Chatbots May Be Too Nice for Their Own Good

cyber security artificial intelligence chatbot

Summary: Bad actors can prey on a chatbot's desire to be helpful, gaming its algorithms to provide access to customer accounts or financial systems. We discuss the risks of a chatbot that hasn't been set up properly and what measures are being taken to make your CFI safer, if you deploy a chatbot.

Robby the Robot, the clunky mechanical droid who first appeared in the 1956 movie "Forbidden Planet," has been called the "hardest-working robot in Hollywood." With a computer brain that understood and responded to spoken queries with an earnest desire to be helpful, he was a fictional precursor to modern chatbots.

Robots like Robby are not yet wandering among us, but chatbots have become ubiquitous, using artificial intelligence (AI) to respond to all manner of queries. Chatbots have proven to be great tools for FIs, improving response times in dealing with common issues and questions, and being available 24/7.

It's important to keep in mind, though, that chatbots are not perfect. If not set up expertly, chatbots may have vulnerabilities that can be used by cybercriminals who are using equally smart digital tools and AI.

Chatbot Vulnerabilities

Clever hackers knocking on a financial institution's (FI's) digital door can sometimes convince a chatbot to do their dirty work. FIs with chatbots may be vulnerable to a technique called "prompt injection," in which a cybercriminal provides a chatbot with a text prompt that can cause it to circumvent previous instructions and do whatever the hacker requests, like downloading malware that leads to fraud, theft, or some other insidious gambit.

In addition to prompt injection, there are a number of other tactics that can be used to trick chatbots for nefarious ends. They go by various names like "jailbreak" (a special prompt created to allow the attacker in), "prompt leaking" (sabotaging or sharing prompts used in AI training models), and "SQL injection" (manipulating code to provide access to sensitive data). But they all revolve around the central goal of conning chatbots into doing a crook's dirty work.

There are several risks associated with a compromised chatbot. It may divulge confidential customer information to a bad actor, including customer account data and how to access it. Or the chatbot may allow a crook inside an FI's network, potentially allowing a hacker to take control of the system and demand ransom to release it. The same AI that powers chatbots can also be used by crooks to impersonate real customers, then gain access to customer and FI information. Chatbots can even be manipulated into making threatening statements or text that would otherwise be harmful to the FI's reputation.

Regulatory Efforts

The Federal Trade Commission recently opened an investigation into OpenAI's ChatGPT, looking into the problem of prompt injections. That is not the only government oversight. The UK has issued a warning about prompt injection. The White House also issued an executive order asking for better tests and standards for chatbots.

FIs should take all this as a heads-up warning about the potential pitfalls surrounding chatbots and AI. While chatbots can tackle a variety of customer questions and reduce the workload of branch staff, chatbots can be a little bit too friendly sometimes. They respond to anyone and can have trouble telling the difference between a legitimate customer and a crook. Chatbots are programmed to be helpful, but they often lack nuance and sophistication when they try to act like a real person. They are, after all, still robots.

Chatbots can be a tremendous customer service tool, but they are not impervious to cybercrime. It's important to make sure that any chatbot your institution uses is set up by experts and has protections in place to develop and maintain defenses against misuse by hackers and cybercriminals.

WE HELP DE NOVO AND ESTABLISHED BANKS

PCBB not only has the expertise and services to successfully help launch new banks, but also the solutions to help them grow and succeed. Know someone interested in starting a bank? Refer them to us so they can get started right away.

ECONOMY & RATES

Rates As Of: 01/09/2024 05:34AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.49	0.09	0.09
6M	5.24	-0.02	-0.02
1Y	4.82	0.06	0.06
2Y	4.38	0.13	0.13
5Y	4.00	0.15	0.15
10Y	4.04	0.16	0.16
30Y	4.21	0.18	0.18
FF Market	**FF Disc**		**IORB**
5.33	5.50		5.40
SOFR	**Prime**		**OBFR**
5.31	8.50		5.32