

How Facebook and its 'vampire apps' can still track you AFTER you remove your account: Here's how to stop them

Facebook uses an advertising strategy called the 'Audience Network' This lets brands target advertisements even when users move off the site Users can limit Facebook's ad tracking via their smartphone or web browser It has also emerged that thousands of plugin apps were siphoning user data Users have to delete each app manually to ensure their future data security
By Tim Collins For Mailonline and Annie Palmer For Dailymail.com

3.5k

share

703

View comments

Facebook's latest scandal has caused many users to question whether they should pull the plug and delete their account in order to protect their private data.

But this may not be enough to keep Facebook, its advertisers, and so-called 'vampire apps', from tracking you across the web.

Facebook uses pieces of code - which include tags, pixels and cookies - to collect information and build up a profile of your digital self - even if you don't have an account.

It also allows thousands of third-party 'vampire apps' to plug in to its social network and siphon off data from its users.

In response, many are choosing to manually remove permissions previously granted to individual apps - a time consuming process.

However, it remains unclear whether this will allow them to claw back data already shared via third-parties.

This means third-party apps may still have enough data to build up a digital profile of you, even if you have stopped using them.

CEO Mark Zuckerberg has since admitted Facebook 'made mistakes' leading up to Cambridge Analytica privacy breach, which has led to accusations the firm mismanaged user data.

Scroll down for video

Facebook's latest scandal has caused many users to question whether they should pull the plug and delete their account in order to protect their private data. (stock)

Facebook's latest scandal has caused many users to question whether they should pull the plug and delete their account in order to protect their private data. (stock)



+13

Facebook Audience Network

Facebook uses an advertising strategy called the '**Facebook Audience Network**' to promote ads targeted to your browsing tastes.

It means brands can direct marketing messages to you based on your interests, even when you're not on the site, via other company's apps and mobile websites.

They can collect information ranging from your IP address to the websites you have visited, the length of time you spent on a website and in what sequence pages were accessed.

Facebook can use this information to track your activities across different websites, gaining insights into things like your location, age group, gender, and interests.

Facebook marketed its Audience Network as the 'power of Facebook ads, off Facebook' at the time of its launch in 2014.

The company is not alone in using targeted advertising and the many who do engage in it - including Google and Apple - say they do so to ensure that the commercial messages you are exposed to online are relevant to you.

**SHARE THIS
ARTICLE**

3.5k shares

RELATED ARTICLES



Prepare for more extreme weather: Storms like the 'Beast...



Outraged Facebook users react with fury after finding out...



Underwater 'fountain' of magma is found beneath Yellowstone...



Self-driving Land Rover cars are tested on public roads in...



Vampire Apps

By connecting your Facebook profile to third party plugin apps found on the social network, many of which are from the same firms paying for targeted advertising, you're also typically granting them permission to access your data.


That includes your name, profile picture, cover photo, gender, networks, username and user ID.

Some fear this may also include details like your IP address and other identifying information which can be used to track your online activities.

Facebook has since amended a policy which allowed third-party apps to access your friends' data as well.

Some of the better known apps that may be connected to your profile include those of popular sites like Amazon, BuzzFeed, Expedia, Etsy, and Tinder.

You can check which apps your Facebook account is sharing data with by clicking [here](#).

In the wake of Facebook's Cambridge Analytica row, Mark Zuckerberg (pictured) has admitted his firm 'made mistakes'. Calls have intensified for the Facebook CEO to address the scandal in public or testify in front of lawmakers (stock)



+13

In the wake of Facebook's Cambridge Analytica row, Mark Zuckerberg (pictured) has admitted his firm 'made mistakes'. Calls have intensified for the Facebook CEO to address the scandal in public or testify in front of lawmakers (stock)

HOW CAN YOU STOP FACEBOOK'S ADVERTISING NETWORK TRACKING YOU ONLINE?

Part of what makes companies like Facebook and Google so valuable, is that they oversee vast treasure troves of user data which can be of huge benefit to brands.

For advertisers, it means they're more likely to get a higher click-through rate on their advertisements, boosting the effectiveness of their campaigns.

For users, it means forfeiting personal information to a variety of unknown sources.

Thankfully, there are a number of steps that can be taken to prevent Facebook's ad partners from following you as you browse the internet on your phone or desktop computer.

Changing your settings on your smartphone or tablet

If you own an iPhone or iPad, the steps to block targeted adverts are relatively simple.

Go to Settings, tap Privacy and then scroll down to click on Advertising.

From there, swipe the 'Limit Ad Tracking' button.

If you choose to leave the 'Limit Ad Tracking' feature off, that means that advertisers can track your browsing behaviour by assigning your device a unique ID number, or a Identifier For Advertising.

When you the option on, your device will be represented as '00000000-0000-0000-0000-000000000000.'

In turn, it will be harder for ad technology companies to track your browsing behaviour.

If you own an Android phone or tablet, the process is very similar.

Open up Settings, navigate to Accounts and Sync, select Google, then Ads and finally, select 'Opt Out of Interest Based Ads.'

Changing your browser settings

If you're browsing the internet on Google Chrome, go to 'Settings' in the right-hand dropdown menu.

From there, click on 'Show advanced settings,' then select Privacy.

Finally, click on 'Send a do not track request with your browsing traffic.'

A popup on Chrome further explains what this means: 'Enabling Do Not Track means that a request will be included with your browsing traffic.'

'Any effect depends on whether a website responds to the request, and how the request is interpreted.'

'For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited.'

'Many websites will still collect and use your browsing data-- for example, to improve security, to provide content, services, ads, and recommendations on their websites, and to generate reporting statistics.'

What this means is that not all websites necessarily have to honour 'Do Not Track' requests.

Contacting your local data privacy alliance

Google, Facebook and Twitter are just a few of the major corporations that are part of a number of privacy alliances that have agreed to honour requests to stop tracking.

These are the Digital Advertising Alliance in the US, the Digital Advertising Alliance of Canada and the European Interactive Digital Advertising Alliance.

The websites of each of these organisations contain instructions on how to add your details to their 'do not track' schemes.

Change your tacking settings in Facebook

Facebook has given users of its social network the option to opt out of ad tracking via the site.

First, log in to Facebook, go to Settings, then click on 'Ads' in the menu on the left-hand side of the screen.

Under Ad Settings, click on the button that says 'Ads on apps and websites off of the Facebook Companies.'

Then scroll down to the bottom and select 'No.'

Facebook says that if you select that option, it means that you'll still see ads, but 'they won't be as relevant to you.'

Additionally, you may still see ads related to your age, gender or location.



How you can stop Facebook tracking you online

Part of what makes Facebook and Google so valuable is that they oversee vast treasure troves of user data, which can be of huge benefit to brands.

For advertisers, it means they're more likely to get a higher click-through rate on their advertisements, boosting the effectiveness of their campaigns.

For users, it means forfeiting personal information to a variety of unknown sources.

Thankfully, there are a number of steps that can be taken to prevent Facebook's ad partners from following you as you browse the internet on your phone or desktop computer.

This can be achieved through software settings on your device, or by contacting a number of non-governmental organisations who enforce responsible privacy practices.

When it comes to vampire apps, removing permissions is the most effective route of ensuring they are no longer able to gather information, although this is time consuming.

If you have left Facebook, there are still options for finding out what data, if any, third parties still hold on you and to request that they delete it.

This may also be time consuming, as you will need to contact these third parties

Facebook uses an advertising strategy called the 'Facebook Audience Network' to promote ads targeted to your browsing tastes. It means brands can serve up marketing messages based on your interests even when you're not on the site, via third party apps and mobile websites



+13

Facebook uses an advertising strategy called the 'Facebook Audience Network' to promote ads targeted to your browsing tastes. It means brands can serve up marketing messages based on your interests even when you're not on the site, via third party apps and mobile websites

WHO ARE THE DATA VAMPIRES MINING FOR INFO ON FACEBOOK?

Facebook's latest scandal involving communications firm Cambridge Analytica has served as a startling wake-up call for many users on the countless companies mining our social data.

Through a feature that meant apps could ask for permission not only to your data, but that of your Facebook friends as well, the firm was able to mine the information of 55 million users.

And, only 270,000 had given them permission to do so.

In 2014, Facebook changed its rules so that apps could no longer obtain data about a person's friends unless those users had also authorized the app.

Still, Cambridge Analytica is far from the only firm to have access to Facebook users' data.

By connecting your Facebook profile to a third-party app, you're typically also granting that app permission to access your data.

You can check which apps your Facebook account is sharing data with by clicking [here](#).

To view the apps you've given permission to (as shown above), go to Settings > Apps



To view the apps you've given permission to (as shown above), go to Settings > Apps

That includes your name, profile picture, cover photo, gender, networks, username and user ID. These apps can also access your friends list, and any other public data.

Once the outside parties have access to your data, they can then use it to track different types of activity.

Many popular apps such as Instagram, Spotify, Airbnb, and Tinder can be connected to your Facebook account.

Just weeks ago, for example, MoviePass CEO Mitch Lowe bragged that the company stores 'an enormous amount of information' about users, and even tracks where they go after the movies.

MoviePass is also among the many apps that can be connected to your Facebook.

And, it doesn't stop there.

Facebook users are waking up to just how much of their private information they have accidentally handed over to third-party apps. Social media users are sharing their shock at discovering thousands of software plugins have been gathering their data



+13

Facebook users are waking up to just how much of their private information they have accidentally handed over to third-party apps. Social media users are sharing their shock at discovering thousands of software plugins have been gathering their data

Taking Facebook quizzes from third-party services, or doing image generators (such as the ever-popular 'What Would Your Baby Look Like, or What Would You Look Like As The Opposite Sex), also often gives outside firms access to your data.

While these are usually preceded by a pop-up asking permission to access certain parts of your profile, many users have taken to clicking through without thoroughly reading what they've just agreed to.

Some users are now expressing their horror upon realizing they've granted permission to hundreds of third-party apps.

Other apps that have experienced viral popularity over the last few years, such as Facetune and Meitu, can access your Facebook data as well.



Changing your settings on your smartphone or tablet

If you own an iPhone or iPad, the steps to block targeted adverts are relatively simple.

Go to Settings, tap Privacy and then scroll down to click on Advertising.

From there, swipe the 'Limit Ad Tracking' button.

If you choose to leave the 'Limit Ad Tracking' feature off, that means that advertisers can track your browsing behaviour by assigning your device a unique ID number, or a Identifier For Advertising.

When you the option on, your device will be represented as '00000000-0000-0000-0000-000000000000.'

In turn, it will be harder for ad technology companies to track your browsing behaviour.

If you own an Android phone or tablet, the process is very similar.

Open up Settings, navigate to Accounts and Sync, select Google, then Ads and finally, select 'Opt Out of Interest Based Ads.'

Thankfully, there are a number of steps that can be taken to prevent Facebook's ad partners from following you as you browse the internet on your phone or desktop computer. Chrome and Safari both have options to send 'Do Not Track' requests when browsing the internet



+13

Thankfully, there are a number of steps that can be taken to prevent Facebook's ad partners from following you as you browse the internet on your phone or desktop computer. Chrome and Safari both have options to send 'Do Not Track' requests when browsing the internet

HOW CAN YOU STOP FACEBOOK 'VAMPIRE' APPS FROM HARVESTING YOUR DATA?

One way to try and ensure that your data stays private is to request that your Facebook account be deleted, but that doesn't necessarily protect information you have already supplied.

Many users are willing to trade off the risk of supplying their data for the convenience of staying connected to friends and others on the social network.

So what can you do to protect your data if you want to stay on Facebook?

To begin, visit the settings area of Facebook found via the drop-down arrow in the top right-hand corner of your profile page on the desktop version of the site.

Then click on the apps tab on the left of the page and click 'show all' at the bottom, then you can see, edit, and remove all the apps you've 'consented' to track your account.

Now, a likely vast list of all apps that can access and view your own personal data will be revealed.

To edit or remove these apps from your list of permitted platforms, simply hover the mouse over one of the options.

Clicking the pencil icon will bring up the edit options and clicking the 'X' will bring up the option to remove it.

For each app that has access to the data, users can go in and customise what permissions are granted to each app.

For example, many apps use friends list information, profile information and sometimes even work and educational history.

Most will already know your email and have access to any information on your profile.

To restrict access, there is a blue tick option on the right-hand side of different permissions such as email, profile picture, education etc.

Apps can make some permissions compulsory and these cannot be unchecked and appear as a faded out blue.

If this makes you uncomfortable then the only way to restrict this data reaching that specific company is to click the 'X' and remove the app.

Users can make a judgement call on the optional pieces of information too and customise the data that is shared.

To change the data permissions for all of the apps is time consuming, but it is the only way to gain control over the free distribution of personal data.

By scrolling further down the Settings>Apps window there are other options to further customise who can view personal data.

At this point, it is important to remember that all previous apps were, at some point, granted permission by the user to access their data.

Under the 'Apps Others Use' tab, this gets taken out of the user's hands.

Here, it shows all the data available for Facebook friends to see.

Whilst there may be no issue with this being shared with friends and acquaintances on the social media platform, that data is also being seen by the apps your friends use.

These will include apps that a user did not individually grant permission to.

Here, a checklist of options will appear when selected, and users can customise and restrict what non-authorized third-party apps can view.



Changing your browser settings

If you're browsing the internet on Google Chrome, go to 'Settings' in the right-hand dropdown menu.

From there, click on 'Show advanced settings,' then select Privacy.

Finally, click on 'Send a do not track request with your browsing traffic.'

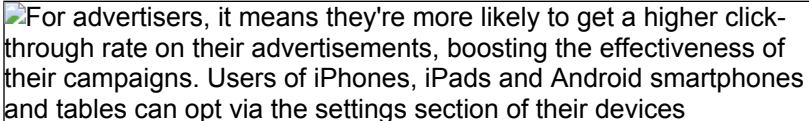
A popup on Chrome further explains what this means: 'Enabling Do Not Track means that a request will be included with your browsing traffic.'

'Any effect depends on whether a website responds to the request, and how the request is interpreted.'

'For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited.'

'Many websites will still collect and use your browsing data-- for example, to improve security, to provide content, services, ads, and recommendations on their websites, and to generate reporting statistics.'

What this means is that not all websites necessarily have to honour 'Do Not Track' requests.

For advertisers, it means they're more likely to get a higher click-through rate on their advertisements, boosting the effectiveness of their campaigns. Users of iPhones, iPads and Android smartphones and tables can opt via the settings section of their devices



For advertisers, it means they're more likely to get a higher click-through rate on their advertisements, boosting the effectiveness of their campaigns. Users of iPhones, iPads and Android smartphones and tables can opt via the settings section of their devices

WHAT ARE COOKIES AND WHAT DO THEY DO?

A cookie's content is determined by the specific website that created it and vary from site to site.

As a general rule, cookies are text files containing random alphanumeric text characters.

They are intended to help you access a site faster and more efficiently.

For example, cookies can store information to help you enter a site without having to login.

When the user visits a website's login page, the web server typically sends the client a cookie containing a unique session identifier.

When the user successfully logs in, the server remembers that that particular session identifier has been authenticated, and grants the user access to its services.

Tracking cookies, especially those used by third-parties, are commonly used as ways to compile long-term records of individuals' browsing histories.

They can collect information including IP address, length of visit, pages visited, length of time spent on a page, in what sequence pages were accessed.

Advertisers can use this information collected to build up a digital profile of a user.

This might not be linked to your real world identity, using a user ID rather than your name, although some websites may link this to your account name.

By adding tags to a page, advertisers can track a user or their device across different websites.

That helps build a profile of them based on their habits, so messages can be better targeted to their interests.



Similar options are available in other browsers, including Apple's Safari.

To access this, pull down the Safari menu and open Preferences

Click the 'Privacy' tab and find the 'Website tracking' section. Checking the box next to 'Ask websites not to track me' sends out a 'Do Not Track' request.

Contacting your local data privacy alliance

Websites and apps that are part of a number of privacy alliances have agreed to honour requests to stop tracking.

Google, Facebook and Twitter are just a few of the major corporations that have signed onto the Digital Advertising Alliance in the US, the Digital Advertising Alliance of Canada and the European Interactive Digital Advertising Alliance.

The websites of each of these organisations contain instructions on how to add your details to their 'do not track' schemes.

Users can also opt out of tracking by contacting a number of non-governmental organisations who enforce responsible privacy practices. Facebook's has also given users of its social network the option to opt out via the settings section of the site and app

Users can also opt out of tracking by contacting a number of non-governmental organisations who enforce responsible privacy practices. Facebook's has also given users of its social network the option to opt out via the settings section of the site and app



+13

HOW DO YOU DELETE FACEBOOK?

Click on the 'help' button on the top right hand corner of your Facebook page.

There is a search bar that says 'How can we help?'. Type in 'delete account'.

This will link you to Facebook's Delete Account page, where you will need to select 'Delete My Account' and enter your login credentials.

'If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you', the message reads.

'Keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added.'

If you want to keep your personal data you need to download it before deleting your account. Pictured is Mark Zuckerberg



+13

If you want to keep your personal data you need to download it before deleting your account. Pictured is Mark Zuckerberg

After two weeks, Facebook will begin the process of deleting all your data from the site, which may take up to 90 days.

If you want to keep your personal data you need to download it before deleting your account.

To download your archive go to 'Settings' and click 'Download a copy of your Facebook data' at the General Account Settings tap.

Then click 'Start My Archive'.



Change your tracking settings in Facebook

Facebook has given users of its social network the option to opt out of ad tracking via the site.

First, log in to Facebook, go to Settings, then click on 'Ads' in the menu on the left-hand side of the screen.

Under Ad Settings, click on the button that says 'Ads on apps and websites off of the Facebook Companies.'

Then scroll down to the bottom and select 'No.'

Facebook says that if you select that option, it means that you'll still see ads, but 'they won't be as relevant to you.'

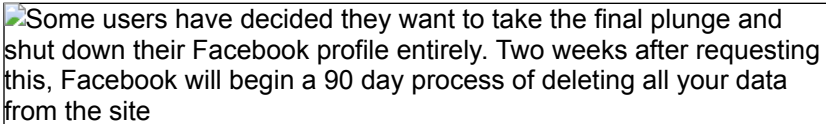
Additionally, you may still see ads related to your age, gender or location.

Deleting your Facebook profile

Some users have decided they want to take the final plunge and shut down their Facebook profile entirely.

To do so, click on the 'help' button on the top right hand corner of your Facebook page. There is a search bar that says 'How can we help?'. Type in 'delete account'.

This will link you to Facebook's Delete Account page, where you will need to select 'Delete My Account' and enter your login credentials.



Some users have decided they want to take the final plunge and shut down their Facebook profile entirely. Two weeks after requesting this, Facebook will begin a 90 day process of deleting all your data from the site



+13

Some users have decided they want to take the final plunge and shut down their Facebook profile entirely. Two weeks after requesting this, Facebook will begin a 90 day process of deleting all your data from the site

'If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you', the message reads.

'Keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added.'

After two weeks, Facebook will begin the process of deleting all your data from the site, which may take up to 90 days.

If you want to keep your personal data you need to download it before deleting your account.

To download your archive go to 'Settings' and click 'Download a copy of your Facebook data' at the General Account Settings tap. Then click 'Start My Archive'.

Using data protection laws to check your data

Facebook users in Europe who want to check what data the firm, and third-party apps, have on them have the legal means to do so.

Under existing data protection laws, the Data Protection Act 1998, you have the right to know what data a company or organisation holds on you.

Most large organisation will have a privacy notice which states what it intends to do with your information and if it intends to share it. If this is unclear, you are entitled to ask for clarification.

In the case of smaller businesses or individuals, you may need to contact them directly.

Facebook users in Europe who want to check what data the firm, and third-party apps, have on them have the legal means to do so. Rules in the US are covered by a wide array of legislation, which varies from state to state



+13

Facebook users in Europe who want to check what data the firm, and third-party apps, have on them have the legal means to do so. Rules in the US are covered by a wide array of legislation, which varies from state to state

WHAT IS THE EU'S GENERAL DATA PROTECTION REGULATION?

The European Union's General Data Protection Regulation (GDPR) is a new data protection law that will enter into force on May 25.

It aims to strengthen and unify data protection for all individuals within the European Union (EU).

This means cracking down on how companies like Google and Facebook use and sell the data they collect on their users.

The law will mark the biggest overhaul of personal data privacy rules since the birth of the internet.

Under GDPR, companies will be required to report data breaches within 72 hours, as well as to allow customers to export their data and delete it.

The European Union's General Data Protection Regulation (GDPR) is a new data protection law that will enter into force on May 25. It aims to crack down on how companies like Google and Facebook use and sell the data they collect on their users



+13

The European Union's General Data Protection Regulation (GDPR) is a new data protection law that will enter into force on May 25. It aims to crack down on how companies like Google and Facebook use and sell the data they collect on their users

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.

Further, the controller must provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Under the right to be forgotten, also known as Data Erasure, are entitled to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

The conditions for erasure include the data no longer being relevant to original purposes for processing, or a data subject withdrawing their consent.

This right requires controllers to compare the subjects' rights to 'the public interest in the availability of the data' when considering such requests.



You can make a 'subject access request' to any organisation you think may hold information about you. It is then legally required to send you the details in 'intelligible form', although there may be a small charge for this.

You are also within your rights to request that an organisation to stop using your details.

If they ignore your request you can take the firm to court or complain to a regulatory body. In the UK, this is the Information Commissioner's Office.

These laws are due to be bolstered with the introduction of the European Union's General Data Protection Regulation, a new data protection law that will enter into force on May 25.

Rules in the US are covered by a wide array of legislation, which varies from state to state and across different industries.

The main national act that impacts Facebook's data is the Federal Trade Commission (FTC) Act.

The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorised disclosure of personal data.

The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising.

They also suggest that company's disclose that consumers can opt out of these practices, providing an opt-out mechanism.


WHAT IS THE CAMBRIDGE ANALYTICA SCANDAL?

Communications firms Cambridge Analytica has offices in London, New York, Washington, as well as Brazil and Malaysia.

The company boasts it can 'find your voters and move them to action' through data-driven campaigns and a team that includes data scientists and behavioural psychologists.

'Within the United States alone, we have played a pivotal role in winning presidential races as well as congressional and state elections,' with data on more than 230 million American voters, Cambridge Analytica claims on its website.

The company profited from a feature that meant apps could ask for permission to access your own data as well as the data of all your Facebook friends.

 The data firm suspended its chief executive, Alexander Nix (pictured), after recordings emerged of him making a series of controversial claims, including boasts that Cambridge Analytica had a pivotal role in the election of Donald Trump



+13

The data firm suspended its chief executive, Alexander Nix (pictured), after recordings emerged of him making a series of controversial claims, including boasts that Cambridge Analytica had a pivotal role in the election of Donald Trump

This meant the company was able to mine the information of 55 million Facebook users even though just 270,000 people gave them permission to do so.

This was designed to help them create software that can predict and influence voters' choices at the ballot box.

The data firm suspended its chief executive, Alexander Nix, after recordings emerged of him making a series of controversial claims, including boasts that Cambridge Analytica had a pivotal role in the election of Donald Trump.

This information is said to have been used to help the Brexit campaign in the UK.

Read more: <http://www.dailymail.co.uk/sciencetech/article-5528785/Facebook-track-delete-account.html#ixzz5AVJHLbQC>

Follow us: [@MailOnline](#) on Twitter | [DailyMail](#) on Facebook