kaspersky daily

Phishing in Netflix and beyond

We analyze some typical examples of phishing bait for movie streamers.

November 17, 2021

Movies and TV shows have been a huge source of comfort for many in these COVID times, and the number of new shows on Netflix, Amazon Prime, and the like has skyrocketed. But when searching for the latest megahit, don't neglect basic security measures or you might find that someone else is enjoying it at your expense — or worse, that the money in your bank account has evaporated.

It's more fun to ponder what to watch next than to dig through security settings, but attackers are ready and waiting to siphon off your personal and payment information.

Phishing bait

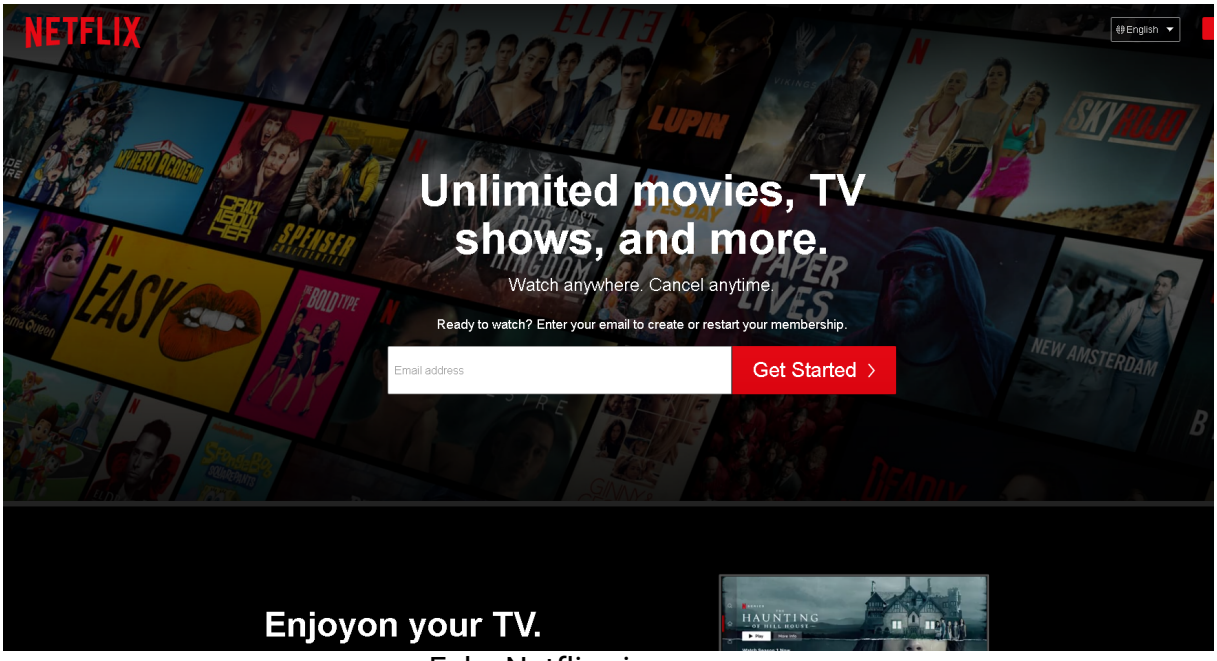
Streaming services offer a variety of payment plans, but generally they all involve paying with a credit card. And where there are card details, there is phishing. What's more, newbies and seasoned account holders may experience different forms of bait. We collected some examples from users who agreed to share threat information.

“Subscribe now!”

To sign up for a streaming service, you need a valid e-mail address; and to pay, you need some form of online payment such as a credit card or PayPal account. (If you plan to watch Apple TV, you’ll also need an Apple ID.)

Unsurprisingly, cybercriminals have created fake sign-up pages to net all of those goodies in one go. Armed with your info, they can withdraw or spend your money right away; your e-mail address should come in handy for future attacks.

In the example below, the fake site is not very convincing. Can you spot the phishing signs?

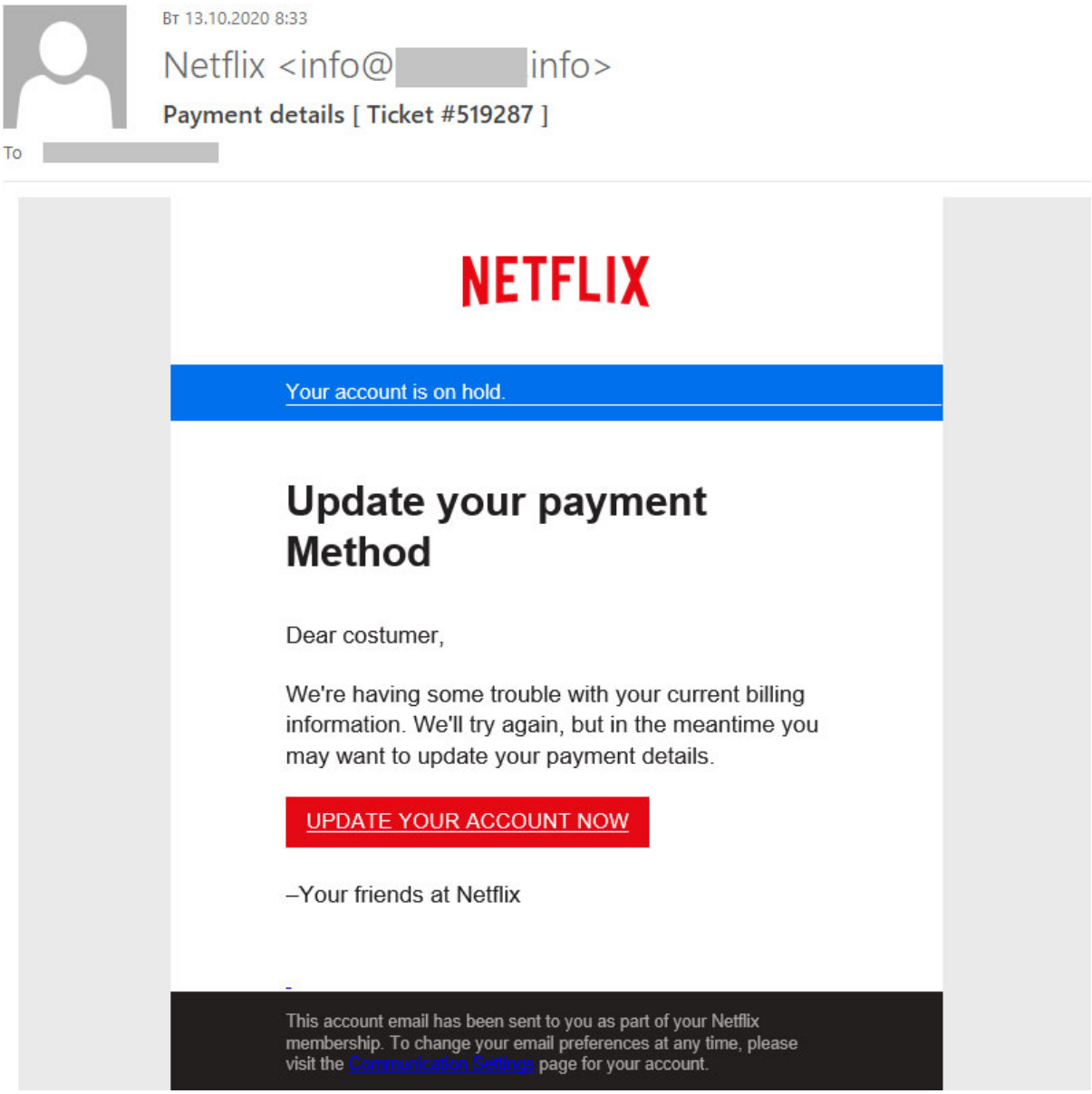


Fake Netflix sign-up page

“Refresh data”

If you already have a paid subscription, then attackers will threaten to block it, assuming, logically, that you value it. Here’s an e-mail from “friends at Netflix,” telling the recipient to update or confirm payment details or they’ll close the account. And it

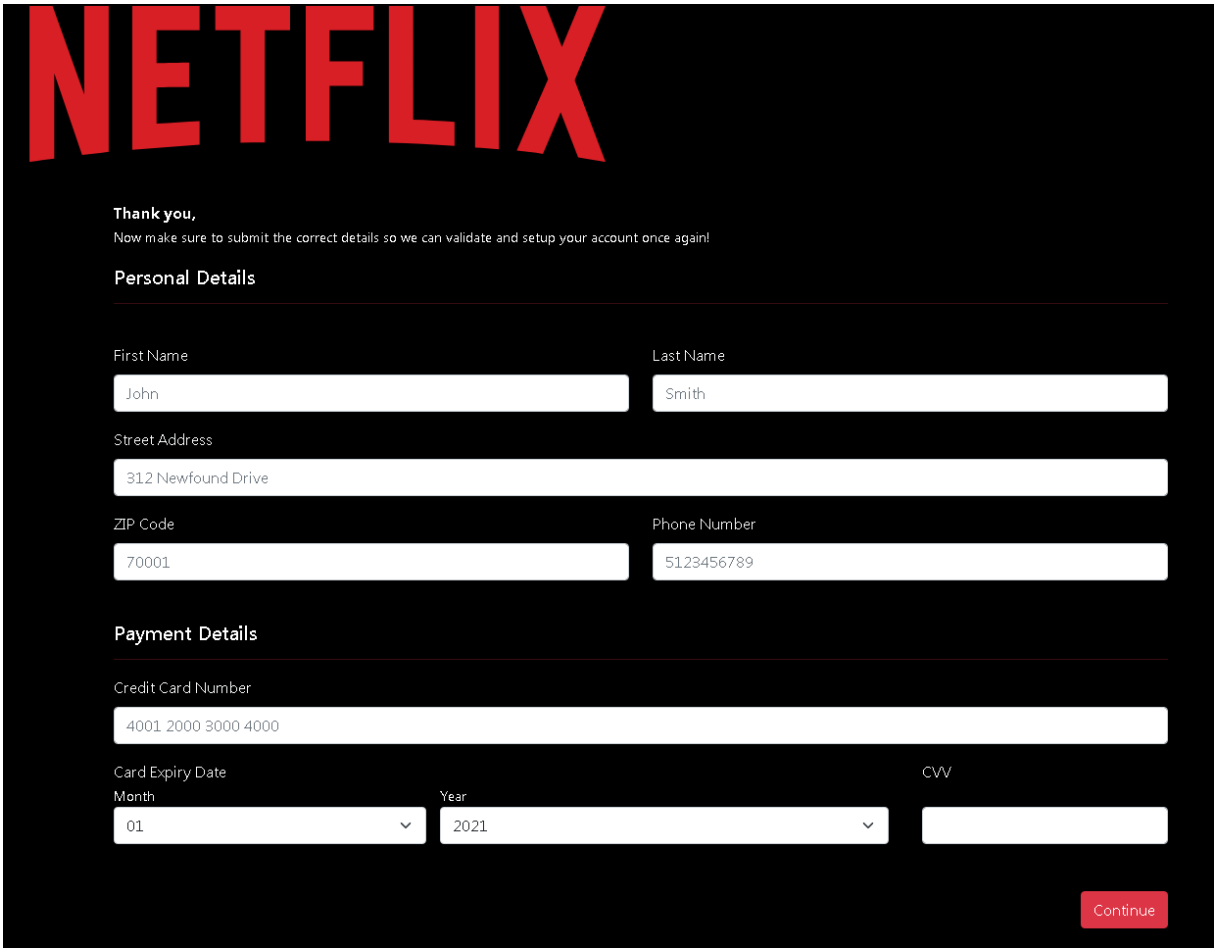
includes a big, red button. Don’t rush to click that — remember what happens in the movies when they push the big, red button?



“Dear costumer, please update your account”

The link takes you to a payment confirmation page.

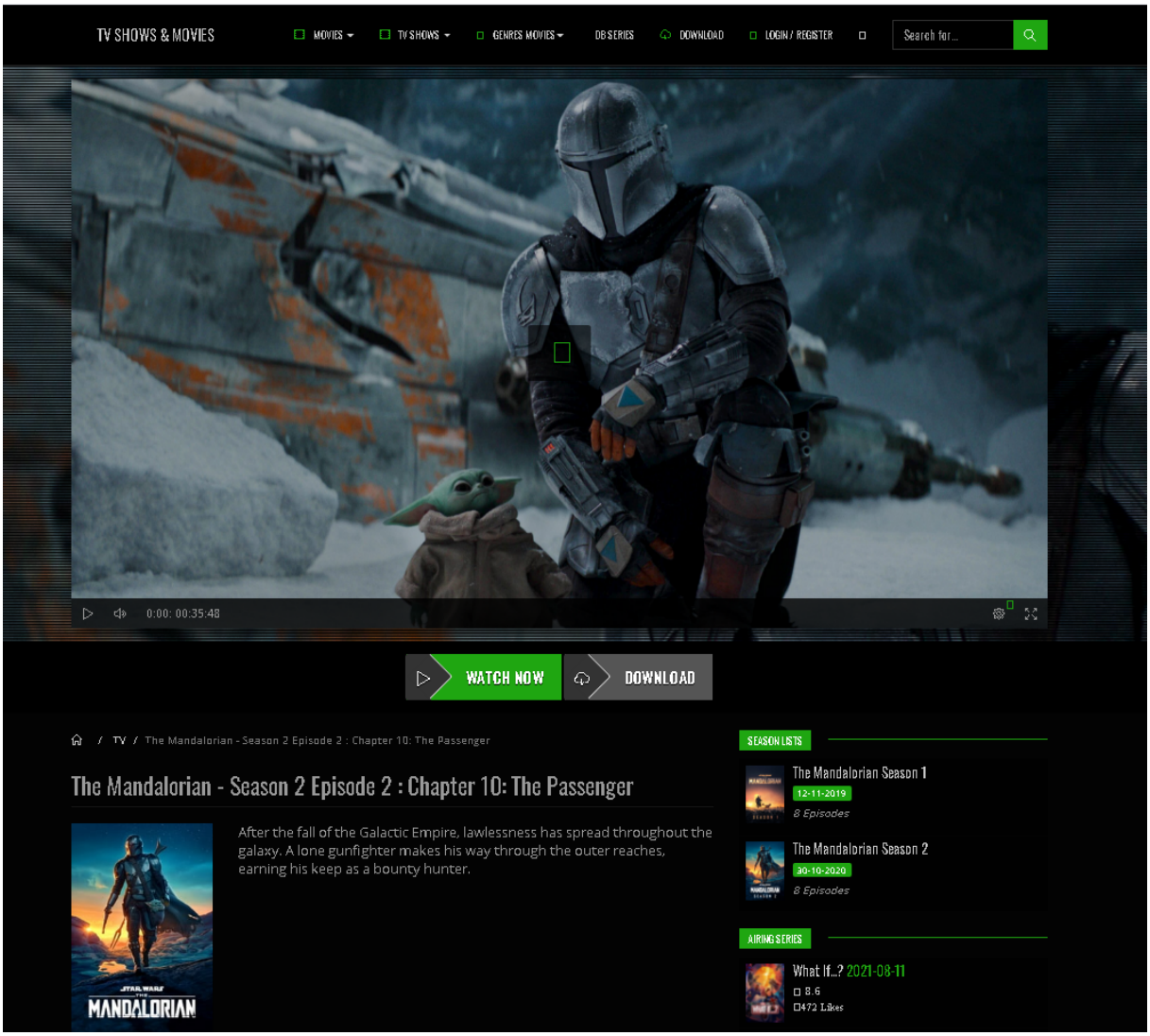
Now, many phishing messages contain such obvious mistakes as addressing “costumers,” but take the form below as an example that actually looks plausible. It has no spelling mistakes or weird design elements, but the inattentive user who falls for it could lose money from their bank account.



Fake Netflix website prompts to enter personal and banking data, allegedly for account reactivation

A dangerous premiere

In the example below, cybercriminals used popular shows to attract fans who didn't have subscriptions, offering them the opportunity to watch the shows on the fake website.



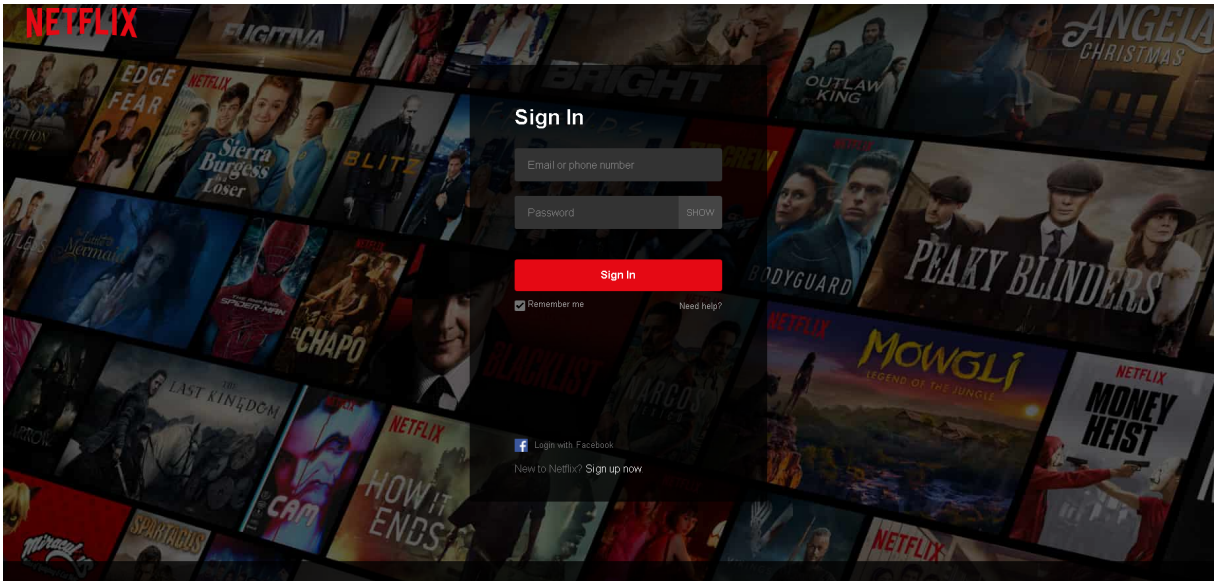
This unofficial page invites fans to watch or download The Mandalorian

As a teaser, they show a short clip, which they sometimes try to pass off as a new, previously unaired episode. More often than not, it is cut from trailers that have long been in the public domain. Intrigued victims are then asked to buy a low-cost subscription to continue watching. What follows is a classic scenario: Any payment details users enter go straight to the crooks, and the never-before-seen episode remains such.

No longer your account

Cybercriminals are interested in more than bank account details; account credentials for streaming services are also hot. Because hijacked accounts with paid subscriptions get put up for sale on the dark web, you could log in one day and discover someone else is already there.

After all, depending on your Netflix plan, you can stream on 1–4 devices simultaneously, and cybercriminals can sell your login credentials to any number of streamers. That means you might find yourself having to wait in line until some stranger decides to sign out.



This fake Netflix login page looks just like the real one

That may not be the end of it, either: Many people use the same password for different accounts, and databases of stolen passwords die hard. If their password is the same everywhere, the victim need only enter it on a phishing page once.

Buy a subscription for yourself, not cybercriminals

Cybercriminals scam movie and TV show lovers in different ways. Some of their ruses are quite easy to spot, others less so. By following simple digital security rules, you can protect your data not only in online movie theaters, but elsewhere as well.

- Do not click links in e-mails, even if a message seems to be from a real streaming (or other) service; always go to the official website by entering the address manually or through the app;
- Do not trust any person or site promising viewings of movies or shows before the official premiere;
- Pay attention to red flags that warn of phishing e-mails or fake websites;
- Stay alert and read more about scams and phishing schemes to learn how to sense which e-mails and websites are trustworthy, and which you should avoid;
- Use different passwords for all accounts that you value, and use a password manager to remember them for you;
- Use a reliable security solution that identifies malicious attachments and blocks phishing websites.