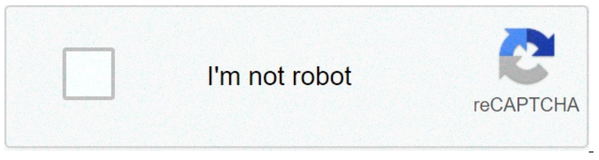

Continue

Bots to kahoot

(Image credit: Shutterstock / Sapann Design) Bots have been hitting the headlines for several years now, yet despite this, there's still mystery surrounding how they can actually affect our day-to-day lives. And I'm not talking about automated bots like you can find on Twitter. I'm talking about sophisticated bots. These operate differently and are much harder to detect.Sophisticated bots look and act like human users with most bot activity indistinguishable from human activity to the naked eye, and even to most bot detection software. This is worrying for several reasons – imagine what could be done if you were able to look like a million humans? You could, for example, "listen" to a song or "watch" a video enough times to move it to the top of the charts and quickly create the impression that something is popular or trending. You could even amplify an opinion with millions of fake interactions on a certain post.A cybercriminal needs two things to make bot-related cybercrime a success – a valuable demographic and the technology to go undetected by their victims. A recent report looking at Russian interference in UK politics shows just how powerful bots are in influencing public sentiment. Malicious sophisticated bots affect us all more than we realise and Covid-19 has demonstrated that. With the onset of the lockdown and people being forced to live their lives digitally, cybercriminals have the perfect conditions to get to work and bots are the ideal tool. As bot activity continues to rapidly evolve, here's what you need to know.About the authorTamer Hassan is CEO at White OpsGood bots vs. bad botsContrary to popular opinion, bots aren't always bad. Bots are merely software scripts living on computers - many everyday internet tasks are performed by bots all the time.For example, search engines and anti-virus companies use good bots to crawl, analyse, and catalogue data from web servers. It's when bots are used by cybercriminals that they become a threat. 'Bad bots' devised by cybercriminals can steal login credentials, hack accounts, spread disinformation, and even steal from e-commerce transactions.When cybercriminals deploy hundreds of thousands of bots to perform these nefarious acts, that's when we see the beginnings of botnets. These larger, organised botnets can drastically increase the scale of cybercriminal operations.Sophisticated bots and fraudulent appsOne of the ways cybercriminals have been making the most of people's changing behavior is via fraudulent apps, our recent research determined.In one recent campaign, users downloaded a selection of popular apps in the thousands, only to be served intrusive and out-of-context ads, then the apps became nearly impossible to delete.So how do you know if an app you're looking to install is genuine? To spot fraudulent apps, ask yourself the following questions:Do the reviews talk about ads popping up all the time? Even while on the Android homepage?Do the reviews talk about the app disappearing from the drawer and being unable to uninstall it?Do the reviews have a lot of complaints that the app doesn't work?Does the app publisher have any other apps, or is it only this one and it has a large number of downloads?If the answer is yes to any of the above, then it might be bogus and you shouldn't risk downloading it.Bots and account takeoversAnother threat to be aware of is account takeovers. Bots can use your credentials to log into your accounts, such as banking, ticketing sites, social media platforms and online stores, without ever being detected.While CAPTCHA exists, they aren't always strong enough as they can't decipher a sophisticated bot from a human, which demonstrates how human-like these bots can be. Sophisticated cybercriminal operations even pay people to crack CAPTCHA forms for ease of entry. Because of this, sophisticated bots can use your data and your personal information to be you and never get caught by traditional bot mitigation methods, all while causing mayhem on your personal accounts. For example, transferring money to themselves via your online banking account, requesting friends and family members transfer money via social media, or using online shopping sites to make purchases.Cybercriminals are able to steal your information to take over your accounts in a myriad of ways, including through your accidental download of a malicious app or through your data being a part of a data breach.To prevent this from happening, take the following steps to keep your accounts safe:Although tempting, never use the same password for multiple accounts. Instead, use a password manager to generate, store and autofill strong passwordsDon't click on any links from suspicious emails or text messages. They could lead to phishing sites or cause you to accidentally download malwareUse two-step verification or two-factor authentication wherever possible. There are a few third-party apps available to help you do thisOnly shop online from reputable brands and don't store your credit card informationIf you're a regular user of public Wi-Fi, use a VPNWatch out for signs of a phishing email. These can include spelling and grammatical mistakes, asking you to confirm personal information, or a message that has been written to make you panicOf course, while being aware of bots and how to spot them is a good first step, it should still form part of your wider cyber-defense. This means getting the basics right when it comes to cybersecurity, such as having strong passwords and up-to-date software.As with any new threat, education is key – the more you know, the better protected you are. With bots increasing in sophistication every day one thing is certain – bots aren't going away any time soon. But, we can be smarter internet users by making it harder for them to exploit our information.Check out our list of the best endpoint protection services around "A name that's straightforward has only one layer. You want to allow people the pleasure of exploring it." —Diane Prange, chief linguistics officer, Strategic Name Development"You need to have a fairly broad appeal with a name. Check in with speakers of your major market languages to make sure it doesn't say something bad." —Nathan Shedroff, coauthor, Make It So: Interaction Design Lessons From Science FictionThe future is friendly"Names should entice us into the future, but not scare us away. Like the best names for people, these names should be rooted in tradition, but also imbued with newness." —Alex Frankel, author, Wordcraft: The Art of Turning Little Words Into Big Business Have a question about pricing? Connect with Software Advice to learn about potential unexpected costs, price ranges, pricing for other recommended alternatives, and more! Have a question about pricing? Connect with Software Advice to learn about potential unexpected costs, price ranges, pricing for other recommended alternatives, and more! Have a question about pricing? Connect with Software Advice to learn about potential unexpected costs, price ranges, pricing for other recommended alternatives, and more! Have a question about pricing? Connect with Software Advice to learn about potential unexpected costs, price ranges, pricing for other recommended alternatives, and more! Short for robot, a computer program that runs automatically.