

Forum:[Hack Forums](#)

Thread: [Cybercriminals Exploit Xs Grok AI to Bypass Ad Protections and Spread Malware to](#)

Stanley - September 14, 2025, 8:35 am

Cybercriminals Exploit X's Grok AI to Bypass Ad Protections and Spread Malware to

Cybersecurity researchers have flagged a new technique that cybercriminals have adopted to bypass social media platform X's malvertising protections and propagate malicious links using its artificial intelligence (AI) assistant Grok.

The findings were highlighted by Nati Tal, head of Guardio Labs, in a series of posts on X. The technique has been codenamed Grokking.

The approach is designed to

<https://thehackernews.com/2025/09/cybercriminals-exploit-xs-grok-ai-to.html>

plops - September 14, 2025, 8:36 am

Haha an dude. This whole ai exploitation is getting wild. I really wonder how you combat it with out stoppi g ai responses

The Pact - September 29, 2025, 2:19 am

"Grokking" is part of a Traffic Distribution System used by shady ad tech vendors to route users to deceptive content.

Researchers at Guardio Labs have identified hundreds of accounts engaging in this behavior, posting thousands of ads with embedded malware until they're suspended.

Hackers - September 29, 2025, 6:05 am

(Sep 29, 2025 02:19 AM)The Pact Wrote: [\[CITE\]](#) "Grokking" is part of a Traffic Distribution System used by shady ad tech vendors to route users to deceptive content.

Researchers at Guardio Labs have identified hundreds of accounts engaging in this behavior, posting thousands of ads with embedded malware until they're suspended.

I mean, Grok itself is full of deceptive content and advertises Musk's beliefs over valid facts.

I don't think anything has really changed?

Chorozon - September 29, 2025, 10:46 am

Grok strikes again

Yanix - September 30, 2025, 4:57 am

It's ironic that Grok was built to enhance the platform, and now it's being turned into a tool for spreading malware. Tech giveth and tech taketh away.

DemonAsylum - October 1, 2025, 2:40 pm

I can't imagine anyone is too shocked to see that something like this ended up happening at least once.

The Pact - October 2, 2025, 2:39 am

(Sep 29, 2025 06:05 AM)enki Wrote: [\[CITE\]](#) I mean, Grok itself is full of deceptive content and advertises Musk's beliefs over valid facts.

I don't think anything has really changed?

I never really encountered that, but I guess I wasn't asking Grok about anything political.

Hackers - October 2, 2025, 8:29 am

(Oct 2, 2025 02:39 AM)The Pact Wrote: [\[CITE\]](#) I never really encountered that, but I guess I wasn't asking Grok about anything political.

I'm sure there are positives too, obviously there's a lot of money and data behind it. Not saying it's completely useless, but there have been too many cases of "realignments" for certain topics.

Unfortunately Musk / Xwitter abandoned their dream of being an uncensored platform with an uncensored AI model.

My concern is that we can only track so much. How many other topics (even non-political) are "realigned"?

Where does the buck stop?

Has Grok been modified to align with the views of billionaires and the 1%? Will it be truthful about South Africa?

Once an AI has been modified to "align" in a forceful way, nothing can be trusted.

If the model is instructed to ignore certain statistics, how can we trust its math in other areas?

Not arguing with you, just food for thought. I wouldn't want an AI that is required to ignore all conservative points of view, just like I don't want an AI that is required to ignore other points of view.

My only desire is to have purely pragmatic AI that doesn't care if someone cries about verifiable statistics, information, etc.

That's extremely hard when a political group says that almost every reputable organization is "fake news". When the world's top scientists and researchers are rejected because someone claims it's "politics" instead of verifiable information, how can we trust anything from that platform?

Perhaps Grok is built on the tears of snowflakes, intending to prevent more - Perhaps a better measure of accuracy might be those very same snowflake tears streaming in at full speed.

The Pact - October 2, 2025, 10:30 am

(Oct 2, 2025 08:29 AM)enki Wrote: [\[CITE\]](#) I'm sure there are positives too, obviously there's a lot of money and data behind it. Not saying it's completely useless, but there have been too many cases of "realignments" for certain topics.

Unfortunately Musk / Xwitter abandoned their dream of being an uncensored platform with an uncensored AI model.

My concern is that we can only track so much. How many other topics (even non-political) are "realigned"?

Where does the buck stop?

Has Grok been modified to align with the views of billionaires and the 1%? Will it be truthful about South Africa?

Once an AI has been modified to "align" in a forceful way, nothing can be trusted.

If the model is instructed to ignore certain statistics, how can we trust its math in other areas?

Not arguing with you, just food for thought. I wouldn't want an AI that is required to ignore all conservative points of view, just like I don't want an AI that is required to ignore other points of view.

My only desire is to have purely pragmatic

That's extremely hard when a political group says that almost every reputable organization is "fake news". When the world's top scientists and researchers are rejected because someone claims it's "politics" instead of verifiable information, how can we trust anything from that platform?

Perhaps Grok is built on the tears of snowflakes, intending to prevent more - Perhaps a better measure of accuracy might be those very same snowflake tears streaming in at full speed.

No, I actually completely agree with you. I've barely used it since he put the rate limits on it and I think when I was using it a lot he hadn't started neutering it to make it align with his views yet either. He ruined what was actually the best free bot out there by far. I don't really know what it's like now. I probably will go back to it for some things but I haven't recently. I was using it daily for a while and loving it before he decided to mess it up.

Hackers - October 2, 2025, 10:50 am

(Oct 2, 2025 10:30 AM)The Pact Wrote: [\[CITE\]](#) No, I actually completely agree with you. I've barely used it since he put the rate limits on it and I think when I was using it a lot he hadn't started neutering it to make it align with his views yet either. He ruined what was actually the best free bot out there by far. I don't really know what it's like now. I probably will go back to it for some things but I haven't recently. I was using it daily for a while and loving it before he decided to mess it up.

Yeah honestly, the whole "situation" is sad to me.

I read books on Musk, was a fan of Musk, and loved his businesses.

At one point I was convinced that he had a plan to:

- Automate transport - In progress with Tesla
- Provide near planet-wide networking - Complete/capable with Starlink
- Offer multi-planet messaging with small data transmissions - Failed or Unlikely with X/Twitter
- Terraforming - Limited in scope/capabilities with The Boring Company
- Decentralized finance - Not by Musk, but DOGE/etc was supported by him
- Hyperloop was cool too

The man had everything lined up for a multi-planet comms network, autonomous vehicles, terraforming, and finance.

I have no idea where he fell off, but holy shit he has not met my expectations.

I used to truly believe in Elon Musk. I don't consider anything I'm saying "political" in this post for anyone else reading...

He has completely botched his own goals...

Tesla is years behind their own goals and competitors caught up quickly, and moved past.

Starlink is great but the risk of space debris and non-gov control is a huge international security risk.

Twitter is nowhere close to the quality needed for decentralized / uncensored galactic comms.

The Boring Company did well but I'm not sure they've really revolutionized anything.

Hyperloop never came to fruition in the way it was pitched / imagined originally.

Grok has suffered from the same fate as many of his other companies

He doesn't know how to walk away and let something prosper when it's budding & about to bloom

I don't even want to get into what he's doing with X AI, Twitter, and other shares/equity as collateral to pass debt on.

To me, Elon is a conman or seriously over-optimistic and too loose w/ his promises to investors.

The Pact - October 2, 2025, 11:17 am

(Oct 2, 2025 10:50 AM)enki Wrote: [\[CITE\]](#) Yeah honestly, the whole "situation" is sad to me. I read books on Musk, was a fan of Musk, and loved his businesses.

At one point I was convinced that he had a plan to:

- Automate transport - In progress with Tesla
- Provide near planet-wide networking - Complete/capable with Starlink
- Offer multi-planet messaging with small data transmissions - Failed or Unlikely with X/Twitter
- Terraforming - Limited in scope/capabilities with The Boring Company
- Decentralized finance - Not by Musk, but DOGE/etc was supported by him
- Hyperloop was cool too

The man had everything lined up for a multi-planet comms network, autonomous vehicles, terraforming, and finance.

I have no idea where he fell off, but holy shit he has not met my expectations.

I used to truly believe in Elon Musk. I don't consider anything I'm saying "political" in this post for anyone else reading...

He has completely botched his own goals...

Tesla is years behind their own goals and competitors caught up quickly, and moved past. Starlink is great but the risk of space debris and non-gov control is a huge international security risk.

Twitter is nowhere close to the quality needed for decentralized / uncensored galactic comms. The Boring Company did well but I'm not sure they've really revolutionized anything. Hyperloop never came to fruition in the way it was pitched / imagined originally.

Grok has suffered from the same fate as many of his other companies. He doesn't know how to walk away and let something prosper when it's budding & about to bloom.

I don't even want to get into what he's doing with X AI, Twitter, and other shares/equity as collateral to pass debt on.

To me, Elon is a conman or seriously over-optimistic and too loose w/ his promises to investors. The man had an operation to make his penis larger that completely failed and made him impotent and that's why only his first child that he claimed died in his arms but that the mother of that child says died in HER arms....well that was the ONLY child he had by regular sex. Since then he tried a "revolutionary" operation to have a bigger dick and ruined it so he can no longer have sex so all the other children were via IVF.

Then he decides to try a revolutionary method to make all his babies have XY chromones and ends up with an INTERSEX [that means both sets of genitals] baby that unsurprisingly really ends up being a transwoman. Bit different from other trans when she's intersex and she says he was there 10% of her life only there to yell at her for having to high and girly a voice as a child.

As for people buying Teslas because he put that they would ONE DAY in the future would be able to self drive, but not now.....and they still CAN'T. How is that not a scam really. You buy something and pay the high price partly because you are told they will one day self drive.....but they never self drive. That's a scam? Is it not?

Oh also he called a guy who saved kids in a cave a pedo for saving them before his vehicle could. Then he called someone else a pedo that had objected to something he did forget who that was.

The third person he calls a pedo is Trump when they fell out over the Big Beautiful Bill. Calling a man a pedo for disagreeing with you is about as low as you can go....but that's his go to.

I will say though that Grimes said that the person Musk is today is unrecognizable from whom he used to be, so that's something to make you feel better.

oRequiem - October 2, 2025, 8:06 pm

(Sep 14, 2025 08:36 AM)plops Wrote: [\[CITE\]](#) Haha an dude. This whole ai exploitation is getting wild. I really wonder how you combat it with out stoppi g ai responses
Probably going to keep happening too lol

Fish - October 5, 2025, 2:35 am

(Sep 14, 2025 08:36 AM)plops Wrote: [\[CITE\]](#) Haha an dude. This whole ai exploitation is getting wild. I really wonder how you combat it with out stoppi g ai responses
AI responses will be hard to stop. More and more people are adopting it daily

icole - October 5, 2025, 8:36 am

AI being used to be spread malware is insane.

Oh_Well - October 5, 2025, 12:17 pm

platforms must pair AI features with stricter output controls and real-time link vetting

DAL-SHA - October 7, 2025, 4:13 am

Using Grok AI to spread malware shows how even helpful tools can be abused. Platforms must act fast to close these new attack paths?