Cyber Aware Activity Sheet

These fun, quick, five minute activities have been created by The National Cyber Security Centre to help families think about how they can be Cyber Aware.

Choose the activity most suitable for your child's age and development.

National Cyber Security Centre

NCA National Crime Agency

CEOP A National Crime Agency command

Activity 1

1. Ask your child to collect up a few things that are important to them and put them all in a box or bag to keep them safe.
2. Now ask them to choose a secret password to protect them, if someone cracks the password it will allow access to the box to take one item.
3. Have a go at playing 20 questions to guess the password. You can play a few rounds!
4. Explain that when they start to have accounts on the internet for things like emails, social media and online games, these accounts will contain important personal information that needs to be kept safe, just like these treasured items.

They will keep them safe using passwords and it's key that they are hard to guess - have a go at activity 2 to show them what makes a good password.

National Cyber Security Centre

Activity 2

1. Ask your child to draw all sorts of things they like on different squares of paper, just one on each square, anything from colouring in a patch of their favourite colour, to a teddy, a sailing boat, or the moon.
2. Put them all into a bowl and get them to take the pieces out at random and lay them out in sets of three.
3. Explain that these sets are examples of good strong passwords, they are hard to guess because they are three unrelated things – TeddyBoatMoon – but it's memorable because individually each of them means something to them.
4. You can try another round of Activity 1 and see if it's harder to guess their password!

Activity 3

1. Ask your child to collect up two or three things that are important to them, and then hide them somewhere at home.
2. The whole family can then have a go at finding them. If they're found all in one place, explain that if those things had been hidden in different places it would have stopped them being discovered in one go and protected them better.
3. If they chose to hide them separately of their own accord, congratulate them!
4. Explain that they should apply the same principle when keeping their accounts and information safe online. If a password to one of their accounts is discovered, and they use it for lots of different accounts, then all those accounts can all be unlocked at once. The most important password to keep unique and hard for others to guess, is their email account.

Activity 4

1. Cut out some squares of paper and ask your child(ren) to have a go at writing out random, but memorable words.
2. Explain as you go that they should avoid information as public as a pet name, favourite sports team or personal information such as the name of the street you live on, but it would be good to pick words such as ‘rollercoaster’ if they enjoy theme parks, ‘yellow’ if it’s a colour they like, ‘cabbage’ if it’s their most hated vegetable!
3. Put all their words into a bowl and then play at picking them out in sets of three.
4. Explain that using a password such as YellowCabbageRollercoaster is something they are likely to remember but is very difficult for someone else to guess or hack. You can also try putting it into a password strength checker online to see how long it might take to hack.

Activity 5

1. Ask your child to write down all the different accounts they have, this can be anything from an account on a shared family device or at school, to an online gaming account or social media, to an email account.
2. Now ask them to tally up how many different passwords they use for the accounts, (if there is more than one child, compare scores, the highest number wins!).
3. Explain that it is very important to use separate passwords, so that if one got into the wrong hands, it wouldn't mean someone has the key to all those accounts at once.
4. Now get them to reset one of the passwords, using the principle of three random words (you could use activity 4 to help)
5. You can find instructions for resetting passwords for a number of accounts on the NCSC Cyber Aware website: www.cyberaware.gov.uk

National Cyber Security Centre

Activity 6

1. Lay out a scrabble board with lots of words, or arrange some toys and household items in a pattern – take a photo.
2. Now ask your child(ren) to have a quick look at the words or pattern, then mix it all up.
3. Can they decipher the scrambled version and put it back to what it was?!
4. Once they've given it a go, show them the photo, look how much easier it is to restore the original with a back up of exactly what it looked like!

Make sure you keep a copy of all your important data by backing it up. If a hard drive corrupts or your device is hacked or stolen, you'll be able to get your important information, photos and treasured memories back. You can find instructions for how to turn on automatic back up on several devices on the NCSC Cyber Aware website:

www.cyberaware.gov.uk

National Cyber Security Centre

Activity 7

1. Together with your child(ren), have a read over the six top tips on the National Cyber Security Centre's Cyber Aware website (www.cyberaware.gov.uk).
2. Now ask your child to have a go at designing a campaign for how to promote Cyber Aware to their friends and other young people.
    - How will young people find, and engage with it?
    - Might there be a poster, what would it look like?
    - Would there be a webpage for their age group? How might that look, they can have a go at designing it on a piece of paper or on the computer.
    - Would there be a social media campaign, what might the posts say to catch young people's attention?
1. Encourage them to share and explore ideas with you, or with a friend.
2. They can follow the NCSC on Instagram @cyberhq to check out some of their real-life posts!

National Cyber Security Centre

Activity 8

1. With your child, watch the You Tube video ‘How private is your personal information’ https://www.youtube.com/watch?v=yrjT8m0hcKU
2. Ask your child to think through ways that leaving personal information exposed online as shown on the video, could lead to their accounts being broken into.
3. Key things they might identify that could lead to a hacked account are:
    - If any of that information is being used directly as part of a password
    - A scammer could use that information to falsely identify themselves as you by answering account security questions
    - Scammers could send you highly personalised, and therefore convincing, phishing emails, which could lead to you clicking on a dodgy link
4. In case someone does obtain your password you should add an extra layer of protection. Two-factor authentication (2FA) is a free feature that does just that, by asking you to provide a second piece of information such as getting a text or code, to check you are who you say you are.
5. With your child, try activating two factor authentication on their accounts. You can find instructions for how to do this for several email providers and social media accounts on the NCSC Cyber Aware website: www.cyberaware.gov.uk

National Cyber Security Centre