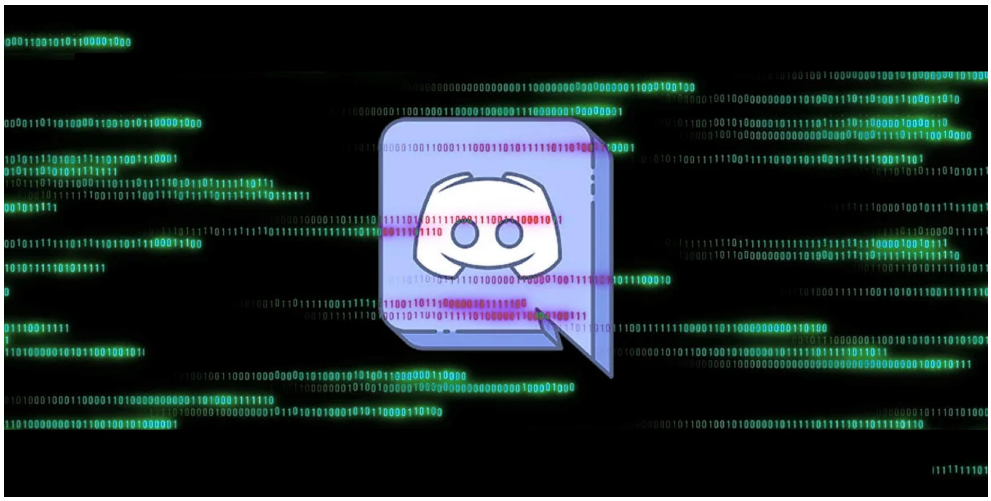
Beware: Free Discord Nitro phishing targets Steam gamers

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** November 3, 2021 02:22 PM **0**

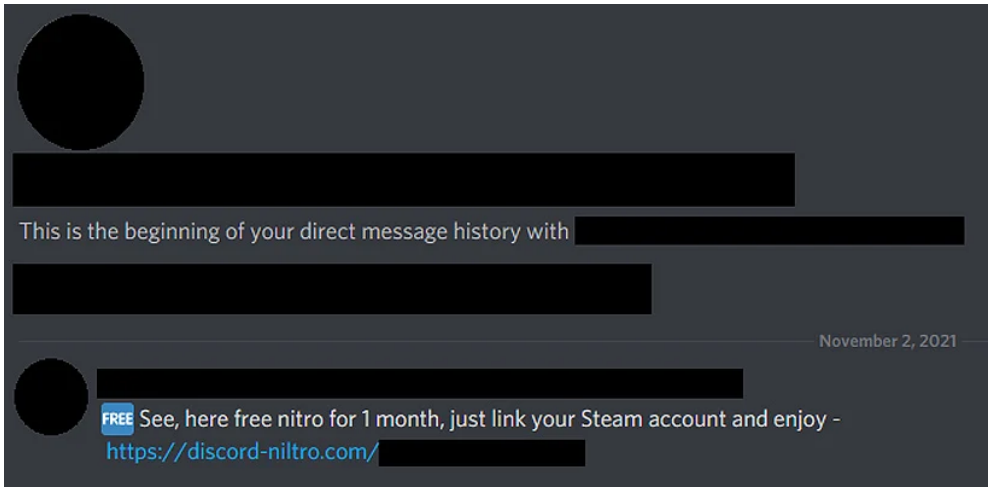


A new Steam phishing promoted via Discord messages promises a free Nitro subscription if a user links their Steam account, which the hackers then use to steal game items or promote other scams.

The phishing scam is being conducted by many Discord accounts controlled by the threat actors or as automated bots that send other users links to what is supposedly a guide on how to receive Discord Nitro for

free.

"See, here free nitro 1 month, just link your Steam account and enjoy," reads the phishing messages sent to Discord users as shown below.

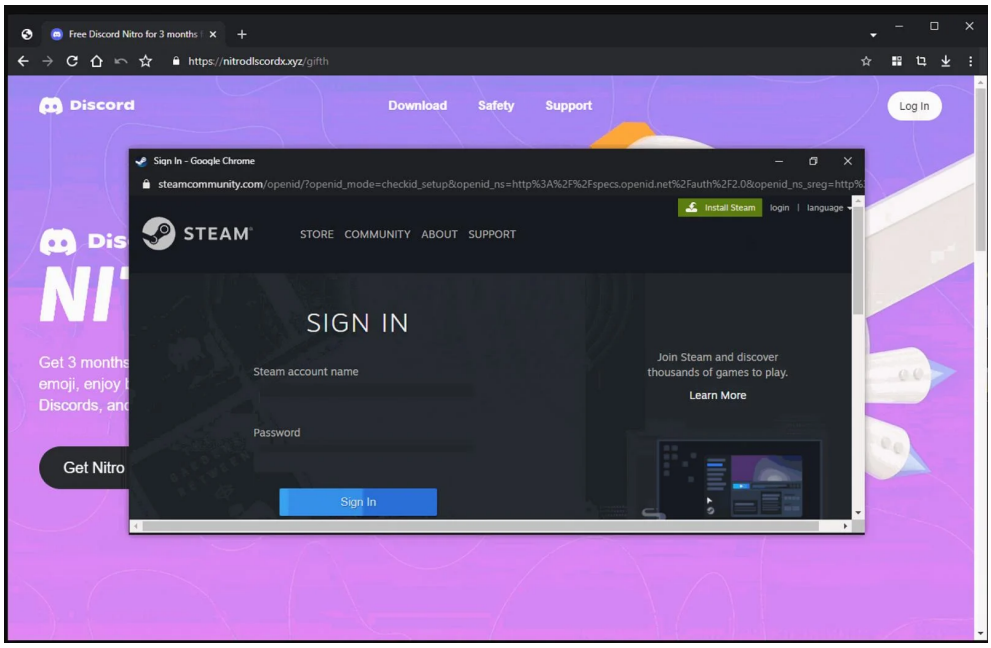


Baiting victims with direct messages on Discord
Source: Malwarebytes

While this sounds like a promotional campaign (other than the grammar), the links take victims to a phishing site that the attackers made to look like a legitimate Discord page promoting the Nitro feature.

After clicking on the "Get Nitro" button, a fake Steam login form is displayed, which looks almost identical to the legitimate form.

In reality, the pop-up is a new window opened right on the phishing page, so whatever Steam credentials are entered are sent directly to the hacker's server.



Fake Steam sign-in pop-up on the phishing site
Source: Malwarebytes

When attempting to login, victims are shown an error saying, "The account name or password that you have entered is incorrect," and prompts the user to log in again.

This double-verification method ensures that no typing errors were made during the phishing process and that the stolen credentials are correct.

Nitro as bait

Discord Nitro is a paid membership plan on the popular VoIP and instant messaging platform, which comes with a set of highly sought-after account customization, content uploading, and server boost perks.

Such is the popularity of Nitro that we've seen malware strains distributed using the same bait (https://www.bleepingcomputer.com/news/security/discord-modified-to-steal-accounts-by-new-nitrohack-malware/) and even ransomware gangs asking for Nitro gift codes (https://www.bleepingcomputer.com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/) in return for a working decryptor.

The latest scam analyzed by Malwarebytes (http://blog.malwarebytes.com/malwarebytes-news/2021/11/this-steam-phish-baits-you-with-free-discord-nitro/) is very similar to the one seen by BleepingComputer in the Summer of 2019. However, with that scam, threat actors used a "free game" as bait (https://www.bleepingcomputer.com/news/security/steam-accounts-being-stolen-through-elaborate-free-game-scam/) to serve victims with a fake Steam single sign-on page.

As these landing URLs get reported and blacklisted, actors register new ones and move their malicious operations to new infrastructure, as shown by the list below shared by Malwarebytes.

```
1nitro.club
appnitro-discord.com
asstralissteam.org.ru
discord-steam-promo.com
discordgifte.com
dicsord-ticket.com
discord-appnitro.com
ds-nitro.com
nitro-discordapp.com
nitrodsgiveways.com
steam-nitro.online
```

Domains used in the recent campaign.
Source: Malwarebytes

Similarly, phishing lures are constantly changing with new lures to intrigue gamers with a promise for something free.

With that said, when using Discord, users should be suspicious of any messages claiming to offer something for free if they click on an URL.

There are no things offered for free outside the platforms themselves, so if Steam and Discord run a promotional campaign together, you would see it on either of the respective official apps/websites.