



MessageLabs[®]

Be certain

Everything you need to know about email and web security *(but were afraid to ask)*

A Non-Technical Guide For Owners And Managers
Of Small To Medium Sized Businesses

Table of Contents

Understand the risks	3
'It can't happen to me.' Really?	3
Viruses, spam and phishing	3
Inappropriate content, employees behaving badly	4
How to assess your risks	5
What to do about it	5
The MessageLabs Solution	6

Understand the risks

What you don't know can destroy your business. It's hard to imagine modern business without the internet but in the last few years it has become fraught with danger. Internet crooks are the dotcom entrepreneurs of crime, using the power of computers and the interconnections of the network against innocent businesses to make money.

Make no mistake; viruses, spam and spyware are the products of a global 'business' that is worth as much as \$60bn a year. To put that into context, online crime is bigger than the global drugs trade. With so much money at stake, it's not surprising that the problem is getting worse.

The risks are only part of the story. Internet security is also a competitive advantage. Customers and suppliers want you to care about their privacy and protection. Who will pick up your customers if a computer security incident hits your business? IT security isn't just good practice, it's good business.

IT security isn't
just good
practice, it's good
business.

'It can't happen to me.' Really?

Many businesses, especially those with little or no IT support, tend to put a low priority on protecting themselves. Ironically, this makes them more attractive targets.

Consider the accounting firm that was infected by a virus because their anti-virus software wasn't up to date. It took them days to clean up their computers, and their reputation suffered because their computers turned into 'zombies' which send out spam emails to all and sundry. The repairs cost thousands, but the damage to reputation is incalculable.

Imagine a manufacturing business where certain employees downloaded pornography in the office. It sounds like a cringe worthy episode of The Office. But if an employee took the company to an Employment Tribunal for permitting a degrading and offensive environment it could turn into a serious waste of management time, with a substantial fine to make it worse. It can happen. In one recent case, a tribunal found an employer guilty of sex discrimination because employees were looking at pornography in the room where the complainant worked.

Internet crime affects nearly two-thirds of British firms, according to a DTI survey. The average serious incident can set you back between £8,000 and £17,000. The good news is that an ounce of prevention is worth a pound of cure.

Viruses, spam and phishing

According to MessageLabs' analysis of over a billion emails a week, one email in every one hundred contains a virus. One in nearly two hundred are fraudulent phishing emails. Seven in every ten contain spam. Put simply, unless you protect yourself properly, email and web access is always going to give you problems.

But what do these terms mean for business? If 70 percent of email is unwanted spam advertising, it means 70 percent of your email server's capacity and 70 percent of the bandwidth you give to email is wasted. Email seems 'free', but you pay for servers and internet connections. Wouldn't it be better to cut off the flow of spam before it reaches your network? That way you keep the bandwidth and server capacity for your business not the criminal's.

Phishing emails are more dangerous. They are used to trick people into giving away private information on fake (but highly realistic) websites. A common example is to persuade people that they need to log into the online bank account and sort out a bogus transaction.

Criminals use these sites to get bank account numbers, passwords and credit card information. Another common trick is to get employees to log into a fake company website, so that criminals can get user names and passwords to log into your network. The risks of business fraud are obvious. Some of these fake sites are so realistic even experts can tell them apart from the real thing. Wouldn't it be better if these emails never reached your employees?

However, the worst threat comes from malware. Call them viruses, worms, trojans, spyware - they all spell bad news. Malware is an unwanted program written by criminals running on a computer in your business, and that's a never good idea.

What sort of damage could this do? Viruses can give hackers remote access to your data and remote control of your systems. They can also be used to launch criminal attacks on other computers. They can send out thousands of spam email messages. They can infect other computers. Worst of all, they can do all this without any outward sign that something is wrong. Other kinds of viruses display intrusive adverts for pornography and gambling, and even disable security software. If there is a way to make money from your computers, there is a virus that will do it.

Viruses spread in email attachments, when people visit certain websites or simply spreading from computer to computer on the network. The only way to be safe is to be 100% virus-free.

The only way to
be safe is to be
100% virus-free.

Inappropriate content, employees behaving badly

Then there are also pressing legal, productivity and reputation issues:

- What if an employee inadvertently defames someone or binds the company to a damaging contract by email?
- What if someone takes you to an employment tribunal claiming a hostile working environment? Damages in discrimination cases are potentially unlimited.
- Do you want your employees downloading pornography or other inappropriate content on work computers? It'll probably happen – the majority of visits to pornographic sites occur during office hours.
- How much productivity can you afford to lose to 'cyber slacking' – employees browsing non-work related websites on company time?
- What would happen if an employee sent sensitive information to a competitor or disclosed confidential information to an unauthorised person by email? Would you be able to enforce company policies, or even track the breach? One of the eight principles of the Data Protection Act is that personal information must be 'secure'. Reckless disclosure is a criminal offence.

These are important questions. The problems behind them are not the result of outside attack but reputations still suffer, clients still leave and careers still crash and burn. Companies need to write and enforce acceptable use policies, and they need technology to help them do it.

The first step is not about technology - it is about asking some simple business questions.

How to assess your risks

Security starts with putting a business value on different kinds of risks so that you can allocate resources to reducing them. It makes sense to prioritise: you don't have an infinite IT budget, and some risks are more threatening than others. Therefore, the first step is not about technology - it is about asking some simple business questions.

What are you trying to protect? Typical issues include legal requirements, such as the Data Protection Act, and professional obligations such as client confidentiality. Then there are straightforward business issues. Nobody wants to publicise sensitive information like plans, lists of potential customers and so on. You may have mission-critical systems such as your email, ecommerce site and accounting records. Don't forget intangibles such as management time, IT resources, your company's reputation and morale.

What are the risks? There are external risks, such as viruses and hackers. There are legal threats, such as the risk of employee misbehaviour landing you in an Employment Tribunal.

Who is responsible for IT security? It is not enough to delegate the question to your IT department or supplier. You need to see IT security as a business-wide issue and address it at a board level. If you know what you want to protect and what the risks are, setting priorities, delegating responsibility and allocating budgets all fall in line with what is important to the business. Which manager is going to take the lead? Who is responsible for creating and implementing a plan? What budgets are available and appropriate? For example, compare your IT security budget with your insurance costs.

Where's the plan? Even if it is a couple of pages, an IT security plan is the first step to protecting your business. It's better to have a good plan now - and carry it out - than a perfect plan next year. Do you have the right software and technology? Do you have appropriate staff policies and training? What is the budget and timetable?

What to do about it

So far, we've talked about the business risks and taken a management view of IT security. Now we're going to talk about the steps you need to take to protect yourself. You can use this checklist as a starting point.

- **Virus and spyware protection.** You need to stop viruses and other unwanted programs from getting in the door. With thousands of new virus variants materialising each month, it is critical that your protection is able to keep up with new and previously un-known threats as they emerge.
- **Spam filtering.** Blocking spam will save employees time and reduce the risk of fraud from phishing emails.
- **Firewall.** A firewall will stop viruses that spread directly over the internet, and it can also keep hackers away from your network and servers.
- **Access control.** Make sure that employees only have access to the information they need to do their job. To give an obvious example, don't let the whole company have access to payroll records.

- **Policy enforcement.** You need effective staff policies about employee use of the internet backed up with training that covers policies and practical matters such as the use of strong passwords. Technology can help enforce company policies on appropriate use of the internet, such as bans on downloading inappropriate images or sending certain information by email.
- **Encryption.** Consider encrypting data on laptops and other portable devices to prevent thieves accessing sensitive information if they are stolen. Also, consider email encryption to protect the confidentiality of messages between your business and its partners. By default, email travelling over the internet is not encrypted which means that it can be read – like the text on a postcard – as it moves from sender to recipient.
- **Physical security.** Don't forget that a stolen server is as much of a risk as a virus-infested one. Locks, alarms, secure server rooms and visitor access control are all part of IT security.
- **Backup.** Critical data, including email archives and business databases, need to be regularly backed up with copies stored offsite. Test the restore process regularly too.
- **Software updates.** Make sure that all the computers in your business are kept up to date with manufacturers' updates. These are published regularly by the major vendors and fix known flaws and vulnerabilities. Virus writers exploit these vulnerabilities to attack people who do not update quickly enough.

An NOP survey of 5,000 IT professionals and finance directors was conclusive: MessageLabs ranked first in overall satisfaction, ease of integration, reliability and return on investment.

The MessageLabs Solution

MessageLabs specialises in protecting businesses from internet messaging and web threats, scanning a billion emails a week for viruses, spyware and spam for 15,000 customers in 80 countries worldwide.

MessageLabs deals with the problems before they even reach your network. Spam, viruses and inappropriate content is stopped at the 'internet level'. MessageLabs service is backed, 24 hours a day, by industry-leading support.

Don't take MessageLabs' word for it. An NOP survey of 5,000 IT professionals and finance directors was conclusive: MessageLabs ranked first in overall satisfaction, ease of integration, reliability and return on investment.

The MessageLabs service combines three components:

- **MessageLabs Protect.** This provides multi-layered protection against email and web based viruses, malware, spam and phishing scams.
- **MessageLabs Control.** This identifies and controls confidential, malicious or inappropriate content in inbound and outbound email, URL filtering and content management web services. It also checks emails for pornographic images and blocks them.

- **MessageLabs Secure.** This uses encryption to allow users to send emails that are completely confidential and secure to your employees and trusted partners. Unlike many encryption systems, this is completely transparent to users – they don't need to become cryptographic experts.
- **MessageLabs Recover.** MessageLabs Archiving Service provides an easy to use archive for email, comprehensively addressing the requirements for regulatory compliance, legal discovery, and email management – collectively reducing the risks and limiting the liability businesses face.

For more information about MessageLabs world leading services for email, web and instant messaging (IM), visit www.messagelabs.com/services.

www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
FeringasträÙe 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

© MessageLabs 2006
All rights reserved

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300