Online shopping, streaming phishing attacks multiply

Cybersecurity experts have seen a rapid growth of phishing attacks with websites that imitate online shopping and streaming platforms as lockdown continues...

Kaspersky experts have reported on the rapid growth of phishing attacks with websites that imitate online shopping and streaming platforms. Comparing the numbers for Q1 2019 and the same period this year, the share of users attacked by fake e-shops doubled, growing from 9 to 18%, of users, while the figure for streaming services tripled up to 4%.

While millions of people who would usually be out socialising or shopping in the evening and on weekends are staying home, streaming and e-markets are becoming more and more popular.

Unfortunately, cybercriminal follows trends too, setting traps for any popular activities online: they either create a copy of a web page that imitates a landing of popular retailers and streaming platforms or create new ones that offer users free access in return for their credentials or bank cards details.

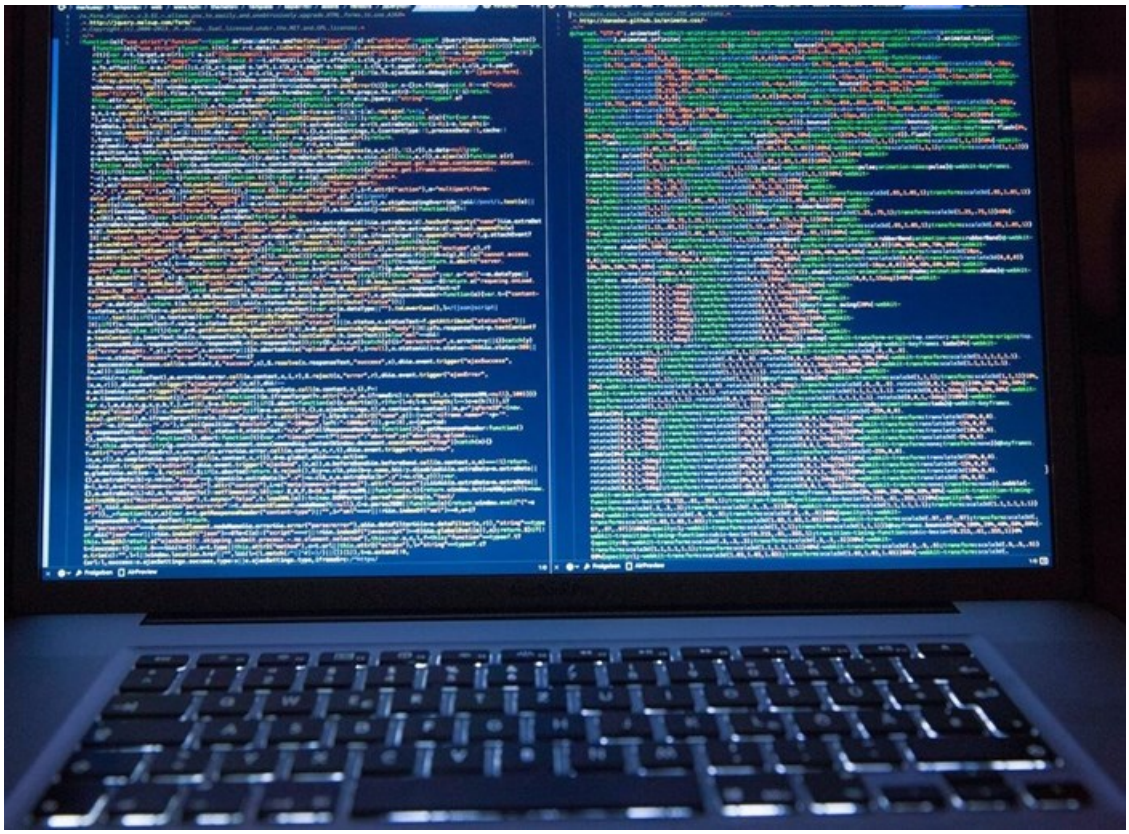

Photo by Markus Spiske from Pexels

"Not being able, or not wanting, to leave the house at the moment is bound to create a higher demand for online shopping and services as people seek to buy food, entertainment and other items online. This, coupled with boredom shopping, as well as desirable offers from retailers trying to stay afloat as the economy takes a hit, often creates a situation where cybercriminals are prowling," says Tatiana Sidorina, a security researcher at Kaspersky.

“In addition, this situation undoubtedly puts streaming services under huge strain. It may cause some slowdowns in service provision, which in turn will lead to people looking for alternative ways to access online content".

There are many ways to stumble upon a phishing website. Most often, the user is being redirected there from various websites, or scam emails. It is also possible to reach such websites from search engines despite significant efforts from their developers, scammers still manage to insert their fake pages thereby using "Black SEO" instruments.

These are the actions attackers take attempting to improve the site's position in search results using methods that are prohibited or not approved by search engines. Black optimisation includes various methods to deceive search robots that allow sites with content that is irrelevant to the user's request to get to the top of the search results. As an example of Black SEO can be placed on the page text that is not visible to the user, but indexed by the search engine.

"While streaming services and online shopping are a blessing in times of strict quarantine, providing us with essentials and entertainment, straying from the protected portals of our favourite legitimate streaming services for films, games and other content, will play into the hands of cybercriminals and may leave the public vulnerable to attack,” adds Sidorina.

“As tempting as it may be to find alternate sources of content, we ask users to be patient and stick to trusted streaming sources".

Be vigilant

Kaspersky is advising consumers to be extra vigilant at this time and remember these tips when watching movies, shopping online, and opening emails from online retailers:

- Stick to trusted sources, i.e. services for which you have a subscription, not random sources by double-checking the URL format or company name spelling before you download. Fake websites may look just like the real thing, but there will be anomalies to help you spot the difference.
- Use a credit card if possible for payments and try to avoid saving card details to the streaming site.
- Be wary of deals that seem too good to be true – they usually are.
- Type the URL into your browser to check the deal on the website, rather than click on links in emails.
- Use a unique, complex password for each of your online accounts.
- Use a reliable security solution that delivers advanced protection on Mac, as well as on PC and mobile devices.