

Email Security

The Ten-Step Guide for Small Businesses



Ten steps to email security

Small and medium-sized businesses today face a growing number of email threats — from spam and unacceptable content to viruses that can bring their operation to a grinding halt.

So how does a business go about getting affordable protection?

The pivotal problem is that not all email security solutions can keep pace with the escalation of email threats. According to Maurene Caplan Grey, Research Director at IT research consultants Gartner: "Today's measures are based primarily on reacting and responding to email threats once they hit the enterprise. To defend against the dynamic and changing nature of threats such as viruses and spam, enterprises must be equipped with proactive and more intelligent defence solutions."

This is a quick guide to achieving just that.

1

Create an enforceable email security policy

Management resources must be dedicated to develop and implement a coherent, enforceable policy. At its most basic, the policy should set hard-and-fast rules to guard against damage to the system and cover:

- Rules for permitted use
- Virus and content filtering
- System monitoring and privacy
- Confidential information and trade secrets
- Prohibited, illegal, licensed and copyright material
- Sexual harassment, discrimination and defamation
- Guidance on professional email usage
- Reporting of incidents and vulnerabilities
- Rules on policy enforcement
- Review and evaluation procedures

2

Use an email security solution that operates outside your network boundary

You must stop threats before they enter your enterprise. This can only be achieved by a managed email security provider, with the equipment and knowledge to keep one step ahead of the cyber criminals. Using PC-based software or dedicated appliances is no answer.

3

Secure outbound email as well as inbound

Many viruses, much malicious content and spam, are unwittingly passed on from one company to another, so you must be able to detect and stop threats before they leave your system.

4

Get complete email protection and control

Your email security provider must give you protection from multi-level email threats and enable you to control content entering and leaving.

For instance, the predominant email security trend during the first half of 2004 has been "convergence" — where virus writers and spammers combine to produce a more sophisticated breed of email threat — a huge risk for businesses without expert protection.

Without the proper email usage controls in place for your users, damaging and expensive problems can all too easily arise — from defamation and libel, to obscenity and sexual harassment and even breaches of corporate confidentiality or contractual liability.

5

Get proof the solution works

Many claims are made for email security solutions. Set demanding service level agreements for effectiveness and accuracy from your service provider and ask for credible references from businesses similar to yours.

6

Avoid disruption when switching to the new solution

Your service provider should survey and understand your email system configuration and requirements. This ensures minimum disruption to end users and the continuity of the business.

7

Understand the true capability of the service provider

With email security such a rapidly-growing problem, many IT suppliers have their capability stretched to the limit. How do you make sure a company is up to the job?

- Expect your service provider to have highly-trained expert staff to develop, monitor, manage and administer the service
- The technology should be proven and not rely on single techniques which could leave you vulnerable
- Your service provider should have an infrastructure that can deliver email during peak loads and major outbreaks as well as being able to process email across the globe.

8

Get the service to fit your business requirements

All businesses differ. You must have an email security service which:

- is adaptable to your needs
- meets the requirements of your information security policy and email usage policy
- can flex and grow along with your business
- fits your existing email systems and won't cause disruption when it's turned on.

9

Be sure you can predict the cost of the service

A predictable monthly cost, agreed before you start, enables you to plan your business effectively — with no add-on costs for software licences, hardware or dedicated IT staff.

10

Stay in control with good monitoring and reporting

You are making the service provider responsible for clean email. Be sure you can monitor and fine-tune the service if required and expect detailed performance reports.

So what's next?

- From now on you should be able to relax and expect all your legitimate email as before — but none of the bad stuff.
- You hear about a new virus or scam and remain relaxed — you're automatically protected.
- You no longer worry about staff abusing your usage policy and putting the company at risk.
- You're in control, and you've fully costed the service.
- You can also tell the rest of your management team that — despite being a small business — you now share the same email protection service as some of the world's best known companies.



MessageLabs is the leading provider of managed email security services for small businesses. Operating at Internet level, we offer industry-leading protection for over 5,500 small businesses in the UK alone, against threats such as spam, viruses and other unwanted content. MessageLabs' managed services are backed by a multimillion-dollar infrastructure spanning four continents, which proactively protects your business from global threats on a local level.

MessageLabs Ltd

1260 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB, UK

T +44 (0)1452 627627

F +44 (0)1452 627628

Freephone UK 0800 917 7733

www.messagelabs.com