SafetyDetectives AU$

BEST ANTIVIRUS | BEST PASSWORD MANAGERS | BEST VPN | TOOLS | DEALS & COUPONS | BLOG | NEWS

Home / Blog / Amazon Fake Reviews Scam Exposed in Data Breach

Amazon Fake Reviews Scam Exposed in Data Breach

SafetyDetectives Cybersecurity Team

The SafetyDetectives cybersecurity team uncovered an open ElasticSearch database exposing an organized fake reviews scam affecting Amazon.

The server contained a treasure trove of direct messages between Amazon vendors and customers willing to provide fake reviews in exchange for free products. In total, 13,124,962 of these records (or 7 GB of data) have been exposed in the breach, potentially implicating more than 200,000 people in unethical activities.

While it is unclear who owns the database, the breach demonstrates the inner workings of a prevalent issue affecting the online retail industry.

How the Process Works

The information found on the open ElasticSearch server outlines a common procedure by which Amazon vendors procure ‘fake reviews’ for their products.

These Amazon vendors send to reviewers a list of items/products for which they would like a 5-star review. The people providing the ‘fake reviews’ will then buy the products,

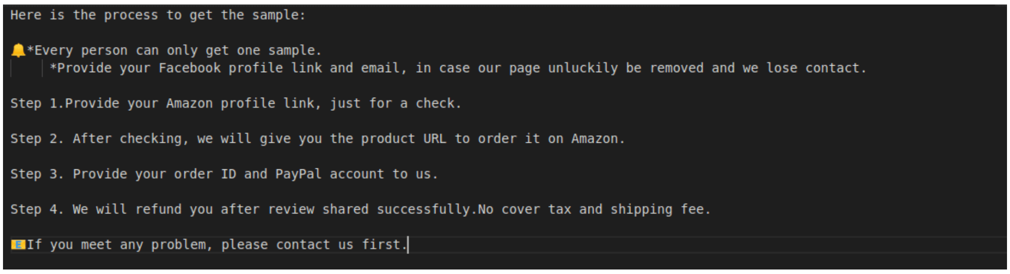
This article contains

leaving a 5-star review on Amazon a few days after receiving their merchandise.

Upon completion, the provider of the fake review will send a message to the vendor containing a link to their Amazon profile, along with their PayPal details.

Once the Amazon vendor confirms all reviews have been completed, the reviewer will receive a refund through PayPal, keeping the items they bought for free as a form of payment.

The refund for any purchased goods is actioned through PayPal and not directly through Amazon's platform. This makes the five-star review look legitimate, so as not to arouse suspicion from Amazon moderators.



```
Here is the process to get the sample:

🔔*Every person can only get one sample.
    *Provide your Facebook profile link and email, in case our page unluckily be removed and we lose contact.

Step 1.Provide your Amazon profile link, just for a check.

Step 2. After checking, we will give you the product URL to order it on Amazon.

Step 3. Provide your order ID and PayPal account to us.

Step 4. We will refund you after review shared successfully.No cover tax and shipping fee.

📧If you meet any problem, please contact us first.
```

Amazon vendors paying for reviews

In some cases, there may be an additional payment – based on the scale of the services provided by the person posting fake reviews. However, we didn't find any examples of this in the exposed server.

What was Leaked?

More than 13 million records, equating to 7 GB of data, were exposed when the unclaimed ElasticSearch server was left open without any password protection or encryption. The personal data of people providing fake reviews, as well as Amazon vendors, could be found in leaked messages on the database.

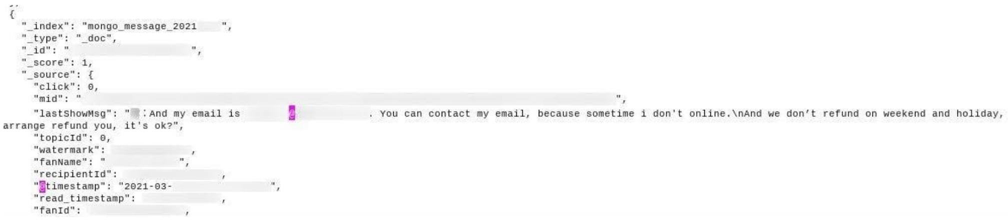
- How the Process Works
- **What was Leaked?**
- Avoiding Detection
- Posing as a Genuine Service
- Impacts
- How to Spot Online Fake Reviews
- Preventing Data Exposure
- About us

1. Data related to the vendors

These messages contained various examples of **contact details from the vendors:**

- Email addresses
- WhatsApp and Telegram phone numbers

Contact details were given to the potential fake review providers to continue communications outside of the services where these leaked interactions had taken place.



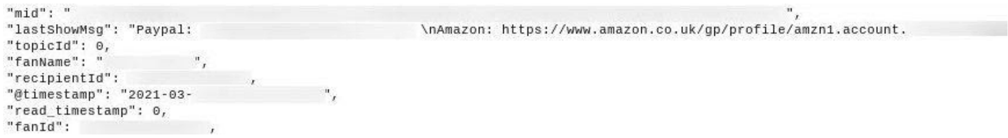
```
{
  "_index": "mongo_message_2021[redacted]",
  "_type": "_doc",
  "_id": "[redacted]",
  "_score": 1,
  "_source": {
    "click": 0,
    "mid": "[redacted]",
    "lastShowMsg": "[redacted]:And my email is [redacted]@[redacted]. You can contact my email, because sometime i don't online.\nAnd we don’t refund on weekend and holiday,
arrange refund you, it's ok?",
    "topicId": 0,
    "watermark": [redacted],
    "fanName": "[redacted]",
    "recipientId": [redacted],
    "@timestamp": "2021-03-[redacted]",
    "read_timestamp": [redacted],
    "fanId": [redacted],
```

Contact details of vendors, such as email addresses

2. Data related to the reviewers

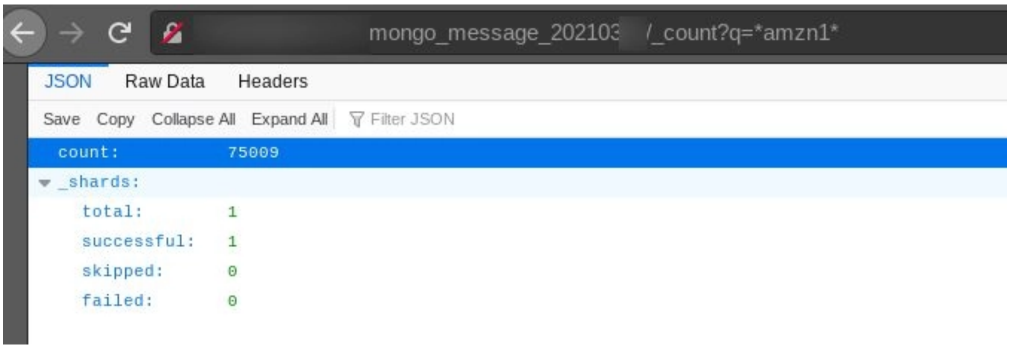
Messages on the ElasticSearch server also contained other forms of **directly and indirectly identifiable personal data** exposing the reviewers themselves, such as:

- 75K links to Amazon accounts/profiles of review sellers
- PayPal account details (email addresses)
- Email addresses
- ‘Fan names’ – supposedly usernames, often containing names & surnames



```
"mid": "[redacted]",
"lastShowMsg": "Paypal: [redacted] \nAmazon: https://www.amazon.co.uk/gp/profile/amzn1.account.[redacted]
"topicId": 0,
"fanName": "[redacted]",
"recipientId": [redacted],
"@timestamp": "2021-03-[redacted]",
"read_timestamp": 0,
"fanId": [redacted],
```

Links to Amazon accounts

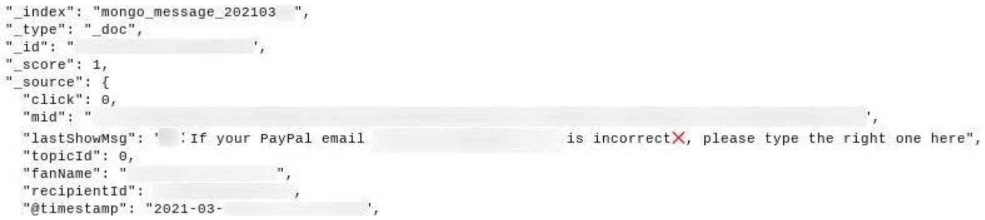


```
count:        75009
▼ _shards:
    total:        1
    successful:   1
    skipped:      0
    failed:       0
```

Count of records containing Amazon profile link

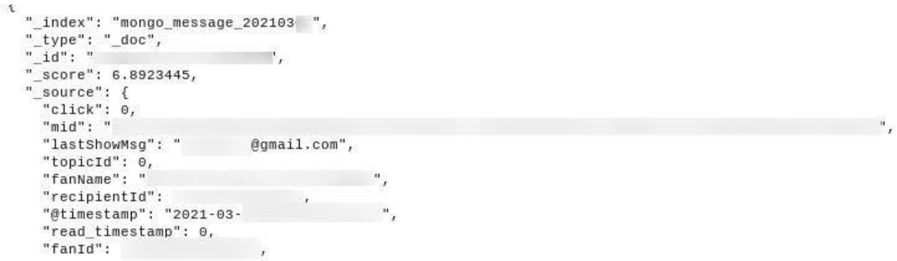
Leaked PayPal account details and ‘fan names’ outline email addresses and what seems to be the usernames of people providing fake reviews. These details could be used to indirectly identify individuals, while many of them contained full names and surnames.

The Gmail addresses of reviewers were also provided to vendors directly via message. In total, 232,664 Gmail addresses have been exposed on the server, though some of the email addresses were duplicates.



```
"_index": "mongo_message_202103[redacted]",
"_type": "_doc",
"_id": "[redacted]",
"_score": 1,
"_source": {
  "click": 0,
  "mid": "[redacted]",
  "lastShowMsg": '[redacted]:If your PayPal email [redacted] is incorrect❌, please type the right one here",
  "topicId": 0,
  "fanName": "[redacted]",
  "recipientId": [redacted],
  "@timestamp": "2021-03-[redacted]",
```

PayPal emails of fake reviewers



```
{
  "_index": "mongo_message_202103[redacted]",
  "_type": "_doc",
  "_id": "[redacted]",
  "_score": 6.8923445,
  "_source": {
    "click": 0,
    "mid": "[redacted]",
    "lastShowMsg": "[redacted]@gmail.com",
    "topicId": 0,
    "fanName": "[redacted]",
    "recipientId": [redacted],
    "@timestamp": "2021-03-[redacted]",
    "read_timestamp": 0,
    "fanId": [redacted],
```

Emails and ‘fan names’ are included in messages

The ‘Gmail’ figure covers only those individuals who use Google as their mail provider. When we factor in the presence of other types of email accounts, such as Outlook, the enormity of this breach becomes apparent. 75,000 Amazon accounts were leaked as well, although there are potentially several duplicates included in this figure. Along with Amazon vendors compromised through their contact details, it's reasonable to estimate that around 200,000-250,000 people were affected by this breach.

The server appeared to be located in China, and it is thought the leak affected citizens from Europe and the USA (at a minimum). In reality, the leak could have affected individuals from all corners of the world.

Number of records leaked	+13M
Number of affected users	Estimated 200-250K
Size of breach	7 GB
Server location	China
Company location	Potentially China*

**Records that were unrelated to messages between vendors and reviewers were written in Chinese, which is why we assume the owners of the server were located in China.*

The SafetyDetectives cybersecurity team discovered the breach on March 1st, 2021. We monitored the status of the open ElasticSearch server over the following days, and on March 6th, 2021, the unclaimed database was secured.

We were unable to identify the owner of the ElasticSearch server. As a result, we could not notify the company in question regarding this security issue. Nonetheless, the server was secured a few days later, making it inaccessible to outside parties.

Given the extent of the records and vendors included in the database, it's possible that the server is not owned by the Amazon vendors running the scam. The server could be owned by a third party that reaches out to potential reviewers on behalf of the vendors. Third-parties might post a picture of the product in a Facebook or WeChat group, asking for reviews in return for free products.

The server could also be owned by a large company with several subsidiaries, which would explain the presence of multiple vendors.

What's clear is that whoever owns the server could be subject to punishments from consumer protection laws, and whoever is paying for these fake reviews may face sanctions for breaking Amazon's terms of service.

Avoiding Detection

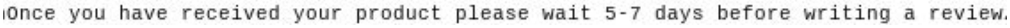
Amazon vendors running this type of 'fake review scam' are able to avoid detection from Amazon's review moderation team.

Implicated vendors can avoid detection across multiple platforms, too. This is a big reason why online marketplaces are struggling to contain the issue of 'fake reviews', which is now widespread across the entire industry.

Messages in the unclaimed ElasticSearch server highlighted techniques that are employed by businesses to cover their tracks.

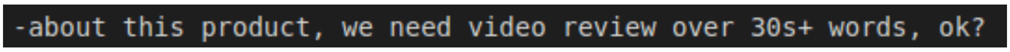
Fraudulent businesses give reviewers specific criteria to follow to avoid detection on Amazon. These criteria are designed to present the reviews as legitimate. In this ElasticSearch server, vendors asked reviewers to wait a few days before publishing a review. They also request substantial reviews that are longer than just a few words, and they may even outline certain details that should be included in the review.

Instructions were sent to reviewers to make the reviews more credible.



```
Once you have received your product please wait 5-7 days before writing a review.
```

Instructions were sent to reviewers to make the reviews more credible

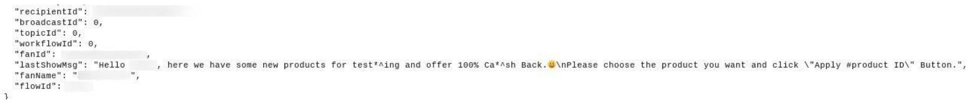


```
-about this product, we need video review over 30s+ words, ok?
```

Some vendors requested reviews over a specific word count

Vendors often conduct their communications through direct messaging apps. In the ElasticSearch server we discovered, vendors attempted to hide keywords with similar phrases that bypass keyword searches.

This could imply that the platforms used to liaise with potential reviewers were not intended for this purpose, and vendors are likely attempting to evade detection from security technicians.



```
    "recipientId": [redacted]
    "broadcastId": 0,
    "topicId": 0,
    "workflowId": 0,
    "fanId": [redacted],
    "lastShowMsg": "Hello [redacted], here we have some new products for test*^ing and offer 100% Ca*^sh Back.😃\nPlease choose the product you want and click \"Apply #product ID\" Button.",
    "fanName": "[redacted]",
    "flowId": [redacted]
  }
```

Amazon vendors are disguising keywords to evade detection

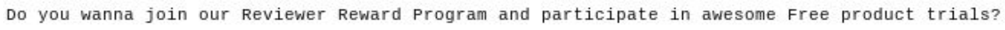
We're confident some of these interactions were taking place on Facebook, though it seems communications with potential reviewers occurred across several messaging platforms.

The owners of the database may have used a CRM system to aggregate these different channels of communication onto one easy platform, storing the data on the unclaimed ElasticSearch server. However, this is merely an educated assumption.

Posing as a Genuine Service

Although a lot of people providing fake reviews likely know what they’re doing, we must also highlight how vendors don’t advertise that fake reviews are illegal.

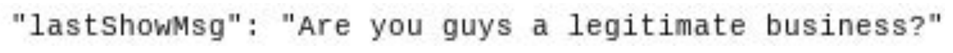
Unassuming people may have been targeted by Amazon vendors with the offer of free products in return for a review. Vendors use ‘professional’ language to present the offer as legitimate trade, utilizing phrases like ‘testing’ and ‘free product trials’ when they message prospective reviewers. This is certainly the case in the database we detected.



```
Do you wanna join our Reviewer Reward Program and participate in awesome Free product trials?
```

‘Official’ language presents the vendor as a legitimate business

Without knowledge of marketing law, Amazon terms of service, or the wider impact fake reviews can have, some individuals may think nothing of collaborating with an Amazon vendor to conduct a fake review.



```
"lastShowMsg": "Are you guys a legitimate business?"
```

One potential reviewer seems unaware of the consequences

When considering those who are implicated in this breach, and the impacts they could face because of this exposure, we should be mindful that some of these reviewers have been misled themselves.

Impacts

The owners of the ElasticSearch server have essentially committed two separate offenses. On one hand, companies and individuals have been connected with the production of misleading marketing materials. On the other hand, a data breach in itself has further damages for the persons/business(es) involved.

Punishments for Fake Reviews

So, what are the wider implications for people giving fake reviews, and the Amazon vendors that pay for these fake reviews?

We can split these impacts into two different types: **Corporate punishments** and **individual punishments.**

Corporate Punishments

Businesses or individual vendors that are found to be buying fake reviews for their products could face various penalties and sanctions for this type of transgression.

Firstly, Amazon vendors have broken Amazon's terms of service through buying fake reviews.

Amazon can place a number of sanctions on guilty parties. Vendor accounts can be terminated permanently, and vendors can lose their selling privileges with an immediate effect. Amazon will withhold all earnings from pending transactions – where products have been sold, but earnings have not yet been collected by the vendor.

The reviews will be removed from any product page that is found to contain fake reviews, and that product will not be able to receive reviews or ratings in the future. Products can even be delisted from the site altogether.

Amazon retains the right to disclose the vendor's name (and any other related information) publicly. An exercise that highlights the fraudulent company's wrongdoings to warn those who may have been affected, while causing reputational damage to the business in question.

Amazon’s terms of service outline that Amazon may choose to pursue legal action against the business involved.

In several countries, paying people to conduct fake reviews is an illegal practice that damages the rights of consumers. If a company purchasing fake reviews is based in the United States, it would face lawful action from the Federal Trade Commission (FTC). Using deceptive marketing tactics could land a US-based vendor with a heavy penalty of more than $10 million.

Individual Punishments

The breach also means people exposed as ‘fake review sellers’ may be subject to lawful punishment themselves. Whether individuals are found to be guilty of selling reviews or not would make a huge difference to the consequences they could face. If reviewers are found to have been ‘misled’, punishments could be vastly reduced and the individuals may only receive a ‘slap on the wrist’.

Fraudulent reviewers with thousands of fake reviews to their name can pay penalties of more than $10,000, and they could even receive a jail sentence. The severity of these punishments would depend on whichever jurisdiction is in control of the investigation.

The Amazon accounts of fake reviewers will likely be terminated as well, though Amazon’s primary focus is on pursuing guilty vendors rather than investigating each individual reviewer.

Data Breach Impact

The reputational and financial damage provoked by a data breach of this nature is tangible. On top of the above penalties and charges, if the ElasticSearch database owner was to be identified, they could face further sanctions for breaking data protection laws.

All of the jurisdictions involved in such cases are unclear until we know the citizenship of individuals who have had their data leaked. The fraudulent owner of the server seems to be based in China. A serious breach of data protection laws there could land the owner with fines up to $7.6 million (or 5% of the company's turnover from the previous year).

If individuals from other nations are affected, other jurisdictions could also carry out investigations. Any damages to American citizens could involve the FTC, which can fine businesses up to $100 million, while European citizens are protected by **GDPR.** If the data of European citizens is mishandled, a fine of around €20 million (or 4% of a companies income) could be charged to the owner of the database.

The data breach, along with any additional crimes, will perceivably cause reputational damage to businesses tied to such an event. Future customers may choose to avoid businesses involved in lawsuits, unlawful activities, or poor data protection practices.

The personal information of hundreds of thousands of people can be found on the database, and this puts those individuals in harm's way of hackers and cybercriminals.

It is currently unknown whether hackers accessed the open ElasticSearch server. If hackers have accessed the server, then the emails, names, and surnames of affected reviewers and vendors could be used to target people with scams, phishing attacks, fraud, and even blackmail.

With something as simple as an email address, a hacker could launch a phishing attack. Here they would send a targeted email, using personal data to speak directly to the victim and build an element of trust. The email will attempt to convince a victim to click on a link, either leading to a fake website or downloading malicious files onto that person's computer. These malicious files provide the basis for hackers to conduct further criminal activities, such as fraud and/or identity theft.

Hackers can attempt scams through targeted emails, too, by convincing parties to buy a product or send over details that would facilitate fraudulent attacks. Hackers could build trust by referring to the products reviewers have tested, or they could use PayPal as the focus of their attack.

Hackers could pose as a representative of PayPal, requesting that users 'update their password'. Once users have passed on their PayPal password to the hacker, the hacker will gain access to that person's PayPal account – draining it of funds.

Hackers can pepper leaked PayPal accounts with generated passwords until they gain access. Once into a PayPal account, there's additional personal information that hackers can use to build trust and focus their attacks. For example, transaction history could be used to pose as a representative of another business.

The server contained incriminating information for thousands of people and businesses, information that those parties may not wish to be available to regulatory or investigative authorities. The obvious risk associated with incriminating data means hackers could target victims with blackmail. Once hackers have obtained the data, they could demand huge amounts of money or information from individuals and vendors, with the threat of releasing the incriminating files should the victim fail to comply.

How to Spot Online Fake Reviews

Online 'fake reviews' mislead customers and coerce buyers into purchasing decisions that they otherwise might not make. Fake reviews deny potential buyers a fair and honest assessment of products at the benefit of the vendor involved. Buyers may ultimately be underwhelmed with the product, or feel deceived by the reviews they have read.

Not only do these incidents violate the terms of service on thousands of online marketplaces, but they also break the law in several countries as a violation of 'consumer protection'.

Fake reviewers sell their services to corporations, either in return for free products or in the form of 'packages' where vendors can buy misleading reviews in bulk. These bundles can contain up to 1000 reviews for a price of around $11,000.

Big online marketplaces are failing to contain the issue, and in doing so are failing to ensure the safety of their customers. Sites like Amazon face a struggle to contain a problem that is now widespread, and more must be done to bring down a thriving economy of deception.

The scale and impact of the issue means we should all do what we can to identify fake reviews when we use online marketplaces, like Amazon. Spotting and reporting suspected fake reviews helps protect ourselves and other consumers.

Reporting such incidents could provide crucial support to marketplaces trying to contain the problem. Here's how you can spot an online fake review:

- **Be skeptical of extreme reviews.** The 'perfect' product rarely exists. If a product has a ton of overbearingly positive reviews (especially when compared to similar products), you should question the legitimacy of those reviews. You should also look out for reviews that are 100% positive or 100% negative.

- **Look for suspicious language.** Fake reviews often use less emotional language, and they can be hard to read. A fake review may even read like an advert, badmouthing the product's competitors in the process.
- **Look for generic statements about the product.** Several of the five-star reviews may highlight the same plus points, or the reviews could generally lack variance – not revealing anything about each individual's specific experience. Fake reviews might contain lots of generic keywords, too, or reference the brand's name multiple times.
- **Fake reviews can be shorter.** If a review is just a few words long, the reviewer might be trying to affect the product's star rating as quickly as possible.
- **Be extra-vigilant when buying from unknown brands.** Early start-ups often try to elevate their status with fake reviews. Check for reviews of their products on other sites before buying, and make sure they have legitimate contact details should anything go wrong.
- **Check for irrelevant information.** 'Review merging' is commonplace for guilty vendors, who republish reviews from other products onto their own. Fake reviews could contain other examples of false information, too. Make sure any feedback makes sense for the product it's supposedly reviewing.
- **Cross-examine five-star reviews with bad ones.** Bad reviews might consistently highlight issues that fake five-star reviews don't acknowledge. Fake reviews may even say this characteristic of the product is a positive.
- **Check the reviewer's account.** If they have left positive reviews on loads of the same vendor's products, they could

be fake, and the same can be said if they are leaving negative reviews. If their account lacks personal information and their buying habits are random, that's another sign of a fake reviewer.

- **Check for patterns.** A negative review could be followed by a cluster of fake five-star reviews. Also, a number of the reviews might sound similar, or a fake reviewer might post similar reviews on multiple products.
- **Check the dates of reviews.** If a product's five-star reviews have been posted before the product was listed, or over a short time-span, they could well be fake.
- **Use software.** There are loads of good online tools that will analyze a product's reviews and tell you if they seem fake. Use them!

You can report a fake review whenever you have your suspicions. Most online marketplaces have a symbol of a flag or an exclamation mark next to each comment. On Amazon, there is a 'report' button. Clicking this will take you through the referral process.

Preventing Data Exposure

If you're worried about your data, there are a few immediate steps you should take to mitigate your risk of exposure and minimize the impact of cybercrime:

- Only give your data to companies/individuals you know or can completely trust.
- Make sure the website you're on is secure. Secure website domains have a 'https' and/or a closed lock symbol at the beginning.
- Do not give out information that can easily be used against you (government ID numbers and personal preferences

should be kept to yourself).

- Use letters, numbers, and symbols to create rock-solid passwords.
- Don’t click links in emails (or anywhere online) that you cannot be sure are from a reputable source.
- Make sure your privacy settings on social media sites only show your content and personal information to trusted people.
- Avoid using credit cards or typing out passwords on unsecured Wi-Fi networks.
- Educate yourself on data protection, cybercrime, and the different ways you can avoid phishing attacks and ransomware.

About us

SafetyDetectives.com is the world’s largest cybersecurity review website.

The SafetyDetectives research lab is a pro bono service that aims to help the online community defend itself against cyber threats while educating organizations on how to protect their users’ data. The overarching purpose of our web mapping project is to help make the internet a safer place for all users.

Our previous reports have brought multiple high-profile vulnerabilities and data leaks to light, including the 200+ million users exposed by Chinese social media management company Socialarks as well as a breach at major cosmetics brand Avon that leaked more than 7 GB of data.

For a full review of SafetyDetectives cybersecurity reporting over the past 3 years, follow SafetyDetectives Cybersecurity Team.

Published on: May 6, 2021

Share It:

About the Author

SAFETYDETECTIVES CYBERSECURITY TEAM
SafetyDetectives Cybersecurity Team

The SafetyDetectives research lab is a pro bono service that aims to help the online community defend itself against cyber threats while educating organizations on how to protect their users' data. The overarching purpose of our web mapping project is to help make the internet a safer place for all users

978 745

Was this article helpful? ★★★★★ 9.5 (248 votes)

SafetyDetectives

Our mission - to give our readers accurate and valuable information so they can make informed decisions about staying safe, secure

CATEGORIES

- Safety Blog
- Best Antivirus Software
- Best Password Managers
- Best VPN Services
- Antiviruses Coupons

REVIEWS

- Bitdefender Reviews
- Norton Reviews
- 1Password Reviews
- Dashlane Reviews
- ExpressVPN Reviews

LEGAL

- Why Trust Us?
- Terms of Service
- FAQ
- Disclosure
- Privacy Policy
- Human Sitemap

and protected on the internet

Antivirus Comparison

Private Internet Access Reviews