



# >MESSAGELABS END USER IT SECURITY GUIDE

>WHAT STEPS CAN YOU TAKE TO KEEP YOURSELF,  
YOUR COLLEAGUES AND YOUR COMPANY SAFE ONLINE?



## **>CONTENTS**

**>WHAT IS MESSAGING AND WEB SECURITY? >P1**

**>EMAIL THREATS >P1**

>VIRUSES >P1

>SPAM >P1

>PHISHING >P2

>DOS & DON'TS >P3

**>WEB THREATS >P4**

>SPYWARE >P4

>DOS & DON'TS >P4

**>IM THREATS**

>INSTANT MESSAGING >P5

>DOS & DON'TS >P5

## >WHAT IS MESSAGING AND WEB SECURITY? AND WHY IS IT IMPORTANT?

Email, the web and instant messaging are all important methods of communicating and exchanging vital business information. While the benefits of these technologies are great, enabling us to communicate and exchange information with practically anyone, they also present a real threat to our security, productivity and profitability.

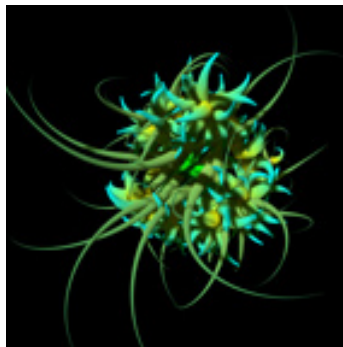
This short guide to messaging and web security outlines the main dangers and the steps you can take to make sure you and your company stay secure.

## >EMAIL THREATS AND HOW TO PROTECT AGAINST THEM

### >VIRUSES

Viruses are one of the most common threats from email. You may also have heard the terms 'worm' or 'trojan', these are essentially different types of viruses. In essence, a virus is a program or programming code that replicates itself by being copied, or initiating its own copying, to another program, document or part of your computer.

Most viruses spread by enticing people to open an innocent looking email and/or attachment, which actually contains the virus. Viruses are particularly dangerous because they often arrive in emails from people you know, sending themselves on to all of the people in your address book.

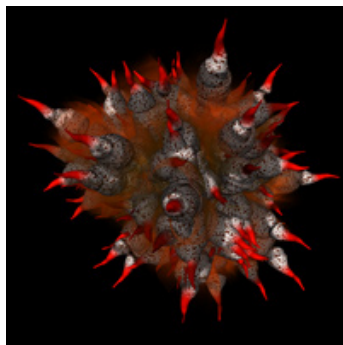


>MYDOOM  
>EMAIL WORM

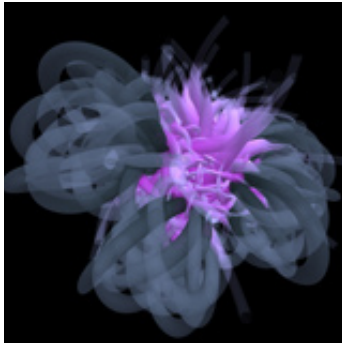
### >SPAM

Billions of spam emails are sent every day, making it a huge problem. Spam has become such a familiar, not to mention annoying, feature of the email landscape that it's easy to forget the damage it does to a business.

Put simply, spam is no longer simply a nuisance. It significantly affects business efficiency and productivity. Think of the amount of time you spend during the course of a year identifying and deleting spam emails. These messages clog up your inbox, requiring more expense and effort to safeguard against the relentless tide of spam.



>RUSSIAN3  
>SUBJECT: EVER HEARD THAT  
YOU'RE GETTING FAT?  
>TEXT AND IMAGE-BASED SPAM



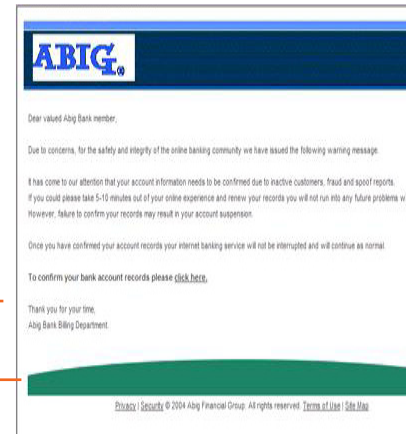
>PHISHING5  
>SUBJECT: ACCOUNT  
NOTIFICATION!

## >PHISHING

A phishing email is designed to look like a genuine email from your bank or other financial institution. However, it will in fact lure you to a fraudulent website where you will be asked to enter your bank account or credit card details. Phishing emails are particularly dangerous because they are a social engineering technique and will in many cases look like the real thing.

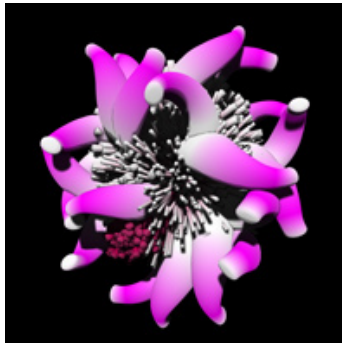
Remember, no bank or financial institution will ever ask you to confirm your account number and login details in an email.

- The email design is spoofed to resemble a well known brand (in this example we have simulated a bank)
- Phishing emails will often direct you to a false site and ask you to confirm your account information
- The false site is made to look like the real website
- The web address is actually a graphic, overlaid onto the screen to make you think it's the correct address
- A graphic simulates the padlock symbol



### **>DOS & DON' TS :**

- **Do** make sure you download the latest security updates.
- **Do** look out for words or language used which would not actually be used by the sender.
- **Don't** open it – if you think you have received a virus, don't open it or even view it using your email preview pane.
- **Do** report any viruses to your IT department and/or delete them immediately.
- **Don't** open or forward a spam email, delete it immediately.
- **Don't** reply to spam, or any email you are unsure about, even if it's to 'unsubscribe' – this will only validate your email address to the sender.
- **Do** ignore delivery failure receipts for messages you didn't send.
- **Do** consider having a secondary email address – this can be used when filling out registration forms, surveys, subscribing to newsletters...etc.
- **Don't** open an unsolicited message unless it is from someone you know and trust. This rule applies to avoiding security breaches in general – don't forget that spam can contain viruses and other malicious software.
- **Don't** post your email address on your website or in newsgroups – many spammers trawl the Internet for as many addresses as they can find.
- **Don't** give your email address to anyone or any website you don't trust.
- **Don't** click on any of the links in a suspicious email.
- **Do** delete any potential phishing email immediately.
- **Do** contact your bank or financial institution if you can't be certain whether an email seemingly from them is genuine.



>GHOST  
>KEYLOGGER

## >WEB THREATS AND HOW TO PROTECT AGAINST THEM

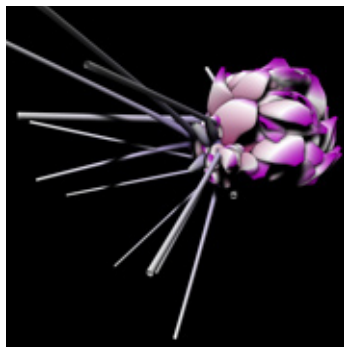
### >SPYWARE

Spyware is a catch-all term for unwanted software that either secretly monitors your online activity to aid advertising and marketing, or in its more sinister form steals private information from your PC. This can include searching for your banking details, logging your key strokes, or even allowing outsiders to control your computer. Spyware can get onto your computer in a number of ways; downloading seemingly legitimate software or freeware on the web, clicking 'agree' to the small print of a download form, signing up for a new 'tool bar', 'smiles' or similar offer, or even just visiting a particularly unscrupulous site, can all lead to you falling victim.

Spyware is a major risk because it isn't easy to detect and can do untold damage before being discovered. Some telltale signs that you have spyware on your computer include: regular pop ups appearing, your computer running slowly, or automatically being directed to a site you didn't want to visit every time you go online. Your IT department will be able to tell immediately if you have spyware on your computer. If you are in any doubt, contact them at once.

### >DOS & DON' TS :

- **Do** comply with your company's acceptable usage policy.
- **Do** make sure your browser is up-to-date with the latest security patches.
- **Do** only visit websites you know and trust.
- **Don't** follow links to sites from email or instant messages that you are not sure of.
- **Do** check the destination of links. If you hover your cursor over a link it will highlight the destination in the bottom left of your browser window.
- **Do** be careful if you use social networking sites like Facebook, LinkedIn or MySpace. Be very wary of friend requests from people you don't know. Many unsolicited friend requests are bogus and will try to lure you into downloading spyware.
- **Do** contact your IT department immediately if you think you have spyware on your computer.



>ROGUEWARE SPYSHERIFF  
>FAKE ANTI-SPYWARE PROGRAM

## >IM THREATS AND HOW TO PROTECT AGAINST THEM

### >INSTANT MESSAGING

As instant messaging (IM) becomes more popular, the risks of using it have increased dramatically. IM systems can receive attachments either containing, or linking to, malware or spyware in just the same way as email. In fact IM can be even more dangerous because it is even more immediate.

#### >DOS & DON'TS:

- **Don't** follow links sent to you by IM. If you must follow a link, cut and paste it into your Internet browser.
- **Do** be wary of IM from friends or colleagues that direct you to a website. Their computer may be infected with a virus that sends out these messages.

For more information on any of the web and messaging security threats detailed in this guide, and for a copy of your company's email and web acceptable usage policy, please contact your IT department.

**>WWW.MESSAGELABS.CO.UK**  
**>INFO@MESSAGELABS.COM**  
**>FREEPHONE UK 0800 917 7733**

**>EUROPE**

**>HEADQUARTERS**

1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom  
Tel +44 (0) 1452 627 627  
Fax +44 (0) 1452 627 628  
Freephone 0800 917 7733  
Support: +44 (0) 1452 627 766

**>LONDON**

3rd Floor  
40 Whitfield Street  
London, W1T 2RH  
United Kingdom  
Tel +44 (0) 20 7291 1960  
Fax +44 (0) 20 7291 1937  
Support +44 (0) 1452 627 766

**>NETHERLANDS**

De Geelvinck, Office 5.06  
Singel 540  
1017 AZ  
Amsterdam  
Netherlands  
Tel +31 (0) 20 5 222 393  
Fax +44 870 238 4401  
Support +44 (0) 1452 627 766

**>BELGIUM/LUXEMBOURG**

Cullinganlaan 1B  
B-1831 Diegem  
Belgium  
Tel +32 (0) 2 403 12 61  
Fax +32 (0) 2 403 12 12  
Support +44 (0) 1452 627 766

**>DACH**

Feringastrasse 9a  
85774 Unterföhring  
Munich  
Germany  
Tel +49 (0) 89 189 43 990  
Fax +49 (0) 89 189 43 999  
Support +44 (0) 1452 627 766

**>AMERICAS**

**>AMERICAS**

**HEADQUARTERS**  
512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA  
Tel +1 646 519 8100  
Fax +1 646 452 6570  
Toll-free +1 866 460 0000  
Support +1 866 807 6047

**>CENTRAL REGION**

7760 France Avenue South  
Suite 1100  
Bloomington, MN 55435  
USA  
Tel +1 952 886 7541  
Fax +1 952 886 7498  
Toll-free +1 877 324 4913  
Support +1 866 807 6047

**>CANADA**

First Canadian Place  
100 Kings Street West, 37th floor  
Toronto, ON M5X 1C9  
Tel +1 646 519 8100  
Fax +1 646 452 6570  
Toll-free +1 866 460 0000  
Support +1 866 807 6047

**>ASIA PACIFIC**

**>HONG KONG**

Unir 1601, 16F  
Lippo Centre, Tower 2  
Tower II  
89 Queensway  
Admiralty  
Hong Kong  
Tel +852 2111 3650  
Fax +852 2111 9061  
Support: +852 2111 3658

**>AUSTRALIA**

Level 6  
107 Mount Street,  
North Sydney  
NSW 2060  
Australia  
Tel +61 2 8208 7100  
Fax +61 2 9954 9500  
Support +1 800 088 099

**>SINGAPORE**

Level 14  
Prudential Tower  
30 Cecil Street  
Singapore 049712  
Tel +65 6232 2855  
Fax +65 6232 2300  
Support +852 2111 3658

**>JAPAN**

Bureau Toranomom 3rd Floor  
2-7-16 Toranomom Minato-ku  
Tokyo 105-0001  
Japan  
Tel +81 3 3539 1681  
Fax +81 3 3539 1682  
Support +852 2111 3658

