# To Bot or Not to Bot

# worksheet

One of the mandatory business objectives of any company doing business online is to prevent fraud through their service, site, or sale, including the integrity and security of their customers. But there's a balance that has to be struck. The companies can't be so heavy-handed with their defense that users feel like they're applying for a government license. The best defense is direct and relatively swift like a doorman sizing a person up before they’re admitted to a club.

The situation becomes a little bit like medicine — nobody wants to be sick but nobody wants to be over-medicated, burdened, walking with a cane, or popping pills every ninety minutes. The online fraud defense has to work, but it has to be quick, like popping a vitamin. So what is the balance?

Unfortunately for online vendors, there's a relationship between advancement in technology and advancement in the complexity of online fraud. Bots have become the go-to means of accessing personal information. The term *bot* is just the programming slang for robots. The technology world loves to create its jargon, like a bot, bug, virus, and a whole unofficial dictionary of terms they bandy about in open space coding hubs at startups and online work forums. It’s almost like if they didn’t say it then the word doesn’t exist, hence robot to bot. One keystroke that is better than three is the coder mantra, efficiency and reduction being key motivators, that and the general *cool* of the ever-growing tech slang.

A bot is not necessarily a good or bad thing. No doubt you’ve interacted with many bots by now if you’re online regularly. Most of the social media platforms use them. There are bots to assist people with the elementary first tasks associated with learning how to navigate a website for the first time, bots to help you make better decisions online, bots to answer questions and connect you with online knowledge bases and documentation. Bots crawl through the web to gather your results every time you do a Google search. Then there are the bad bots, and, like their benign brethren — the unfallen — they are an army of unconscious servants who go out and do a fraudster’s bidding as they have been programmed to do. They don’t eat. They don’t sleep. They don’t need any respite from their task. They simply try, fail, try again, fail, try again, and succeed. Such is the nature of programmed technology.

There’s a fully formed negative bot economy now. The whole system has even become structured like a supply chain. Gone are the days when the fraudster had to be an adept coder. Now they can go on the dark web and buy what they need like a shopper at the mall. There are even instructional videos and how-to documents to deploy bots with an elementary task configuration — Ikea bots are so simple you can configure them yourself, imagine that. Like people, bots come in different shapes and sizes, and with different talents and abilities. One of the most popular forms of attack is the *brute force* attack. These are very simple programs carried out on a large scale. It doesn’t matter to the scammer who deploys them that ninety-nine percent of them will fail. They’re sent out in such volume that the one percent success rate is enough for the fraudsters to call it a success in terms of fraudulent gains. It’s like sales in that way — you keep your numbers up you keep your sales up.

There are now highly sophisticated bots, like the Nexus Six androids in Ridley Scott’s cult-classic film *Blade Runner*. In that seminal work, based on a novel by the extraordinary science fiction writer, Philip K Dick, special police, called *Blade Runners*, are employed to run a test on possible Nexus Six androids to determine whether they are an android or a real human beings. That’s how well the Nexus Six android can blend in with people. Unfortunately for us, the bot world has reached that level as well.

Bots can now open social media accounts to spread misinformation, and propaganda, or initiate spamming or phishing attacks. They can send phishing emails or messages to try to trick people into giving sensitive data or enter a secure website where the scammer can capture the login and password. They can stuff credentials, which is a perpetual attempt to gain access to accounts with username and password combinations, and they can post fake advertisements to pollute the metrics needed by marketing companies to gauge success in advertisements. They can be used to sabotage other companies by scraping e-commerce websites for pricing information and making phony reviews or purchases. They can scalp tickets by mass purchasing when they become available and then selling them online for inflated prices. Then there is a whole other mischief they can get into with distributed denial of service (DDoS) attacks. Bots can form botnets and launch these attacks to disrupt websites and online services. They’re even used in financial markets for *pump-and-dump* schemes. The list is quite long, but you get the idea. Almost anything a motivated scammer could do with a computer and keyboard can be done on a much larger scale with bots.

Now that you understand the security landscape, and the necessity of some form of defense, you can see the dilemma — how do companies defend themselves and their customers without becoming too obtrusive? A common defense used by companies is some form of captcha defense. You’ve no doubt used these before even if you didn’t know that they were called *captcha*. In many instances, you're asked to solve a question or to select a series of images along a theme. You’re told at the very beginning of the exercise that this is to prove you’re not a bot, or, more simply, that you’re human. It used to be that a captcha was enough. It used to be that one dimension was all that was needed. Not anymore.

Now you need something that can learn. The very best capture programs on the market today, like hCaptcha™, incorporate the very best of machine learning (ML) and artificial intelligence (AI). Every decision that a user makes is informing something in the back end through an algorithm and the intelligence of the hCaptcha program is growing. This is what we call intelligent defense. It seems to be the middle ground between the tedious task of making sure users are human and the frustration users feel by having to go through too many hoops.