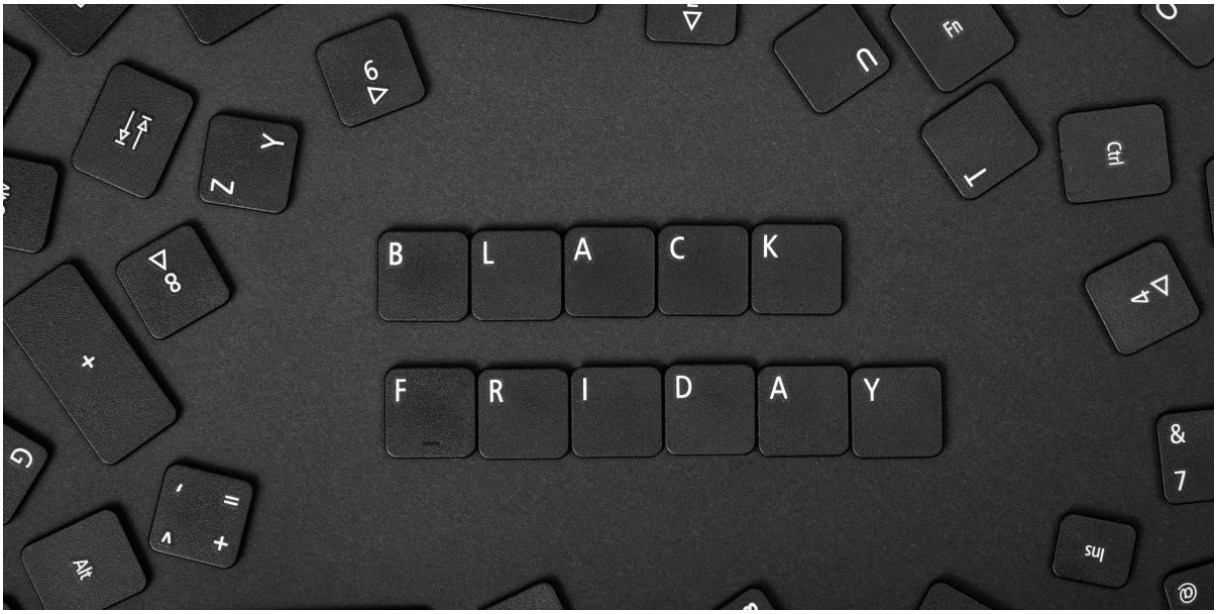
SECURELIST by Kaspersky

Black Friday 2021: How to Have a Scam-Free Shopping Day

PUBLICATIONS

22 NOV 2021



AUTHORS

Fact 1: cybercriminals love to exploit big holidays for personal gain. Case in point: we're already seeing scams targeting World Cup fans more than a year out from the event. Fact 2: the retail sector, particularly e-commerce, has always been popular with cybercriminals. In Q3 2021, online stores were in second place by share of recorded phishing attacks (20.63%). Taken together, both facts mean that Black Friday is a big day not only for shoppers, but for cybercriminals too.

It is important to be aware of the potential threats out there while shopping online. That's why we constantly monitor the landscape of shopping-related threats and release a report tracking the latest criminal activity targeting online shoppers. Here's what we found this year.

Methodology

In this research, we analyzed various types of threats: financial malware associated with major online shopping platforms as well as phishing pages and fake websites mimicking the world's biggest retail platforms.

The data came from Kaspersky Security Network (KSN), a system for processing anonymized cyberthreat-related data shared voluntarily by Kaspersky users. We analyzed the detections related to various online shopping platforms between January and September 2021; and the period from January to October 2021 for financial phishing.

Furthermore, we analyzed financial malware associated with major e-commerce platforms detected during the period from January 2020 to November 2021.

In this report, we analyze data related to the world's five most visited retail platforms: Walmart, eBay, Amazon, Alibaba and Mercado Libre.

Key findings:

- During the first 10 months of 2021, Kaspersky products detected 40 584 415 phishing attacks targeting e-commerce and e-shopping platforms, as well as banking institutions.
- The total number of financial phishing attempts targeting e-payment systems more than doubled from September 2021 (627,560) to October 2021 (1,935,905), showing a 208% increase.
- Amazon was consistently the most popular lure used by cybercriminals to launch phishing attacks. The second most popular was, for most of 2021, eBay, followed by Alibaba and Mercado Libre.
- The number of financial malware infection attempts dropped by half from 20.5 million in 2020 to 10 million in 2021.
- In 2021, 11 malware families were actively targeting online shoppers. More than 50% of malicious activity this year belongs to Zbot.
- From January 2020 through October 2021, the most targeted e-commerce platforms were in e-shopping (eBay, Alibaba, etc.) and entertainment (eg. streaming services, online games) with 30.61% of attacks.

Phishing Threats by the Numbers

Our researchers also took a closer look at financial phishing, which is typically separated into three categories. The first is phishing mimicking e-shops, such as analyzed retail platforms or any online stores; the second type involves banking phishing (i.e. fake banking websites) and the third involves pages mimicking well-known e-payment systems, such as PayPal, Visa, MasterCard and American Express.

Number of financial phishing attempts for banking, e-payment and e-shopping platforms in 2021 (download)

Overall, for the first 10 months of 2021, Kaspersky products detected 40 584 415 attacks targeting e-commerce and e-shopping platforms, as well as banking institutions.

2020 was the year everything went online, meaning in-person shopping wasn't an option. In 2021, the world economy began to open back up and stores quickly rebounded. For example, during the first 10 months of 2021, in-person visits to offline stores, restaurants and entertainment locations increased by 44% in the U.S. This aligns with the fact that, in 2021, Kaspersky researchers didn't observe the typical seasonal trends of a summer decline in online shopping-related phishing and an autumn rise. Instead, the number of financial phishing attempts continued to decline. Of course, in many cases, lockdowns didn't end until the spring and summer months, which could suggest that people were eager to get back to shopping in-person.

However, there is one notable exception. In 2021, the total number of financial phishing attempts targeting e-payment systems more than doubled from September (627,560) to October (1,935,905) — a 208% increase. Right now, e-payment is experiencing tremendous growth with an expected global valuation of 6.6 trillion dollars in 2021; this represents a 40% increase in just two years. Not surprising, then, that scammers would attempt to profit from this trend, especially as people prepare for holiday shopping.

What platforms are most popular as phishing bait when it comes to online shopping? To find out, our researchers examined the total number of phishing attacks using Amazon, Alibaba, eBay, Walmart or Mercado Libre as a lure for the first nine months of 2021.

Number of phishing attempts using shopping platforms as a lure in 2021 (download)

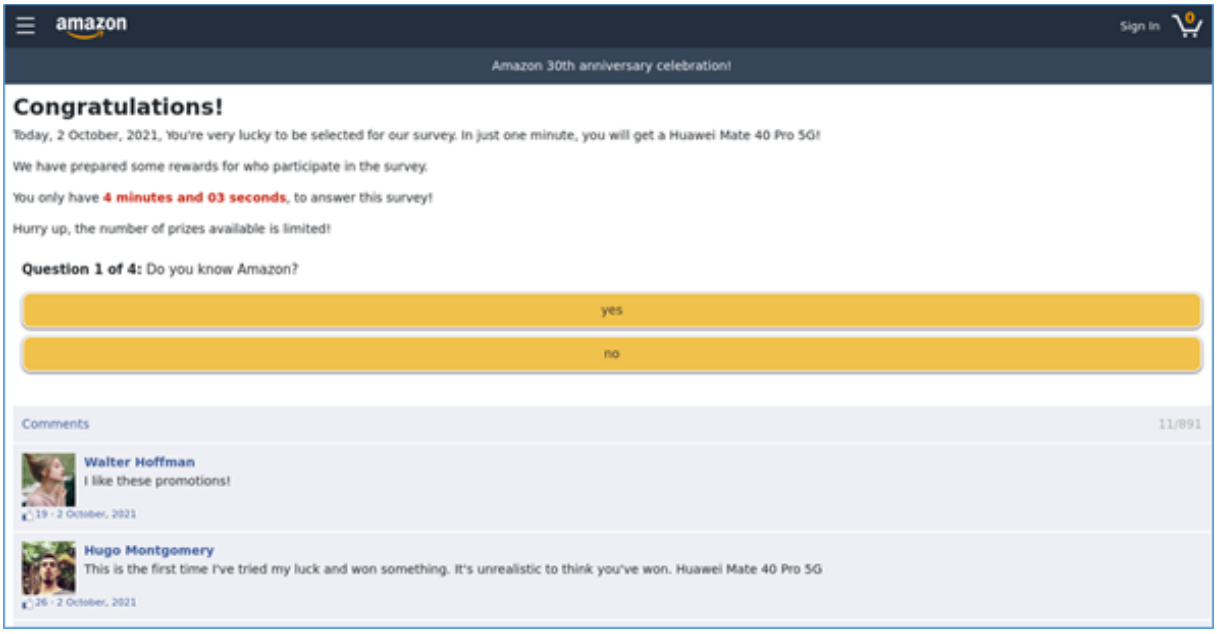
Amazon was consistently the most popular lure, with phishing attempts using its name peaking in January at 289,828. January is typically a very popular shopping month as the sales period starts in many countries and people spend the money they received over the holidays. The second most popular lure was, for most of 2021, eBay, followed by Alibaba and Mercado Libre. For both Mercado Libre and eBay, the greatest number of phishing attempts using these platforms as a lure was recorded in January as well. However, there was also an overall seasonal trend observed: the total number of phishing attacks exploiting the names of these five platforms were on the decline in the summer but began an upward trend in the fall as the shopping season began to kick into high gear. In fact, the number of attempts to lure users with the name Alibaba nearly doubled from August to September — from 24,051 to 45,496.

Phishing for data

Phishing is one of the oldest tricks in the book, precisely because it's easy and often successful — particularly when users are in a rush to benefit from a deal that sounds too good to be true. As the fall shopping season approaches, as well as Black Friday, cybercriminals have been looking to fake websites to phish for users' credentials — from Alibaba to Amazon. The good news is they've been using well-known schemes, meaning users can stay safe if they're aware of the most frequently used tricks.

One of the most common scams is to create a fake website offering great deals for popular shopping portals. Kaspersky researchers uncovered such phishing pages for

Walmart, eBay, Amazon, Alibaba and Mercado Libre in various languages. In the example below, the user can supposedly earn a special prize for completing a four-question survey. In fact, users end up giving away their personal data for free. That's because these surveys often have a long registration form that requires users to fill in their identifying information and, sometimes, bank card details. They're often asked to then send the link to several friends — so that the scammers can reach more potential victims.

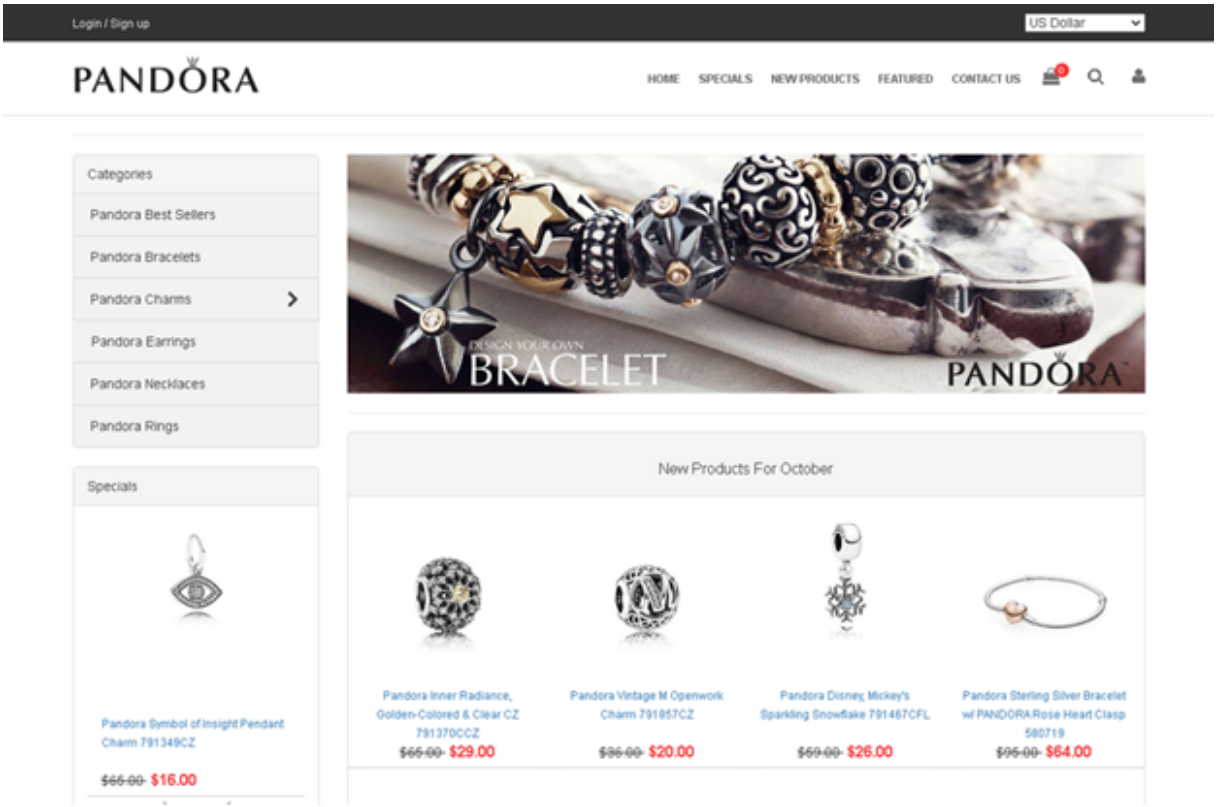


Phishing scam urging users to fill out a quick survey for a fake promotion

Other times, scammers create fake login pages. If users attempt to sign into their account, the scammers gain their login information, giving access not only to the victims' accounts, but to all financial information stored there. These pages might look almost identical to the real platforms' login pages, with only the misspelled URL giving away the fake.

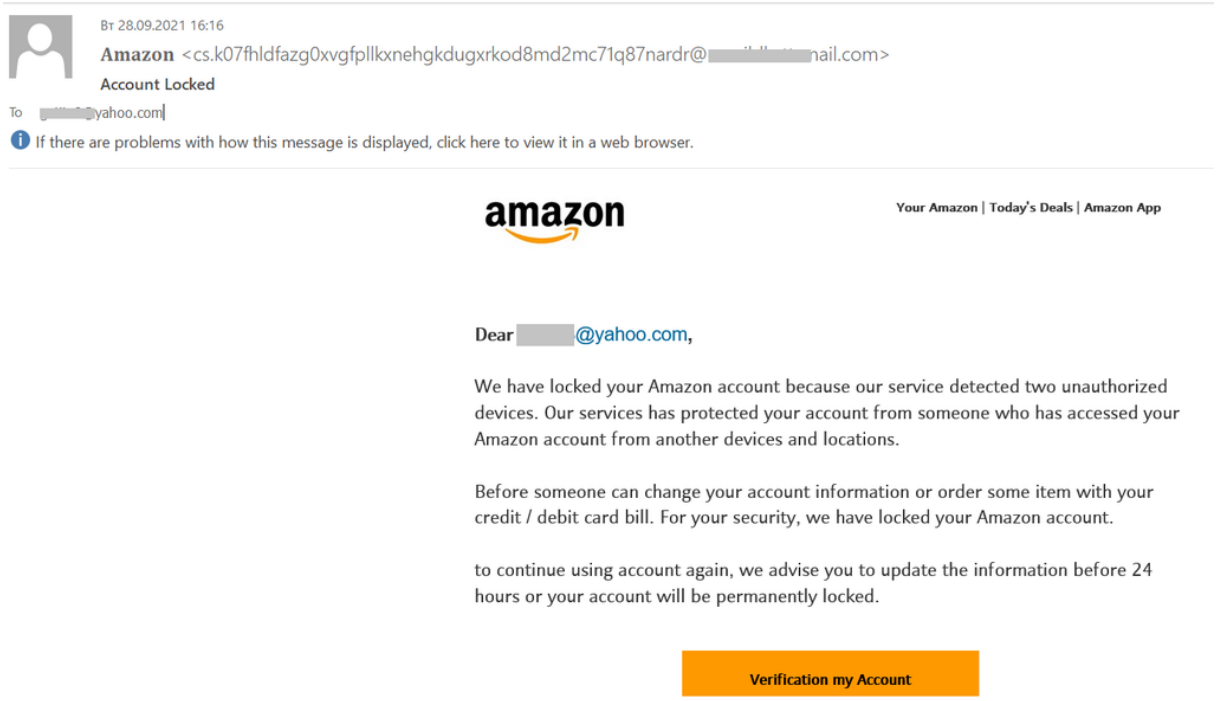
eBay phishing page in German

Scammers don't just focus on shopping platforms — they also target potential customers of popular offline stores, faking their online shopping pages.



The example above shows a phishing page for the popular jeweler Pandora that appears to offer great deals on popular items. Users are offered to buy jewelry at a cheaper price — needless to say, they never receive the order or get a cheap fake pair of earrings.

There is a variety of ways users can encounter these phishing pages. One of the most common is through phishing e-mails.



The example above shows an e-mail sent to a user warning that their account has been locked after a third party tried to access it. The sender gives the user only 24 hours to follow the link in the email and verify their information, or the account will be permanently locked. Of course, if the user clicks on the link, they would most likely be directed to a phishing page that would ask for identifying information and/or a malicious page that downloads malware. E-mails like this often feed on emotions — either scaring users (such as in the example above) or promising them an amazing deal that ends soon.

There also has been a rise in the number of spam letters detected by Kaspersky products. An active spread of spam emails with 221 745 emails containing the words 'Black Friday' was spotted during the month amid the sales season, from October 27 to November 19.

Banking Trojans and e-commerce platforms

Cybercriminals do not limit their malicious activity to spreading shopping-related phishing scams. Banking Trojans are traditional tools for stealing access credentials to online banking or payment system accounts. Some banking Trojan families have evolved and developed their functionality, launching new variants and extending their range. Today, most of them are able to perform transactions, download other malware and more. And some of them target not only people using online banking, but online customers of certain stores.

After two years of rather stable indicators in the number of attacks in 2019 and 2020, we observe a rapid decrease in 2021. In fact, the number of Banking Trojan infection attempts dropped by half from 20.5 million in 2020 to 10 million in 2021.

Overall number of attacks by banking Trojans, 2019-2021 (download)

In 2021, we found 11 families of financial malware targeting not only online banking users, but also online store users worldwide. More than 50% of malicious activity this year belongs to the Zbot family, which aims to steal users' credentials for online stores and retail platforms. The other Top 5 most active financial malware families are: Qbot (13.9%), Anubis (13.4%), Trickbot (11.6%) and Neurevt (4.8%).

As mentioned above, the five banking Trojan families we focus on target e-commerce brands so as to track down users' credentials, namely, login details, passwords, bank card numbers or phone numbers.

Once the victim opens one of the targeted e-commerce websites, the Trojan activates its form-grabbing functionality and saves all the data the user inputs on the website. On an e-commerce website, this often includes login banking details, card number, expiration date and CVV.

From January 2020 through October 2021, the most targeted e-commerce platforms were in e-shopping (eBay, Alibaba, etc.) and entertainment (e.g. streaming services, online games) with 30.61% of attacks. We can assume that fraudsters exploited the increased demand for in-home entertainment and shopping for their own malicious purposes.

The second most targeted category is telecom with 20.4% of targeted platforms.

Proportion of e-commerce categories targeted by malware, January 2020 through November 2021 (download)

Those five banking Trojan families did not target a particular region. Instead, they distributed their malicious activity all over the globe, mostly targeting victims in Russia, China, Italy and Brazil.

Geography of countries and territories affected by banking Trojans, Jan 2021 – Oct 2021 (download)

Conclusion

Most shoppers love great deals — and so, too, do cybercriminals. That's not going to change, which means scammers will continue trying to profit off online shoppers. And they'll continue trying to exploit popular shopping periods. Fortunately, over the past year, scammers have stuck to traditional tools and scams — from phishing pages offering big savings and rewards to tried-and-tested banking Trojans. This means users know what to be on the lookout for. However, as new e-commerce platforms arise, which most likely will become popular and easy targets, it's important to stay vigilant.

To enjoy the best Black Friday has to offer this year, be sure to follow a few safety recommendations.

- Use a reliable security solution, such as Kaspersky Security Cloud, that identifies malicious attachments and blocks phishing sites — on both your computer and mobile device.
- Do not open attachments or click on links in emails from banks, e-payment apps or shopping portals, particularly if the sender insists. It is better to go to the official website directly and log in to your account from there.
- Double-check the format of the URL or the spelling of the company name, as well as read reviews and check the domain's registration data before filling out any information.
- Be wary of any deals that seem too good to be true. They typically are.
- In order to protect your data and finance, it is safe practice to make sure the online checkout and payment page is secure. You'll know it is if the web page's URL begins with HTTPS instead of the usual HTTP; a padlock icon typically appears beside the URL, and the address bar in some browsers is green. If you don't see this, do not proceed.
- Make sure all of your software is up to date — update your operating system and software applications (attackers exploit loopholes in widely used programs to gain entry).
- Make sure you're on a secure network — logging on to the public Wi-Fi at the local coffee shop makes it far easier for attackers to access your online activity. It's also better and safer to do online shopping on your own computer or device to avoid the possible risks of using someone else's.
- Despite taking as many precautions as possible, you probably won't know something is amiss until you see your bank or credit card statement. So, if you're still getting paper statements, don't wait until they hit your mailbox. Log online to see if all of the charges look legitimate – if not, contact your bank or credit card immediately to fix the situation.