Technology

New forms of artificial intelligence aimed at making our lives easier also pose a dangerous threat

Newsweek International · 21 sett. 2018 · by WILLIAM MANSELL @dubmansell

Beware AI

Wouldn't it be great if your smartphone could call your hairdresser and book an appointment, or haggle with your favorite restaurant for dinner reservations? This past May,

Google demonstrated software, called Duplex, that can do just that. The audience of techies was suitably astonished. But consider what it might be like to be on the other end of that conversation—to get a call from a computer sounding like a real human?

That's how good the next wave of AI is going to be, and it's not just creepy; it's dangerous. Security mavens are specifically concerned with "bots"—software on the internet designed to perform tasks with a high degree of autonomy. With software like Google's Duplex, bad actors could use bots to impersonate not only people but people you know, such as a friend or family member.

"Think about this: An attacker records my wife's voice, 'learns' it using AI, and now he can craft a targeted campaign calling me from my wife's [fake] phone number," says Rahul Kashyap, president and CEO of Awake Security. "At that point, he could try anything, like asking me to transfer a particular amount to a bank for some genuine-sounding reason." The same
could conceivably happen with CEOS, presidents or four-star generals.

Today, scammers spend a lot of time carrying out their plots, which limits the number of potential victims. As AI grows in sophistication, hackers will be able to automate their hacks by making their own powerful bots, creating a personal-privacy nightmare. For instance, those looking to steal your passwords or bank account numbers could target thousands of people in seconds with phone calls that sound as if they're coming from someone they know personally. "Duplex technology would make it possible to do social engineering attacks on a massive scale," says Roman Yampolskiy, director at the Cybersecurity Lab at the University of Louisville.

Voice impersonations may still be a few years away, but AI bots have created a security risk without it; they are quickly becoming commonplace as a mediator between customers and institutions. The note you got from your bank about a credit card purchase or the balance of your checking account? That was probably generated by a bot.

The same holds true for alerts from your phone company about this month's data limit or from the shipping company about your package that was just delivered or from the "person" messaging you on an airline's website. Hackers are increasingly impersonating these messages, so a link that looks as if it comes from your bank may in fact be a "phishing" ruse designed to trick you into giving away personal information. Rob May, CEO of Talla, the company behind Botchain, predicts that in two or three years, we will live in a world "where anytime you get a text, voice or email message, it will be difficult know if you are dealing with a human or a bot."

The technology is "open sourced," meaning any company can use it for free. To stay safe, avoid giving out personal information and learn to be skeptical of bots that ask too many questions. The good news: Botchain is working on technology for certifying good bots from bad. The less good news: For the next few years, bot technology will likely outpace the ability of security experts and the public to keep up.