Cyber-attack: Is your small business at risk?

Everyone knows that having a cyber-security plan is important for large corporations. What they don't realize, however, is that small businesses are particularly vulnerable to cyber-attack and therefore frequently targeted.

If you are a small business owner, you are probably wondering what you can do to protect your business. First, let's look at some common types of scams targeting businesses.

Phishing

Phishing is a type of scam that targets critical private data, such as passwords, credit cards and private data. By enticing a recipient to click on something apparently innocuous in an email or a text, hackers can activate malware or redirect the recipient to a form that's designed to collect sensitive data.

In some cases, even opening an email can trigger malicious software.

OK, so we all know not to send money to a prince in Zimbabwe, but do your employees know how to identify sophisticated phishing emails? Even though more and more computer users are aware of this problem, phishing techniques are becoming more sophisticated by the day.

Common techniques include fake receipts from vendors you frequent, fake emails from your IT department and innocent links from people that seem to know you.

If you suspect that you have been phished, immediate steps must be taken to lock out potential hackers and protect identity information. However, irreparable damage may have already been done.

Ransomware

Business runs on data, even when your business is far from the tech industry. The records and data you need to run your business—from payroll to inventory to financials—have become so critical that losing it, even temporarily, can be almost catastrophic.

Scammers have taken advantage of this new vulnerability by launching thousands of ransomware attacks every year.

What exactly is ransomware? It is a malicious software that locks users out of the system, returning control only when an electronic payment has been made.

The data is not always stolen—it's likely valuable only to you—but the ransom demand generally appears less costly than the loss of ability to conduct a business. Only when this occurs does the business discover that some of their most valuable assets have been left exposed.

Protecting your business

The key elements of a cyber-security protection plan include:

1. Ensuring that equipment and software are not obsolete

The vulnerability associated with outdated software and hardware is one of the main ways hackers access networks.

2. Using state-of-the-art anti-virus software

When it comes to anti-virus software, you'll notice there are many free and low-priced options on the market, but you would be wise to avoid using them as all are inadequate for business computers. Some are essentially viruses themselves.

3. Data backup plans

Businesses that back up their data every day can laugh in the face of ransomware, power surges and machine failures. In fact, not backing up your data, especially in this day and age, could be considered foolhardy.

4. Lockout procedures

In the case where sensitive data, such as passwords, credit cards or personal data, has been compromised, detailed contingency plans should be in place so that the response can be as immediate, controlling damage and liability as much as possible.

5. Informed users

Everyone who uses your business computers needs to be oriented to the risks and potential damage of cyber-crime. Even though cyber-crime is not new, many sophisticated techniques are evolving every day. It is critical, then, that staff receive cyber-security training from an IT professional, which can take as little as 15 minutes.

The best practices of cyber-security are simple, but essential.

Want to learn more? Need help with your business computers and/or establishing a cyber-security plan? Contact Kootenay Computer today.