Three simple steps to defend your business from cyberattacks

Here's the good news: preventing a cyberattack is infinitely easier than trying to recover from one.

Many small business owners have an "it won't happen to us" attitude toward hacks, ransomware and other types of cybercrime, believing they are too small to be a target. Others realize the importance of cyber security but feel they don't have the resources to make it a priority. These are some of the reasons why **a staggering 90% of small businesses haven't established any protection for their company's or their customers' data.**[1]

Cyber criminals have caught on to these vulnerabilities—in another recent survey, more than one out of five small businesses reported experiencing a cyberattack.[2]

It can take months to realize you've been a victim of a cyberattack and by then significant damage is done—between an average $84,000 and $148,000 in costs, not to mention the erosion of customer trust.[3] Too often, that damage is insurmountable—a 2017 Better Business Bureau study found that "only 35% of businesses could remain profitable for more than three months if they permanently lost access to essential data."[4]

STEP 1

Tighten Access

Hackers have become very skilled at getting around passwords, either by figuring out how to guess them or how to steal them. That's why security experts recommend adding another layer of protection in addition to a password, often called "two-factor authentication" or "multi-factor authentication." Adding this second barrier is an effective way to keep hackers out. Some examples of multi-factor authentication (MFA) that are often used on either computer hardware or popular websites and applications include:

A four-digit PIN or a secret answer to a question, like: "What was the name of your first pet?"

A unique code sent via SMS/text message (the most popular form of MFA).

Biometric sensors that allow for incredibly fast, personalized access, such as retina scanners, facial recognition or fingerprint readers. For example, Latitude laptops and select Vostro PCs with Windows Hello allow users to securely log in with just a touch or a look.

STEP 2

Spot and Avoid Threats

"Malware" is short for "malicious software." It's an umbrella term that includes a host of nefarious invaders—spyware, viruses, Trojan horses, rootkits and ransomware, just to name a few. Disruptions can range from computer crashes, to identity theft, to a network-wide shutdown in the case of ransomware, where the attacker locks you out of your data until you pay them a ransom.

One of the most common ways malware infiltrates an employee's system is through a phishing email. These are emails posing as legitimate, but if your employee clicks on a link within that phishing email, they could be prompted to give up sensitive information or malware could breach their system. Educate your employees on the importance of scrutinizing emails and URLs for anything that looks suspicious (like misspellings in a URL) before clicking on them.

McAfee

In addition to employee vigilance, software companies like McAfee offer seamless protection that runs automatically in the background, scanning for all types of threats and eliminating them before they have a chance to infiltrate. A comprehensive software package can also warn users about risky websites and help prevent dangerous downloads.

STEP 3

Have a Back-up Plan

Small business owners come to expect the unexpected— mistakes happen, systems crash, surprises pop up. While the first two tips we explored above will eliminate a large number of threats, a breach is still possible. If you've been using a back-up system, you'll have a much easier time recovering your data. There are two major back-up solutions—hardware such as storage drives, or cloud-based storage on offsite servers.

External hard drives are simple to use—you just plug them in, download your data and then store them away. The drawback is that they require a filing system and they take up physical space, which means there's a chance of them being lost or damaged.

mozy BY DELL

Alternatively, cloud data protection from companies like MozyPro offer a convenient solution that eliminates the headache of manually downloading your data onto hard drives and physically storing them somewhere.

Once you upload your files, MozyPro automatically detects changes and saves them in the cloud, syncing edits across all your devices. It also keeps your data safe with military-grade encryption and provides an added layer of protection against ransomware attacks. A ransomware attack only works when you have no other way to access your data, so cloud data back-up renders a ransomware attack ineffective.

Have questions? Dell Small Business Technology Advisors are ready to help with dependable security solutions to help keep your business protected.

SPEAK WITH AN ADVISOR TODAY:

877-BUY-DELL

CLICK | CALL | CHAT

[1] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [2] https://www.bbb.org/stateofcybersecurity/

[3] https://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron | [4] https://www.bbb.org/stateofcybersecurity/