

How to keep you data secure in using the Internet

Surrey Arts is offering advice on how to protect yourself when using the Internet and your email accounts. Even just having an email account can make you susceptible to scams.

It is advisable to install virus software on your computer and keep it updated. It is also advisable to download a spam filter to get rid of unwanted emails.

Of course there are many unwanted emails and scams that still manage to get through your antivirus and email filters. The main advice is, if you receive an email that you are not sure about, no matter the content we advise please forward it to Trading Standards (<http://www.tradingstandards.gov.uk/advice/consumer-advice.cfm>) or Caroline Jackman at caroline.jackman@surreycc.gov.uk and she will advise as to whether it is an email scam or not. (*advise on avoiding scams is outlined below*)

How do people access your details?

Using the same passwords for online usage e.g.: your website/s, email accounts, social media accounts can make you susceptible to have your details accessed. We advise you use different passwords (*advise on passwords is outlined below*)

We also recommend that you have more than one email, using one for general correspondence and one for your online accounts

Paying online: most companies offer online payment, and use a reputable secure online payment system like WorldPay or PayPal. Again the key is to have a good password and to keep your passwords and pin numbers safe.

Passwords

Your passwords are the keys to your online data.

Don't make it easy for hackers to guess your password. Use strong passwords and keep the data safe.

We recommend that passwords must:

- contain a minimum of 7 characters
- include at least one numeric or non-alphabetic character
- not contain more than 2 consecutively repeated characters
- not be easily guessed because of a clear relationship with the user (e.g. not related directly to spouse or children's names, or the type of car owned)

Note that some of systems are case-sensitive, but some aren't. If your password contain both upper and lower case characters, ensure that you use the same combination in the same way each time, or you may find some systems are blocked.

Risks

The best security in the world is useless if a malicious person has a legitimate user name and password. They can do everything you can do.

If you use the same password for every system, a hacker only has to break it once to have access to everything

Do use strong passwords

A good password:

- Needn't be a word at all. It can be a combination of letters, numbers and keyboard symbols.
- Contains a mix of upper and lower case letters, numbers and keyboard symbols (i.e. ~ ! @ \$ % ^ & * () _ + - = { } | [] \ ; < > ? /).
- However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards if you are travelling. You should probably avoid using the pound symbol (£), full stop (.), comma (,) and quote marks (" ").
- Is changed regularly.

Don't use weak passwords

Avoid weak passwords. This means:

- Using no password at all.
- Using a commonplace dictionary word.
- The most common password is 'Password' so that's an obvious one to avoid.
- A password you haven't changed in more than a couple of months.

Look after your passwords

- Never disclose your passwords to anyone else.
- Don't enter your password when others can see what you are typing.
- Use different passwords for different services
- Change passwords regularly.
- Don't recycle passwords (e.g. password2, password3).
- Don't send your password by e-mail. No reputable firm will ask you to do this.
- If you think that someone else knows your password, change it immediately.
- Use key shifting. If you think of your memorable phrase and then use the key to the key north east of the characters on the keyboard. e.g. "cat" becomes "fw6". Of course you could use whichever direction you want.

Password Hints: a useful tool to remember your passwords

Note: they need to be cryptic and not "the usual" or "same as the bank".

Example:

email sallyb.8@btinternet.com who gives the password as "F1sh&Ch1ps" and hint as "fridays"

Example in how to prepare a Strong Password:

1. **Think of a sentence that you can remember.** This will be the basis of your strong password.

Use a memorable sentence, such as "My son Aiden is three years old."

2. **Convert the sentence to a password.** Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".

3. **Add complexity** by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance substituting the number 3 for the word "three", or "1" for the letter "i". This might yield a password like "MsA13yo". Not all of our systems are case-sensitive, but it is a good idea to use upper and lower case characters to make the password harder to break. Ensure you use any mix of upper/lower case characters consistently.

4. **Hint for this password:** 'How many years is my little boy?' Note there are no links to the password.

How to protect yourself against scams

Almost everyone will be approached by a scammer at some stage. Some scams are very easy to spot while other scams may appear to be genuine concerns, offers or bargains. Scams can even take place without you doing anything at all.

Most scams need you to do something before they can work. Scams only work if you enter into correspondence with the scammer. They may request you to send money to someone based on a promise that turns out to be false. You may give your personal details to people who turn out to be scammers. Some scams rely on you agreeing to deals without getting advice first or buying a product without checking it out properly.

The simple tips below will help you protect yourself and your family from scams. Scams can cost people a lot of money and cause a great deal of distress. By following these simple tips, you can protect yourself against scams.

Golden rules

If it looks too good to be true—it probably is.

- **ALWAYS** get independent advice if an offer involves significant money, time or commitment.
- Remember there are no get-rich-quick schemes: the only people who make money are the scammers.
- Do not agree to offers or deals straight away: tell the person that you are not interested or that you want to get some independent advice before making a decision.
- **NEVER** send money or give credit card or online account details to anyone you do not know and trust.
- Check your bank account and credit card statements when you get them. If you see a transaction you cannot explain, report it to your credit union or bank.
- Keep your credit and ATM cards safe. Do not share your personal identity number with anyone. Do not keep any written copy of your PIN with the card.

Digging a little deeper

- Be careful if an email seems genuine as it has come from someone you know, but it has not personalised you into the email, e.g. Dear Jane.
- Do not let anyone pressure you into making decisions about money or investments: always get independent financial advice.
- Read all the terms and conditions of any offer very carefully: claims of free or very cheap offers often have hidden costs.
- Make sure you know how to stop any subscription service you want to sign up to.
- Be very careful about offers for medicines, supplements or other treatments: always seek the advice of your health care professional.
- Remember there are no magic pills or safe options for rapid weight loss.
- Beware of products or schemes that claim to guarantee income or winnings.
- Be wary of investments promising a high return with little or no risk.
- Beware of job offers that require you to pay an upfront fee.

Protect your identity

- Only give out your personal details and information where it is absolutely necessary and where you have initiated the contact and trust the other party.
- Destroy personal information, don't just throw it out. You should cut up, burn or shred old bills, statements or cards so scammers can not get your personal details from them later.
- Treat your personal details as you would treat money: don't leave them lying around for others to take.

Sending or transferring money

- Never send money to anyone you are not totally sure about.
- Do not send any money or pay any fee to claim a prize or lottery winnings.
- Money laundering is a criminal offence: do not agree to transfer money for someone else.
- Make sure that cheques have been cleared by your bank before transferring or wiring any refunds or overpayments back to the sender.
- Do not pass on chain letters or take part in pyramid schemes: you will lose your money and could lose your friends.

Dealing with suspicious or unsolicited offers sent by email or SMS

- Do not open suspicious or unsolicited emails (spam): delete them.
- Do not click on any links in a spam email or open any files attached to them.
- Never call a telephone number that you see in a spam email or SMS.
- **NEVER** reply to a spam email or SMS (even to unsubscribe).

Internet tips

- If you do use a public computer whether in a hotel, internet café or library, always remember to LOG OFF from your email account.
- Talk to your Internet service provider about spam filtering or, alternatively, purchase spam-filtering software.
- If you want to access an Internet account website, use a bookmarked link or type the address in yourself: **NEVER** follow a link in an email.
- Install software that protects your computer from viruses and unwanted programs and make sure it is kept up-to-date.
- Beware of free websites and downloads (such as music, adult sites, games and movies). They may install harmful programs without you knowing.
- Check the website address carefully. Scammers often set up fake websites with very similar addresses.
- Never enter your personal, credit card or online account information on a website that you are not certain is genuine.
- Never send your personal, credit card or online account details by email.
- Try to avoid using public computers (at libraries or internet cafes) to do your internet banking.
- Do not use software on your computer that auto-completes online forms. This can give internet scammers easy access to your personal and credit card details.
- Choose passwords that would be difficult for anyone else to guess.

If you have any queries about this document please contact Caroline Jackman on 01483 519281 or email caroline.Jackman@surreycc.gov.uk.