texaport

The Impact of Spam Emails on Businesses

Spam has a negative impact on any organisation, from decreased productivity and resources to overwhelming employees. To stay competitive, businesses must proactively protect themselves against it.

In this article, we'll explore how spam can negatively affect businesses and look at ways to protect your business from increasingly sophisticated spammers.

What is spam, and how does it affect businesses?

Spam is a blanket term for unsolicited and unwanted emails. It affects businesses by clogging up inboxes and causes recipients to delete emails without reading them, potentially leading to missed opportunities. It can also decrease customer loyalty as people expect companies to protect their data and privacy.

Fortunately, there are solutions such as spam filters that reduce the amount of these messages – but some spammers find ways around the

and continue to send damaging or offensive content into networks. Therefore, businesses must stay vigilant. Spam represents over 50% of email traffic, which is the most intrusive method cyber criminals use to introduce malware to business systems.

This can greatly interrupt workflow and decrease business efficiency.

Common types of spam

Spam can range from phishing emails with malicious links, surveys, and competitions to unsolicited messages about money-making opportunities or fake products and services.

People should stay aware of these threats and always double-check sources before proceeding with any requests – clicking on the wrong link could have serious consequences.

The risks associated with spam

Spam emails can cause individuals and businesses many problems if they are opened and responded to. By opening this mail, the reader confirms that their email address is active and valid and could download malware onto their device by clicking malicious links. Additionally, responding can result in personal information, such as banking details, being stolen.

Suffering a distributed denial of service (DDoS) attack is another risk. This is when a hijacker obtains information through spam that overloads your network bandwidth causing long periods of downtime.

These risks help to highlight the importance of cyber security in your organisation. If spam management isn't part of your existing cyber security plan, it's time to add it in.

texaport

How to identify and prevent spam

Identification

Common signs to look for in determining if spam is trying to reach your mailbox include offers that seem too good to be true, requests for large sums of money, or communications from someone acting suspiciously. If you receive any of these communications, you should talk to colleagues and do your research before responding. You should also report the spam to your IT department – check your cyber security policies so you know what action to take.

Prevention

These simple steps will help you protect yourself against scammers and give you peace of mind.

Use email filtering software to set up effective measures against phishing.

Protect your accounts and stay wary of digital scams with the help of employee cyber security training and refresher courses, and by using email filters to.

Stay sceptical. Even when emails appear authentic, double-check before clicking anything.

Don’t click on links within or respond to spam.

Use trusted antivirus software to ensure that malicious software doesn’t enter your computer. This is often how spammers get access to your emails.

Never give out your email address unless necessary. If possible, create an alternative dedicated account for activities like online shopping that

require sharing it.
texaport

Benefits of filtering software

With over one million malware threats released every day, it's important to implement filtering software within your business.

The main benefit of using anti-spam software is its ability to prevent malicious emails from reaching your inbox, preventing potential damage to sensitive communications and confidential information. Using it can also improve your general data security defences against phishing attacks, viruses and other malicious threats by blocking suspicious emails before they reach employee inboxes.

It also makes it easier for businesses to ensure that their communication policies are being adhered to and that a consistent brand message is projected throughout all stages of communication.

Create a secure environment for your business communications

Take action to protect yourself and your company from the potential risk of scams. Make time to understand what spam is, what it can look like, and how you can implement best practices to monitor and manage it to build a safe environment for your business communications.

‹ Back to blog

CYBER SECURITY