegal activity such as attacking businesses and sending out viruses.

Slow down performance – Have you ever had a computer slowed down by malware or adware? Many of these programs are designed to spread across your network. That can slow down your entire business.

Wipeout files – Some malware, called "ransomware," can find important files on your network, lock them, and demand a ransom payment (in real dollars) to unlock them. If the ransom is not paid in time, the files are lost forever.

Protect your business

The good news is that small businesses can prevent these attacks by having good computer and network security. Not sure if your security is good enough? Call our team of experts.

We specialize in helping small businesses secure their computers and networks so they can rest easy and focus on business.

1. Source: Verizon 2013 Data Breach Investigations Report.
2. Source: Visa 2010 Franchise Data Compromise Trends and Cardholder Security Best Practices

AVAREN