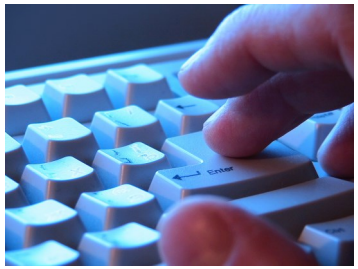
## Always remember:

- Legitimate businesses such as your bank should not ask you to send passwords, login names or other personal information through e-mail
- Phishing links may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate web site
- Web addresses that resemble the name of a well-known company may be slightly altered by adding, omitting, or transposing letters. For example, the address "www.microsoft.com" could appear instead as "www.micosoft.com"



## Useful information and contacts

Childnet International - http://www.childnet.com/ [ctrl + click]
Wide range of resources, in particular 'Know IT All for Parents and Carers'.

CEOP - http://www.thinkuknow.co.uk/ [ctrl + click]
Child Exploitation and Online Protection Centre site with education resources from KS1 and Foundation.

Get Safe Online - http://www.getsafeonline.org/ [ctrl + click]
source of unbiased, factual and easy-to-understand information on online safety

Kidsmart - http://www.kidsmart.org.uk/ [ctrl + click]
Resources and information about e-safety

Sure Start
Children's Centres
Shepway

# Protect Your Family On-line

Kent County Council
kent.gov.uk

## Social networking

Social networking sites can be fun, interactive and a quick way to stay in touch with friends and family online.

### Be careful what you put online

**Review your privacy settings regularly** - make sure only the people you want to know about you can read your profile and updates. Also, review where you're tagged in photos.

**Be careful who you 'friend' online** - some people may not be who they say they are, while others may say nasty or inappropriate things. Think twice before you allow someone to 'follow' you.

**Don't give out personal details** - for example, your date of birth or what school/college you go to. It's a good idea to put as little personal information as possible on social networking sites to avoid people knowing too much about you.

**Think twice about the information you post online** - for example, posting that you're off on holiday (and therefore your house may be empty) or that you have a brand new car. Other people could use this against you and you risk having your property stolen.

Carefully consider what **photos** you share online and what impression this gives (i.e. potential employers).

## Hoax and Chain Messages

### What is a Hoax or Chain Messages?

A hoax or chain message is any message (received via email, text or website etc) that, either through overt instruction or through compelling content, encourages the reader to pass it on to other people. Chain messages can range from promises of money (such as lottery wins or pyramid schemes), hoax stories promising luck, answering questionnaires, threats to personal safety, to hoax virus alerts.

Chain messages are started and sent for many reasons. The most common reasons are for generating money, harvesting personal data (email addresses), virus attacks, clogging up computer networks or programmes or for collecting email addresses to use to send people junk and unwanted (spam) messages.

## Online dating

### Risks

Some of the risks we worry about are:

- Personal safety when meeting someone you met online
- Stalking and harassment
- Meeting people who shouldn't be dating online
- Dating sites being used as vehicles for spam [ctrl + click], selling or fraud

In a few cases, criminals find their victims online and attack them when they meet. These are serious risks, but you can protect yourself by following a few guidelines, trusting your instincts and using common sense.

### Choose your forum carefully

While you can strike up a friendship in many places online, and this guidance applies to all of them, choosing a well-run, reputable online dating service will provide some additional safety. For example, you should look for a site that will protect your anonymity until you choose to reveal personal information. Also look for a site that will enforce its policies against inappropriate use.

### Protect your privacy

You are in control of what happens. Don't let anyone pressure you into giving away more information than you want to.

- You wouldn't give your phone number to every stranger on the street. Similarly, don't post personal information, such as phone numbers, in public places on the internet
- Wait until you feel comfortable with an individual before telling them things like your phone number, place of work or address
- A well-run dating site will offer the ability to email prospective dates [ctrl + click] using an email service that conceals both parties' true email addresses
- As a second line of defense for your privacy, set up a separate email account thatt doesn't use your real name. Similarly, you can use an internet telephone service, such as Skype [ctrl + click] , to call someone instead of using your own phone
- Pick a user name that doesn't include any personal information. For example, "joe_glasgow" or "jane_liverpool" would be bad choices

## Shopping safely online

There are a few steps you can take to shop online safely and keep your financial details secure.

### Before you buy

Before you buy online, note down the address, telephone and/or fax of the company you're buying from. Never rely on just an email address.

### Always use secure site

Sites with 'https' in front of the web address mean the site is using a secure link to your computer. A yellow padlock symbol will appear in the browser window to show the payment process is secure.

When buying online:

1. Never transfer or receive money for someone else
2. Check the site's privacy and returns policy
3. Print out a copy of your order and any acknowledgement you receive
4. Check your bank statement carefully against anything you buy online
5. Keep your passwords secure
6. Take your time making decisions that involve parting with money
7. Get independent financial advice before making investments
8. Only do business with companies you recognize or have been recommended by someone you trust - don't judge a company on how professional their website looks
9. If in doubt, check a company is genuine by looking them up on Companies House or the Financial Services Authority (FSA) websites

### What does a chain or hoax message look like?

Common signs to spot a message could be a hoax or chain message is:

- The email states "this is a completely true story," or "it's perfectly legal." If the author feels he or she has to make it clear, then it's probably not
- It relays an account of events that supposedly happened to an unidentified third person (i.e. "the dear son of the neighbour of someone my friend knows")
- It warns that if you don't forward the message within a certain time frame that something unpleasant will happen such as bad luck, a problem with your computer or even death. People are often motivated by extremes and we respond faster when we believe the consequences of our inaction could be swift and severe
- Most importantly a hoax or chain message **asks, begs or bullies you to forward it on to everyone you know**

### What can I do if I or someone I know receives a chain message?

The simple and most effective solution is to delete the email or text. But all too often people don't do that. These steps can help to keep you safe:

- Don't send anyone any money, whoever contacts you via email.
- Don't forward the e-mail to friends and family.
- If you are still unsure what to do you can call or report the scam to Action Fraud: www.actionfraud.police.uk [ctrl + click] or 0300 123 2040

## Online Phishing

Phishing is a type of deception designed to steal your personal data to commit identity theft. Criminals send emails to thousands of people which pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually contain a very compelling and urgent but bogus reason to go to the site, for example to update your password before your account is suspended.

Victims click on an embedded link in the email itself which takes them to a website that looks exactly like the real thing but is, in fact, a fake, designed to trick victims into entering personal information such as a password or credit card number. .

## How can I tell if it's a phishing email?

Criminals can make an email look as if it comes from someone else. Fake emails often (but not always) display some of the following characteristics:

- The sender's email address doesn't tally with the trusted organisation's website address
- The email is sent from a completely different address or a free web mail address
- The email does not use your proper name, but uses a non-specific greeting like "dear customer"
- A sense of urgency; for example the threat that unless you act immediately your account may be closed
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character difference means a different website
- A request for personal information such as user name, password or bank details
- You weren't expecting to get an email from the company that appears to have sent it

## Protect yourself

- Use Anti-virus/Spyware programmes – phishing filters can often be built into web browsers or can be added on
- Delete and report any emails you are suspicious of
- Report the e-mail to the faked or "spoofed" organisation. Go directly to their website via your browser and not via the link provided in the suspicious email
- You can report suspicious or phishing emails online to the Anti-phishing Working Group at www.antiphishing.org/report-phishing/ [ctrl + click]
- and Bank Safe Online at www.financialfraudaction.org.uk/Consumer-fraud-prevention-advice-remote-banking.asp [ctrl + click]
- , so that the information can be quickly shared between all the banks
- Never click a link in a suspicious email, always make sure you go to the site via your address bar in your browser to ensure you are visiting the

## Keeping your children safe

The best way to help your child to be safe when using the internet is to ensure they understand these rules:

NICKNAME - never give out personal details to online "friends" (an online "friend" is anyone you have not met in real life). Use a nickname when logging on and do not share full name, email address, mobile number, school name and any photos etc

WHERE - encourage your child to use the computer/laptop/other devices on line in a family area in the house, rather than their bedroom so you can see what they are accessing

CONTROLS - use parental controls and filtering products on any internet enabled devices (mobile phones, games consoles, tablets etc) but be aware that they can be bypassed

TALK - be aware that mobile devices cannot always be supervised and parental controls may fail so it is important to talk to your child about online risks and how to manage them

UPSET - If your child receives a message that upsets them, remind them not to reply, they should save the message and show you or another trusted adult

LIES - help your child to understand that some people lie online. They should never meet with an online "friend" without an adult they trust

BLOCK - make sure they know how to block someone online and report them if they feel uncomfortable

SOCIAL NETWORKING - it is often against the site regulations for a child under 13 years to set up social networking profiles

BLAME - make sure your child feels able to talk to you, let them know it is never too late to tell someone if something makes them feel uncomfortable. Don't blame your child, let them know you trust them