Tips to Assist Understanding Ransomware*

Ransomware is now considered a fact of life in today's cyber security landscape, but that doesn't mean businesses are protecting themselves from a potential ransomware attack or even know it's a possibility. Often, users only recognise a ransomware threat after it's too late. In February 2018, according to Osterman Research and Barracuda there was one phishing attempt in every 3,331 emails and one piece of malware for every 645 emails. And falling for one of these emails can be costly.

According to IBM's Data Breach Report 2021, the average cost of a ransomware attack is $4.62 million (up from $4.44 million in 2020), and the average breach lifecycle is 287 days (up from 280 days in 2020). This means that not only are ransomware attacks becoming more expensive, but they're also taking longer to resolve.

Businesses need to start protecting themselves from the growing threat of ransomware. Becoming educated about the threat of ransomware and learning these important tips is an important first step.

1. Put Technical Safeguards in Place

As a best practice, have an intrusion-prevention system and security software running on your computers. This should include antivirus software, firewalls, and spam filters. Then, make sure all security patches are up to date, and deploy new patches on a regular basis.

It's also critical to have a backup solution in place and frequently test the backups running on your systems to make sure they're working properly. If you're hit with ransomware, you'll want to restore operations as quickly as possible, and having a recent backup to recover from will save you both time and money.

2. Ransomware Training

Even with technical safeguards in place, it's employees who are ultimately at risk of exposing a business to ransomware. User error, such as clicking on an infected online advertisement, pop-up window, or attachment in a spam email, is often to blame for inviting ransomware into a computer. Therefore, educating your employees and system users is the most important line of defence.

Talk with your employees about ransomware and educate them on what it is and how they can help defend the business. Try getting the whole staff together for a training session, for example, bring lunch to make it a Lunch-and-Learn event.

As a best practice, businesses should require all new employees to complete the training and offer it on an ongoing basis to avoid information being missed. If you don't have the resources to put this type of training together, talk to your IT service provider. They should be able to run a program like this for you or provide other educational materials.

3. Provide Examples to End Users

The most effective way to educate your employees on ransomware is to show them examples of what it looks like, so they'll know the warning signs and be able to identify a suspicious message or attachment before they click on anything. For example, you can share with them a Phishing Quiz, which includes examples of infected and legitimate emails and provides explanations of how to tell the difference.

Once ransomware has infected a computer, a message is displayed on the screen letting the user know their machine has been compromised.

It's helpful to share this type of information with employees as well so that, even if it's too late, they'll know to alert management and ask for help.

4. Encourage & Respond to Feedback

Oftentimes, employees will find less secure workarounds to accomplish their tasks because the business's systems are too restrictive. Maybe they feel they can get their work done faster if they bypass the company firewall to access a website that's been blocked or download an application that isn't allowed. Or maybe they'll save sensitive files to a personal USB drive because they can't access them from home or on their mobile device. Encourage your employees to bring these types of concerns to your attention so that you can work together to find solutions that will meet their needs without compromising security. In order for your employees to feel comfortable coming to you with questions or concerns, you need to set up an open-door policy and foster an environment where feedback is always welcome.

*With thanks to Lanrex Technology

Disclaimer: This article is general in nature and is designed to provide helpful general guidance on some key issues relevant to this topic. It should not be relied on as legal advice. It does not cover everything that may be relevant to you and does not take into account your particular circumstances and you use it at your own risk. Logical Insurance Brokers specifically disclaims any liability, whether based in contract, tort, negligence or otherwise, for any direct, indirect, incidental, punitive, consequential or other damage arising out of or in any way connected with the use of or reliance on the content of this article. It is only current as at the date of release. You must ensure that you seek appropriate professional advice in relation to this topic as well as to the currency, accuracy and relevance of this material for you.

Logical Insurance Brokers is a
division of Insurance Logic Pty Ltd.
AFSL No: 237633
ABN: 44 002 859 252

t 02 9328 3322

e team@logicalinsurance.com.au
w www.logicalinsurance.com.au

Suite 21, Level 2, 8 Hill Street,
Surry Hills NSW 2010
PO Box 103
Darlinghurst NSW 1300

Steadfast
STRENGTH WHEN YOU NEED IT

NIBA
National Insurance Brokers Association
MEMBER

Page 2 of 2

October 2022