ASK THE EXPERT

Why an Increase in Amateur Hackers is Bad News for Small Businesses

We don't hear about small businesses being hacked in the news. Small business hacks do not make headlines. They are not known nationally. They don't affect 1 billion users. But they are big targets for hackers. According to smallbiztrends.com, 43 percent of cyber-attacks are against small businesses, and 60 percent go out of business within six months of a cyber-attack. These numbers will grow this year, particularly due to the efforts from phishing campaigns and ransomware.

It is estimated that ransomware is a billion dollar industry, and growing. If you're not familiar with ransomware, that's because you haven't been hit with it…yet. Ransomware is malware that is downloaded onto your computer and encrypts your files. When you try to access that information, you find a ransom note instead requesting payment in bitcoin, a form of digital currency. If you pay the ransom, the decryption key will be sent to you and you (hopefully) will get your files back. Without data back-ups or cyber extortion insurance, you will be forced to make the decision to pay the ransom or spend hours recreating the data. There is a reason why this billion dollar industry is growing. Ransomware has gotten more sophisticated. Some ransomware can act as a distraction while additional malware is installed. This additional malware can record key strokes – such as user names and passwords. Once your credentials are stolen, the possibilities are endless regarding what hackers have access to. And because this has become such a lucrative business for these thieves, new amateur hackers are popping up everyday.

Employees are rapidly becoming small business' biggest security vulnerability, when they should be their biggest defense. If you're not sure where to get started, it may be time to look for **cyber/data breach insurance**. It is so important to obtain options. Not all **cyber/data breach insurance** is created equal, especially is such a rapidly growing area. You should look for coverage for cyber extortion, business interruption, data breach expenses that include forensics, credit monitoring, public relations, and more. Does your quote include coverage for regulatory action, fines and penalties? What about Payment Card Industry fines and penalties? In addition to assisting with ransomware attacks, forensics for malware, compensation for lost business resulting from a hack, etc., most cyber carriers can also provide risk management services – including policies to implement and improved training for your employees. Contact your trusted independent agent today to help you navigate through the world of cyber insurance.

Contributed by Meredith Bennett, RPLU, AU, AIT , Usli

Next Month's Ask the Expert Topic:
April Showers Could Bring May Floods - Are You Covered?