CYBER SECURITY AWARENESS

In celebration of Computer Security Day, Support Tree would like to share some insights for how you can help support and protect your child in cyberspace.

CYBER SAFETY GOLDEN RULES:

STAY INFORMED

Staying informed on the latest news and trends for cyber security means being much more alert to any cyber risks or breaches. Keeping an eye on cyber security scams or breaches - such as WannaCry in 2017 - means you can better protect your information and data. You can sign up to e-newsletters like Sophos's Naked Security update and Krebs on Security to stay informed.

NEVER SHARE PASSWORDS

An important one - never share your passwords with friends or strangers. If you or your child need help remembering passwords, you can use a password manager tool to securely save your logins and passwords. Avoid writing passwords onto paper and keeping them near the PC - this is very poor practice!

TWO-FORM AUTHENTICATION

This is where multiple steps are taken to verify your login to a specific account - usually through a smartphone or email account. Also called "Multi-factor authentication", 2FA adds an additional layer of security when logging into important / data sensitive accounts and greatly reduces the chance of unauthorised access.

STRONG PASSWORDS

This is one of the most important rules. Strong passwords made of a few words, numbers and symbols can be the difference between being hacked and being safe.

RANSOMWARE

Ransomware is now a prolific tool for cyber criminals who can easily encrypt machines. Never click on unknown links or download documents in suspicious emails from unknown individuals.

SECURITY SOFTWARE

Use up-to-date security software and make sure your OS and the software you use are up-to-date.

PASSWORD MANAGER

Never share your passwords with anyone else, including friends and family. Keep them stored in a password manager if your child needs help remembering their passwords.

TOOLS FOR SECURITY

With so many methods of connectivity today – from iPads, to social networks and gaming – knowing what your child is accessing is not quite as easy as it was ten years ago.

This said, there are now many parental control tools in place to help you protect your child online. Here are a few that can be quickly and easily set up from the comfort of your home.

ISP PARENTAL CONTROLS

Most internet service providers like Talk Talk, Sky and BT offer parental controls for you to blacklist untrusted websites. The controls include:

- *Router-level controls* - all devices linked to your home WiFi will automatically be subject to any blocks you implement.

- *Simplified settings* – some ISPs categorise content that will be blocked. EG, Sky have PG, 13 and 18 age groups.

- *"Active choice"* – people setting up their broadband for the first time are unable to complete setup until they have defined their parental controls.

SMARTPHONE OPTIONS

Aviva found 1 in 8 children have their own mobiles by the time they are 8. Whether your child owns their own device, or you allow them to use yours, you can easily set up parental controls on your phone.

For iOS devices

Apple users can set up "Restrictions". To do this, open **Settings** on your apple device, then visit **General > Restrictions**. Click **Enable Restrictions** then create a passcode. **Don't lose this code** as you will need it to access settings and make changes in the future.

After doing this, you can select the apps and features you would like to turn off.

For Android devices

With Android, you can set up a separate account on your own phone for your children to use. You can restrict the apps they can access by disabling Google Play or adding controls around downloads.

Go to **Settings > Users** then choose **Add user**. Follow the steps to create your child's account and click **Skip** if you do not want them to use Google Play.

To restrict Google Play use, open the Google Play app in their account, open the menu from the left and choose **Settings**. Look for **Parental Controls** and create a PIN. Here, you can set restrictions on specific categories.

More on Android parental controls here.

BROWSER CONTROLS

Browser controls provide a basic level of restriction for children when browsing the internet. However, we would only suggest these to be used for *younger children* as older children may have the know-how to avoid browser controls.

For YouTube

Enable **Restricted Mode** in Youtube by scrolling to the bottom of any YouTube page, and click on **Restricted Mode**. Choose **On** and click **Save** to hide explicit results. To lock this setting, log into your Youtube account.

Locking the account sets a cookie in your browser to keep restriction mode on. Of course, if your child is more tech savvy, this will not prevent them from clearing the caches!

SafeSearch

In any browser you use, you can activate SafeSearch to set up safety controls on major websites. Go to Google and click **Settings** in the bottom right corner. Choose **Search Settings** and you'll see a box to **Turn on SafeSearch**. This helps to filter a lot of explicit images and search results.

As with YouTube, you can lock SafeSearch mode by clicking **Lock SafeSearch**. You would have to do this in each different browser.

DESKTOP OPERATING SYSTEM CONTROLS

Windows and macOS both now offer built-in parental controls. These settings are much more reliable that the browsers controls mentioned previously as there isn't an easy way for them to be tampered with.

Windows

You can create a **Child Account** which significantly locks down the account. It creates restrictions to app access in the Windows Store, limits screen time and reviews what your children are doing on the computer.

Some of the restriction tools are usable outside of Microsoft Edge and Internet Explorer so should be supplemented with third-party control apps. Find out how to setup Child Account here.

Mac

Mac has built-in controls. Access them via: **Apple Menu > System Preferences** then choose **Parental Controls**.

For those without existing accounts, click **Create a new user account with parental controls** and follow the steps. You can choose from multiple age groups to create the right account (**4+**, **9+**, **12+**, **17+**).

If your child already has an account, go to **System Preferences > User & Groups**. Then select **Enable parental controls**. Apple have a more detailed guide here.

PARENTAL-CONTROL SOFTWARE

Qustodio is arguably the best third-party parental control app. There is a free and a premium version, but the free one is comprehensive enough for most.

It gives website and search result filters, time limits for apps and games, a record of computer activity and live notifications is your child accesses questionable content.

The premium version adds on social media monitoring, call and SMS tracking/blocking, location tracking and a bigger dashboard.

Unlike the free version which only monitors one device, you can monitor 15 devices with the premium version, depending on the package you choose.

KidsWatch is an award-winning tool that provides web filtering, real-time alerts and time limits. The real-time alerts are split into **Predator Alerts**, **Chat Monitoring** and **Email Alerts**.

The first alert automatically shows you if any registered sex offenders live in your area, provides a photo of their face, along with their address.

Chat Monitoring flags keywords within internet chats, like your address, phone number and references to drugs and sex. You can also add your own keywords.

For a complete guide to parental controls, visit Make Use Of's site.

PRACTICAL STEPS BY AGE

Naturally, the use of internet will vary between different age groups. We've outlined some steps to take depending on the age of your child.

AGES 6 – 9

At the age where many children start forming online habits, it's important to instil an understanding of cyber security.

- Set parental controls to match the appropriate age and allow access only to age-appropriate content for devices your child has access to.

- Find the controls your internet service provider has in place for parental controls. These can be activated at any time and allows you to blacklist untrusted or inappropriate websites.

- Talk with your child and agree a list of websites they can visit. Also explain how to be "Share Aware" when online (next page).

- If you have older children too, make sure they know what should or shouldn't be shown to their younger siblings on the internet.

AGES 10 – 12

Set boundaries for your child before they get their first 'connected device' (mobile, laptop or games console).

- Discuss what is okay to share online. Explain how anything they post online, like photos or comments, form their digital footprint which may be accessed by anyone on the internet and forever.

- 10-12-year olds may be looking for information about their changing bodies and exploring relationships. Help them understand the importance of never sending photos of themselves naked, no matter who it may be to.

- Remind them that if they wouldn't do something face-to-face, they shouldn't do it online!

- See if your child can show you how to use and set privacy settings. Ask if they ever receive messages from strangers.

AGES 13+

Your child may now think they are adult enough, they still need your wisdom and guidance!

- Make it your business to stay up to date with technology/cyber security and discuss what you find out with your child.

- It may feel awkward, but having frank talks about cyberbullying, or posting hurtful comments online may help your child to understand the implications they can have. Once it's online, it cannot be taken back.

- Give your child a budget for activities like downloading games or music online, but don't provide access to payment or financial details.

- Review and adjust your parental control settings in-line with your child's age and maturity. It can be a vulnerable time of their lives, so they may try to access dangerous information online.

Visit getsafeonline.org for more tips.

EXPLAINING CYBER SECURITY TO YOUR CHILD

Starting the conversation with your child about internet safety may seem somewhat daunting at first, but explaining cyber security is easier than you may think. Just like adults, children also do not want to be exploited of or misled by others, and this includes the internet.

You can reassure your child that you're interested in all aspects of what they do online, and that you're looking out for them. Explain that you understand the internet is a fantastic place but also express the implications of cybercrime.

BEING "SHARE AWARE"

Help your children understand that personal data is precious and shouldn't be shared with anyone aside from immediate family. This includes, name, address, school and birthdays.

ONLINE IS STILL REAL LIFE

Express the importance of understanding that the online world is still the real world. Help them understand that if they wouldn't do it in real life, they shouldn't do it in online!

ONLINE IS STILL REAL LIFE

Ask your child if they know:

- where reporting functions are
- how to block someone
- how to keep information private

NO OVERREACTIONS

Reassure your child that you won't overreact, and that they should speak up if something is worrying them online.

CONVERSATION STARTERS

The UK Safer Internet Centre has outlined the following questions for parents to ask their children to start talking about cyber security:

1. Ask about the sites you child likes to visit and what they enjoy doing online.

2. Ask them if they have tips for you about staying safe online, and where they learned them? What is OK and not OK to share?

3. Ask if they know where to find cyber safety advice and how to block/report services.

4. Think about ways you can use the internet together, if there are any activities you can enjoy as a family.

   For more information, visit www.saferinternet.org.uk.

RESOURCES

Cyber security, malware and firewalls aren't the easiest topics to explain. But tools like Cynja - an internet safety app and comic - may be much more relatable and effective in helping your children understand the importance of online safety.

Additionally, the NSPCC has plenty of information on their website helping parents understand how to keep children safe online. They also have a dedicated helpline if you need help with setting up parental controls, adjusting privacy settings or getting general advice.

The UK Safer Internet Centre also provides extensive resources from identifying issues, to safety tools and guides on parental controls.

To report concerns about cybercrime in the UK, you can contact Action Fraud, the UK's reporting centre for fraud and cybercrime.

If you would like to find out more about cyber security, you can contact James Carson at Support Tree on 0800 292 2230 or email enquiries@supporttree.co.uk.

Support tree