What Parents and Carers Need to Know about SOCIAL BOTS

WHAT ARE SOCIAL BOTS?

Bots are computer-generated accounts which sit on social media, masquerading as humans. While many are harmless or even have good intentions, others are designed to extort, sell products, spread propaganda or bully human users. Bots – short for 'robots', of course – are often confused with state-funded troll accounts; the two can be difficult to tell apart. However, if the results are the same, then both should be treated similarly.

KNOWING THE RISKS ...

ASTROTURFING

Propaganda and conspiracy theories are usually niche interests on social media. But with an army of thousands of bots amplifying posts through retweets and shares, people can make their messages travel further and appear to reflect mainstream opinion. Known as 'astroturfing', this can make children more susceptible to questionable beliefs.

CYBERBULLYING

Bots can be set to hunt for certain search terms or opinions and then automatically reply aggressively to anybody who uses them in a message. This means that if your child posts something that whoever programmed the bot doesn't like, they may be deluged with angry messages from fake accounts – which can be overwhelming and comparable to cyberbullying.

EXTORTION

Criminals use bots to trap users into sextortion or online blackmail scams. The bot cultivates a flirtatious online relationship with the victim, then persuades them into a video chat during which they are tricked into posing inappropriately or carrying out a sexual act. This footage is recorded, and threats are then made to release it to the victim's friends and family unless money is paid.

SHADY SELLING

Bots are often used for illicit advertising – that is, they spam social media platforms with links to commercial websites. Additionally, some unscrupulous influencers have been found to use bots to artificially inflate their number of followers and the engagement with their account – making them seem more popular and therefore able to charge companies more to work with them.

SPOTTING THE SIGNS ...

BEWARE PROLIFIC POSTING

Bots post a superhuman amount of content. A visit to their profile usually proves they're responding to people far faster than a human could. Check their join date and number of followers. If the account has been around for ages and still doesn't have any friends, it probably isn't a real person. A brand-new page is also a red flag.

NOTICE ODD USERNAMES

Finding a social media username that isn't taken can be difficult. People often end up with their name and some numbers – but not the way bots do it. A username like johnsmith5273 is either a sign of a random number generator or a site offering an unwieldy alternative because the preferred name is taken, which isn't something most humans would accept.

VERIFY PROFILE PICS

Check a user's authenticity by investigating their profile picture: bots obviously don't have faces, so they tend to skim publicly available photos to try to fool people. Put suspicious pics through a reverse-image search like TinEye – you might find they actually belong to someone else or are stock images.

CHECK THE CONTENT

Bots can't think for themselves and usually just exist to amplify somebody else's message. Try copying and pasting the text into the search function on Twitter, for example, and see if it's being said anywhere else. If a lot of similar-looking accounts are saying the same thing, you're probably looking at a bot army.

Advice for Parents & Carers

SPOT THE BOTS

Forewarned is forearmed, so if your children aren't that familiar with the world of bots yet, explain what to look for using the tips in this guide. At the moment, most bots still aren't that sophisticated – so finding accounts which are designed purely to troll people or spread misinformation isn't hugely difficult, even for an untrained eye.

BLOCK AND MOVE ON

Your child isn't obliged to be friends with anyone online, bot or not. Pretty much every social media app has a block button, and you should encourage your child to use it whenever something or someone is making their digital lives less than pleasant. If everyone blocked malicious bots rather than engaging them, they wouldn't pose a problem.

BE SUSPICIOUS

While many people have made lifelong friends over the internet, it's important not to be too trusting. Random strangers adding you on Facebook could well be bots, so do some background checks: do they have any mutual friends? Is it a new account? Even if everything seems fine, encourage your child to be cautious: warn them of potential risks.

Meet Our Expert

Alan Martin is an experienced technology journalist and the former deputy editor of technology and internet culture website Alphr. Now freelance, he has contributed articles to publications including the *New Statesman*, CNET, the *Evening Standard*, Wired, Rock Paper Shotgun, Gizmodo, Pocket Gamer, *Stuff*, *T3*, *PC Pro*, *Macworld*, TechRadar and Trusted Reviews.

National Online Safety®
#WakeUpWednesday

SOURCES: https://www.computing.co.uk/feature/3085226/the-positive-case-for-twitter-bots | https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html
https://truepublica.org.uk/united-kingdom/propaganda-automated-bots-defending-the-government/ | https://www.lbc.co.uk/radio/presenters/james-obrien/what-are-the-twitter-users-with-eight-numbers/