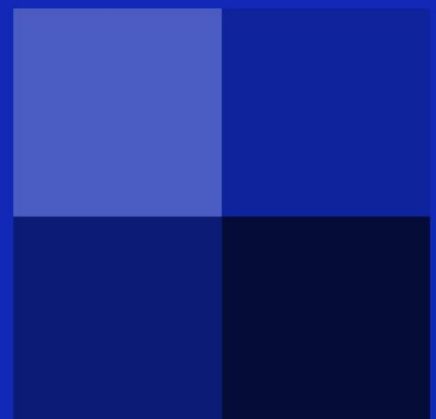




A parent/carer's guide to hoaxes

# E-Sussex, E-Safe

**Safeguarding all children in East Sussex all the time**



Provided by **East Sussex County Council**

We all know that if something seems too good to be true, it usually is, but what if the object presented looks not only reasonable, but has your account number on it as well?

Hoaxes come in a staggering array of shapes and forms online, and range from cold-calling (usually from an overseas call centre) telling you that you either owe money, or are owed money, to texts, emails, even parcel delivery notices left through your door inviting you to phone a number (at VAST expense) to collect an item.

They have also become far more sophisticated.

Here, we will examine some of the more recent hoaxes, and this should enable parents and carers to develop a sixth sense for when something isn't quite right.

### **The Fake “Out” card.**

Over Christmas, people started to find cards from a delivery firm on their doormats. The card stated that a delivery had been attempted but that no-one was home. It then went on to ask the recipient to call a phone number to arrange delivery. The phone number concerned was a premium rate line which incurred a charge of £300.00 just for the connection, and then £150.00 per minute thereafter. All of this was charged to the caller's phone line.

### **The Fix.**

If you get such a card, even if it says it is from a reputable delivery company, always cross-check the number on the card with the number in the Phone Book. If there is a discrepancy, just bin the card. Delivery companies will usually attempt three deliveries before returning the goods to the sender. Reputable companies have re-delivery contacts in the phonebook.

### **The Fake “Call From The Bank”**

This is ever-popular with scammers. You get a phone call from the bank. They tell you that, for security purposes, you should put the phone down and call the number on your credit card. Seems above board, but what you may not know is that the scammer has kept your line open. (You will even hear a dial tone). You think you are calling your bank, but in fact you are speaking to the same person who phoned you. Then comes the inevitable request for account details.

### **The Fix**

If you have ANY reason to think the call is bogus, ask them to put it in writing. Banks will always do this. If you are not sure, and think maybe you should call the number on your credit card, do so from a mobile phone, or put your phone down and wait at least 10 minutes. Preferably, call someone else first to make sure your line has not been kept open.

## The “Utility Company” call.

“Good evening. This is British Gas. For security purposes, can you confirm the first line of your address and your post code?” Many calls start like this these days. However, you have no reason to prove your identity. They phoned you, after all. Sometimes fraudsters may have already gained your credit or bank details and all they need now is the associated address.

### The Fix.

You have a couple of options here. First, you can ask them to tell you something like the numbers in your postcode, or the first, fifth and eighth numbers from the bank account used to pay the bills. If they say they can't do this, (or won't) again, ask them to put it in writing. Remember, you have nothing to prove – they phoned you.

Online, things can get rather trickier. Gone are the days when a poorly worded, and usually badly spelled email would arrive allegedly from “Barclies Bank” saying “There is problem with account. Click here or money kept.” Now, there are perfectly believable emails arriving from everyone from Banks to utility companies telling you any of the following:-

- We have updated our systems. You must confirm your details to continue using our service.
- We have had a problem with our IT systems which has now been resolved. Please confirm your payment method.
- We have reason to believe your account has been compromised. Click here to change your password.


The email may even look exactly like other genuine emails you have received from your bank or building society. If you click on the links (**which you really shouldn't**) the website you end up at may look exactly like the real thing.

### The Fix

No Bank or Building Society will **ever** ask you to do this via an email or phone call. They will always write to you. If you think perhaps, that the email may be genuine, please call into the bank or building society in person to make any such changes, or visit an ATM. (Making sure that it hasn't been tampered with. Using ATMs located inside banks is usually the safest way.)

## The Social Media Hoax(es)

There are more and more of these, almost by the day! They range from, for example, Facebook advertisements telling users they have to confirm their details by following this link, to warnings that Facebook are going to do this or that to your account.

By far the highest risk is the “punch out”. This is usually the Facebook “F” symbol,  that is a hyperlink to, allegedly, Facebook. **However, sometimes it takes you to places that only LOOK like facebook.**

**Always check the web address if you use one of these. It should start with <https://Facebook.com/>**

Remember, fake websites can be almost indistinguishable from the real thing by appearance these days.

Fraudsters think nothing of targeting children. There are several reasons for this. They know that children have access to money – YOURS. They also know that some children have money and bank accounts of their own.

So, they may see advertisements, usually in the form of pop-ups, (but they can arrive as emails too) saying:-

- Congratulations – You’ve won a (laptop, ipod, ipad – etc. etc)
- You’ve been specially selected to receive a cash prize
- You’ve won tickets to Euro Disney for your whole family.

You can pretty much put anything you like into these scam communications.

If your child clicks on the inevitable link, they will have to enter a lot of personal information such as name, address, phone number, email, etc before, again inevitably, arriving at a payment page where, their “free” prize will need a credit card to cover postage and packing.

Needless to say, a great deal of money will be taken from the account, and the fabulous prize will never arrive.

### **The Fix**

The fix here used to be simply to turn on your pop-up blocker. All web browsers have them, but the scammers are getting cleverer. The only way to be really sure is to teach children that no-one is EVER going to give them an iPad for free. It’s a hard lesson, and they don’t want to learn it, but its true nonetheless.

Sometimes one sees advertisements for (usually) Apple products – ipods, Macbooks, Ipads etc that are ridiculously cheap because “the packet has been opened and they can’t be sold.” And so, the advert would have us believe, you can pick up a top specification MacBook Air for £200.00.

Apple did not become a multi-billion dollar company by giving products away at less than cost merely because the box has been opened.

There is a real risk that goods advertised like this may be stolen, or defective, or have been tampered with. It is not likely that you will see a guarantee!

## **The Bottom Line**

The internet is vast, and for the most part unpoliced. Technology has become cheaper and easier to manipulate, and these days, you do not need a degree in website design to build a functioning website. Web parts are freely available online, and a convincing fake site is relatively easy to build.

It is impossible to list, scam by scam, every unpleasant hoax in existence – they change too rapidly for that, but broadly, they fall under the following headings:-

- Scams that want your money – or scams that want to make YOU responsible for someone else's debts.
- Scams that want your identity – or part of it. (Date of birth, place of birth, bank details, etc)
- Scams that are targeted at young people – possibly for the above reasons, but also possibly for more sinister purposes.

We need to have our wits about us at all times online – not easy in the busy world of multiple communications that we now inhabit.

Unlike the thief in the street, cybercrime is around us 24/7/365 – it reaches into our homes, and sits in our pockets. Like cyberbullying, we are never away from it.

In other areas of life, we are often encouraged to take risks – indeed risk taking is seen as a good thing. In education teachers and students are encouraged to take risks – trying out new learning methods – students encouraged to go on outward-bound activities, go on residential trips – try hang gliding! In Banking, traders take risks all the time.

Even our employers encourage us to “think out of the box” and take risks to develop new products and ideas. We are no longer as risk-averse as we were in the past.

This behaviour can also affect us at home too.

Are we losing our sense that something isn't quite right? Are we becoming desensitised to danger?

Some golden rules are needed.

## **Golden Rules.**

- You don't owe anyone an "instant response". If it's important, they will write to you.
- If it seems too good to be true, treat it as if it is. You may only get one chance
- Teach your children never to give any information to cold callers.
- Check requests to phone companies with their entries in the phone book
- If in doubt – do nothing. If it's important, they will get back in touch.
- You don't have to prove who you are to anyone who phones you – ask THEM for proof of who they are. If they can't or won't give it, ask them to write.
- Always check web addresses. Make sure you are where you think you are.

There are other ways in which you can reduce the hassle of scammers.

- Join the Telephone Preference Service – its free and will stop a large number of cold-callers, but not all.
- Consider getting a "Call minder" there are several on the market. These devices can be programmed to only allow incoming calls from people you know, or block all overseas incoming calls.
- Make sure your spam filter is operational and instead of deleting scam emails, mark them as spam – that way you won't get anymore from that particular account, although scammers regularly change their email accounts so it won't stop it completely.
- Get in touch with your Bank/Building society and set up a code word that they will use when/if they phone you. Don't give it out in full over the phone, but you can ask them to tell you the 1<sup>st</sup>, 4<sup>th</sup> and 7<sup>th</sup> letters. Then they can prove they are genuine without compromising any account details. This works for Utility companies too. If they won't then change to a company that will.
- **Make a fuss!** Talk about scams that you know about – spread the word as widely as you possibly can. The more awareness we can generate, the harder it makes the job of the scammer.
- **Report, Report, Report.** Tell your Bank, school, Police, Trading Standards, of scams that you have seen. Let's make sure that the life of a scammer is full of anticipation of that next knock on the door.

**Finally – If you think you have been the subject of a scam – don't delay, report it right away.**

There is no need to feel embarrassed if you have fallen for a scam – they are sophisticated these days, so if you think this has happened, please make sure that you don't delay in reporting it to whomsoever needs to know. Your bank has a duty of care towards you and can help to recover money stolen from your account, and can monitor your account for unusual transactions for a period of time.

If you think you or your family might be in personal danger, contact the Police.