

Personal data is a strange commodity. Cyber thieves can buy huge quantities of personal data on the black market for very little, yet your own personal data is hugely valuable to you. If your personal data falls into the wrong hands, it could lead to identity theft, bank fraud or something even more sinister such as stalking. The severity of that threat is multiplied when it comes to the personal data of children, when threats such as internet grooming begin to emerge. The bad news is that children aren't always great at safeguarding sensitive information, which is why they need parents' help and guidance. That's why we've created this guide to show you how you can protect your own and your family's personal data.





What parents need to know about PROTECTING PERSONAL DATA

EVERY DETAIL IS KEY

Which info should you be wary of sharing online? Aside from the obvious, such as full names, date of birth and address, think of the type of information you're asked for when answering security questions for services such as online banking. The name of your first school, your mother's maiden name, the names of your pets, your favourite band. Data thieves will harvest as much of this information as possible, so don't make it easy for them by publishing it anywhere online.



SOCIAL MEDIA VISIBILITY

Social media sites, such as Facebook, encourage us to share sensitive information in order to build our online profiles. Many people are lulled into thinking that only their friends can see such information, but that's rarely the case. Such information can easily be shared with 'friends of friends' or even anyone searching for you online because privacy settings are opaque. Keep social media profiles to the bare minimum. If you wouldn't be comfortable hanging a sign with that information on your front door, don't enter it into social media sites.

DANGEROUS GAMES

Online games are a particular risk for children. Many of the most popular games – such as Fortnite, Minecraft or Roblox – have voice or text chat facilities, allowing them to talk to fellow gamers. Or, sometimes, people pretending to be fellow gamers. It's very easy for children to be seduced into divulging personal data such as their address, birthday or school. It's critical parents both educate children on the dangers on online chat in games and take safeguards to protect children.

IMPOSTERS AND PHISHING ATTACKS

Even if you're scrupulous about keeping your data private on social media, it's easy to be lulled into handing it over to imposters. There are two golden rules for you and your children to follow: 1. Never divulge personal information to phone callers, unless you can be absolutely certain you know who they are. 2. Never click on links or open attachments in emails or social media, unless you're 100% certain they are genuine. So-called phishing emails are growing ever-more sophisticated, with fraudsters able to replicate the exact look of bank emails and even include details such as account numbers and IDs.



THE RISKS OF PASSWORD SHARING

Password sharing – using the same password for multiple sites – is one of the easiest ways to lose control of your personal data. Hacking of major websites, including usernames and passwords, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, you're handing data thieves an easy route into your inbox, where they will doubtless find all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them reset the password on multiple other accounts. Don't share passwords; use password managers to create strong, unique passwords for every site.



National Online Safety®
#WakeUpWednesday

Safety Tips for Parents & Carers



LOOK OUT FOR LEAKS

Many security software packages have features that look for personal data leaks or prevent people from entering it into risky sites in the first place. For example, Bullguard Premium monitors dangerous sites for usage of data such as your email address, debit card numbers, passport number and more, and then sends you email alerts and details of how to take remedial action if it spots them being used. Such software also issues warnings if it sees personal data being entered into unprotected, high-risk sites.



KEEP DATA GUARDED

Don't give the thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email address such as davesmith1976@gmail.com – an immediate clue that you were born in that year. If you have a less common name than Dave Smith, thieves could immediately start using that information to cross reference against public records or other database breaches, allowing them to start building a profile of information about you. Likewise, don't use your date of birth in a password. If that's hacked, you've handed the thieves another big clue.

DON'T OVERSHARE ON SOCIAL MEDIA

The biggest threat to your child's privacy is you. Parents often overshare personal information on social media: full names, names of schools, children's birthdays, names of their friends. All of this can be easily gleaned to build profiles that could be used to groom your child in online games or in real life. Exercise extreme caution with social media posts concerning your children.

BE WARY OF SHARED NETWORKS/SYSTEMS

Avoid entering any personal data into a web browser when you're using public Wi-Fi (in a coffee shop or airport, for example) or when using shared computers. Shared Wi-Fi connections are much easier to eavesdrop on than your home network, especially if they are not password protected or the password is shared freely with customers. Don't do online shopping, banking or enter any logins/passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very easy for a browser to save logins that could be used by others.



PLAY SAFE IN ONLINE GAMES

Children must be taught to treat strangers in online games with the same caution as they would treat strangers in the street. Don't allow children to use their real name as their username in games to prevent imposters conning kids into thinking they are real-life friends, and only allow them to add friends in the game that they know in real life. Regularly ask to monitor your child's friends list in such games and ask them to identify who the players are. With younger children in particular, ask them to only use voice chat in family rooms, so that you can hear conversations.



Meet our expert



Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as *The Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *BBC Newsnight*, *Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues over the years.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.07.2020