

# Security

## Easy tips for the end user

### Introduction

Basic security is easy and cost effective. It is often said – and truly is – that common sense is the best protection against all on-line nasties.

Always take security seriously. Even a small lapse could cost you or your company much time, effort, cost and lost business if something goes wrong.

### Passwords

- Never give them out!
- Change them regularly.
- Don't use your pet's name!
- Don't make them too short and easy to guess – at least 6 characters.
- Choose a “strong” password, eg.:

987654321 - weak

ceE3Pi0 - strong

...better still, use the password generator on <http://www.ludcastle.co.uk/techsupport.htm>.

### Instant Messaging (IM)

We suggest you don't use this technology, except for new mail arrival notification with [www.BetterAndCheaper.co.uk](http://www.BetterAndCheaper.co.uk) with Google Apps. Use your email system for messaging.

### Email

**Attachments:** Properly secured email systems will help protect you. However, from time to time unwelcome things will get through. In general if you don't recognise the sender do not open an attachment, especially one ending in:

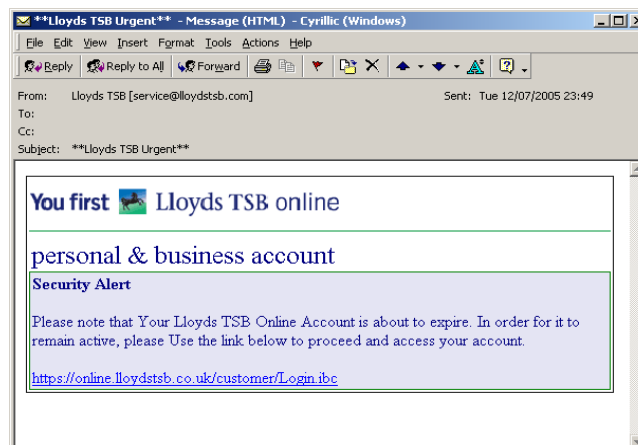
.zip

.com

.exe

**Phishing** (pronounced “fishing”) is literally fishing for your or your company's sensitive data.

Here's an example:



No reputable organisation would ask you to do this. Note also that the text content has poor grammar and makes the wrong use of capitals, "... please Use the...".

Use your common sense, and if in doubt log on to your usual provider's web page (your bank, or other institution) in your usual manner, and send them a message querying the email before clicking the link.

Don't become a victim!

### Golden Rules for Protection Against Viruses

(From Avira Anti-Virus / Malware, [www.avira.com](http://www.avira.com))

- Always keep boot floppy-disks for your network server and for your workstations.
- Always remove floppy disks, CDs, DVDs etc., from the drive after finishing the work. Even if they have no executable programs, disks can contain program code in the boot sector and these can serve to carry boot sector viruses.
- Regularly back up your files.
- Limit program exchange: particularly with other networks, mailboxes, internet and acquaintances.
- Scan new programs before installation and the disk after this. If the program is archived, you can detect a virus only after unpacking and during installation.
- And – last but not least – have an up-to-date virus/malware scanner installed throughout your system

If there are other users connected to your computer, you should set the following rules for protection against viruses:

- Use a test computer for controlling downloads of new software, demo versions or virus suspicious media (floppies, CD-R, CD-RW, removable drives).
- Disconnect the test computer from the network!
- Appoint a person responsible for virus infection operations and define all steps for virus elimination.
- Organize an emergency plan as a precaution for avoiding damage due to destruction, theft, failure or loss/change due to incompatibility. You can replace programs and storage devices but not your vital business data.
- Set up a plan for data protection and recovery.
- Your network must be correctly configured and the access rights must be wisely assigned. This is good protection against viruses.

T: +44 (0) 1828 627 884  
F: +44 (0) 870 051 82 32  
<recipient>@ludcastle.co.uk  
[www.ludcastle.co.uk](http://www.ludcastle.co.uk)

