# Phishing (pronounced fishing)

**The key to your email or any online account, is your password**
**The easiest way to get something is to ask for it!**
**This is what a phishing email does, often successfully.**

## Choose a memorable password

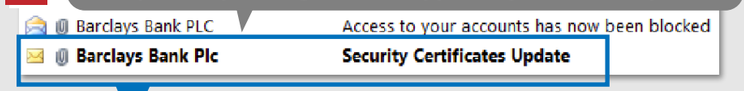
When deciding on a password, think of a sentence and take the first letter of each word e.g. M12dlpulnas!
**My 12 digit long password uses letters, numbers and symbols!**

## Email scams

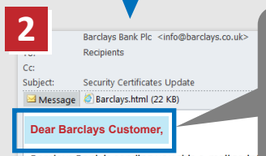
Remember: you will **NEVER** get an email from your bank or email provider asking you for your password or other important information. If you do receive an email like that it is a 'phishing' attempt to steal your password.

**They are often very difficult to spot!**

**1** Examples of 'phishing' emails supposedly from Barclays Bank

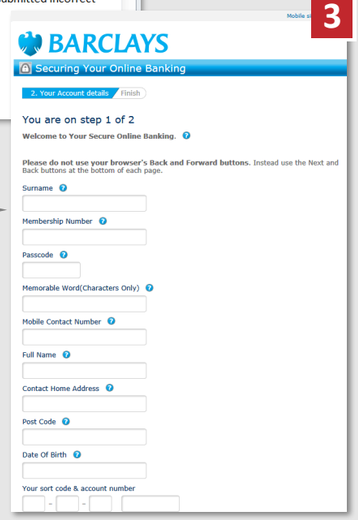



**2**




Be very wary of emails that are not addressed to you by name. This example is addressed to 'Barclays Customer'. It includes an attachment and the message asks you to open it

**3**




The attachment opens a web page which looks just like the Barclays website - **but it isn't!**

Information entered on this fake web page will be used by the hacker to **defraud money from your account!**

## Delete phishing emails

**Don't be caught out!**

If you receive a 'phishing' or scam email that asks for your password, account or credit card details, **DON'T** respond and **delete it immediately.**
**Do not open** any attachments you are unsure about.

# Malware

**Malware or malicious software is designed to damage or compromise a computer. There are different types called:**

worms | viruses | spyware | trojans

## Security software

**Protect your computer!**

Have up-to-date security software on your computer or Mac – a good, free one for Windows is 'Windows Defender' or you can buy software from the following:

Norton by Symantec | McAfee An Intel Company | TREND MICRO | KASPERSKY lab

## Downloading software

Always read carefully what you are downloading as it can contain malware!
Only click on Download links on reputable websites.

## Don't worry, 'cookies' are fine

Web pages are not passive, they often need to interact with your computer to work well. Advertising pays for what we see on web pages and through using small files called cookies we can receive more relevant adverts.

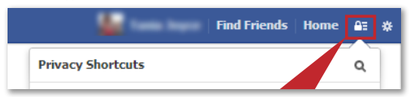
# Online bullying and trolling

**Bullies use the internet to send anonymous, nasty messages on social networking sites or via email. Ignore them and take action. If you are a child and are concerned about bullying, speak to an adult.**

## Privacy settings

**Tip for Facebook!**

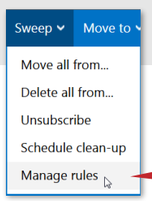
Do learn how to change your privacy settings on Facebook to stop unwanted messages. Click the 'Privacy Shortcuts' icon and use this menu to filter who can send you messages or post on your timeline.




## Block an email address

**Tip for email!**

You can avoid nasty emails by setting a rule which will block an email address or put the email in your Junk folder.




Go to **Manage rules** in Outlook

# Ticket & online shopping fraud

**Always buy from known ticketing companies to get legitimate tickets!**

Good shopping sites will be secure

## What to look for

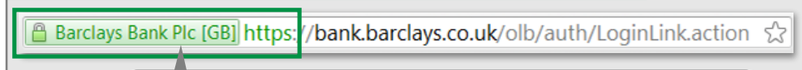
**https: or http: that is the question!**

Check for the 's' after 'http' in the address bar when you enter personal information or credit card details

**This address bar shows this shopping basket web page is secure**

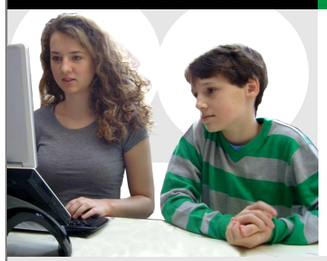

The padlock in the Address bar shows that your credit card details are encrypted and cannot be read by anyone else.

**Online banking websites have another layer of protection**




The green colour shows the site uses Extended Validation (EV) Secure Sockets Layer (SSL) Certificates

# Harmful content



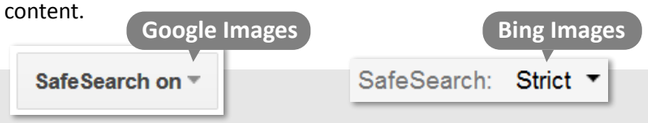
**Sadly there are a lot of videos and images on the internet that are harmful.**

**Children and adolescents are particularly vulnerable.**

**A third of internet content is pornograpy.**

## SafeSearch

Bing and Google have 'SafeSearch' options where you can opt to filter out harmful content.




## Filtering

You can opt to **stop** harmful content coming into your home with a good broadband supplier e.g. TalkTalk's HomeSafe. This free service filters content to **all** devices that connect to your TalkTalk broadband, including tablets, mobile phones and games consoles.

TalkTalk HomeSafe