COMPUTER NEWS from the

September 2019 Volume 7 NO.9

As found on the web and other sources!

Facebook To Reveal User Tracking Secrets

By John Lister on August, 21 2019 at 09:08AM EDT

Facebook is to show users what data it collects about their activity on other sites. It won't stop tracking, but will make the data anonymous if users ask.

The changes will come in a new settings option called "Off-Facebook Activity." This will list all websites and apps that share data about user activity with Facebook.

This most commonly happens through two methods. One is that the user has opted to log in

to the third-party site through Facebook. In other words, as long as they haven't logged out of their Facebook account, they don't need to create or input user names and passwords for the other websites.

The other method is called Facebook Pixel. That's a tracking cookie which third-party sites can use to match up activity on their sites with a user's Facebook data. The idea is that sites can figure out how effective their Facebook advertising is, not just by seeing whether it gets Facebook users on to their site, but what they do there - for example, whether the ads attract users who go on to buy products. (Source: hootsuite.com)

Users Can Block By Site

Both methods allow Facebook to gather data on users beyond what they actually do on Facebook itself. That in turn allows more targeted advertising on Facebook.

As well as seeing a list of apps and sites that share data with Facebook, users will be able to block future tracking by either selecting individual apps and sites or blocking everything. The latter option will also stop apps and sites sharing the personalized data in future.

'Clear History' Label Confusing

The options will have a somewhat misleading name of "clearhistory". In fact, the data from previous tracking won't be deleted by Facebook. Instead, it will be anonymized and aggregated, meaning it won't be linked to the individual user.

Also, the sites and apps will be able to continue sharing data on future activity by the user, but again it will have to be anonymized.

The feature is currently being tested on users in Ireland, South Korea and Spain before rolling out worldwide. However, it won't be heavily promoted and it seems likely users will need to find out about the feature and actively go into the settings menu to use it, rather than Facebook actively prompting users to consider the issue. (Source: bbc.co.uk)

What's Your Opinion?

Did you know third-party sites shared data with Facebook in this way? If you use Facebook, will you change these settings when available? Have you noticed Facebook ads being affected by what other sites you've visited?

Google wants everyone to dump their nasties in its Sandbox

Life could be a beach (box)

Sand in your face, Google in your privates

By Chris Merriman @ChrisTheDJ

GOOGLE HAS ANNOUNCED Another neat little idea to protect your privacy from everyone that wants to steal your personal data, except Google.

The Privacy Sandbox would offer a range of tools for Chrome and Chromium users, which would form an industry-standard going forwards.

"Technology that publishers and advertisers use to make advertising even more relevant to people is now being used far beyond its original design intent - to a point where some data practices don't match up to user expectations for privacy," explains Google.

"Recently, some other browsers have attempted to address this problem, but without an agreed-upon set of standards, attempts to improve user privacy are having unintended consequences."

The key feature of Privacy Sandbox is the ability for you to receive personalised ads (yay for Google) but without data that makes you personally identifiable (yay for the rest of us).

Amongst the proposals would include a feature which would identify you as having certain interests (say, Elon Musk and Wensleydale) but would only allow you to appear in that pool of potential advertisers if there were enough like-minded people in the group to make you part of the crowd.

The "privacy budget" would ensure that companies would be blocked from contacting you unless the pool was big enough to make you disappear.

Although this proposal is still in its early days, it represents a genuine attempt to solve an issue affecting all tech firms right now. They need cookies to make money. But cookies can leak.

If Google can persuade the rest of the industry, which has been invited to comment on the proposal, to join its Sandbox idea, there's a framework there to create some sort of badly needed compromise for the internet.

Something has to give, and it's too late to start the internet from scratch, for now. This, Google thinks, could be the next best thing.

LET’S NOT FORGET THE ANDROID USERS

Cut the Best Part of Your MP3 And Save It As Your Ringtone for Android

Last updated by Jojo Yee on 12. August 2019 -

A ringtone maker is simply an audio cutter or editor that allows you to trim an audio file for use as a ringtone, alarm or notification sound on your mobile.

An early version of Android ringtone maker that is open source and known as Ringdroid developed by the Ringdroid Team from Google was well received by users but it seems no longer available from Google's Play store and the project has moved to GitHub.

If you like the above open source app Ringdroid, which does not contain ads, you may be able to get it from a third party store like APKPure.

Otherwise, look for other popular alternatives like **Ringtone Maker** by Big Bang Inc. It is easy to use with handy features, inclusive of assigning or re-assigning ringtones to your contacts. The Pro version is a paid-for app without any ads, while the free version contains ads that are so far not intrusive.

Chrome to Check Passwords Against Hacked Databases

By John Lister on August, 26 2019 at 01:08PM EDT

Chrome may soon warn users if their passwords have been compromised. It works by checking inputted passwords against those exposed in public data breaches.

The feature is already available for Chrome from an official Google extension known as Password Checkup, but users need to actively install this extension to use it. Web browser Mozilla Firefox already has a similar feature built-in.

Now a similar feature named "password leak detection" has been spotted in the code of Chrome Canary. That's a version of Chrome that includes test features planned for release in the main Chrome edition in a future update. The Canary name comes from miners taking a bird underground, the idea being that they would pass out or die from any gas leak and act as a warning before the humans suffered the same effects.

Feature Currently At 'Experiment' Stage

The new feature is very much at the testing stage as even within the Canary edition, it isn't enabled by default. Instead, users must manually switch it on in a section marked "Experiments." (Source: techdows.com)

The feature kicks in whenever a user enters a password on a website, whether by manually typing it or using a stored password. Chrome then checks the password against a database of publicly leaked passwords that have been exposed by hackers.

If there's a match, the user sees a pop-up message reading "Chrome found this password on a public list of unsaved passwords that were part of a data breach." It suggests the user review their password and also offers a randomly generated password to use in its place. (Source: express.co.uk)

Reused Passwords Could Be Caught

In some cases they'll be left to do this manually. In other cases, Chrome will redirect the user to the relevant page on the website in question for changing password details.

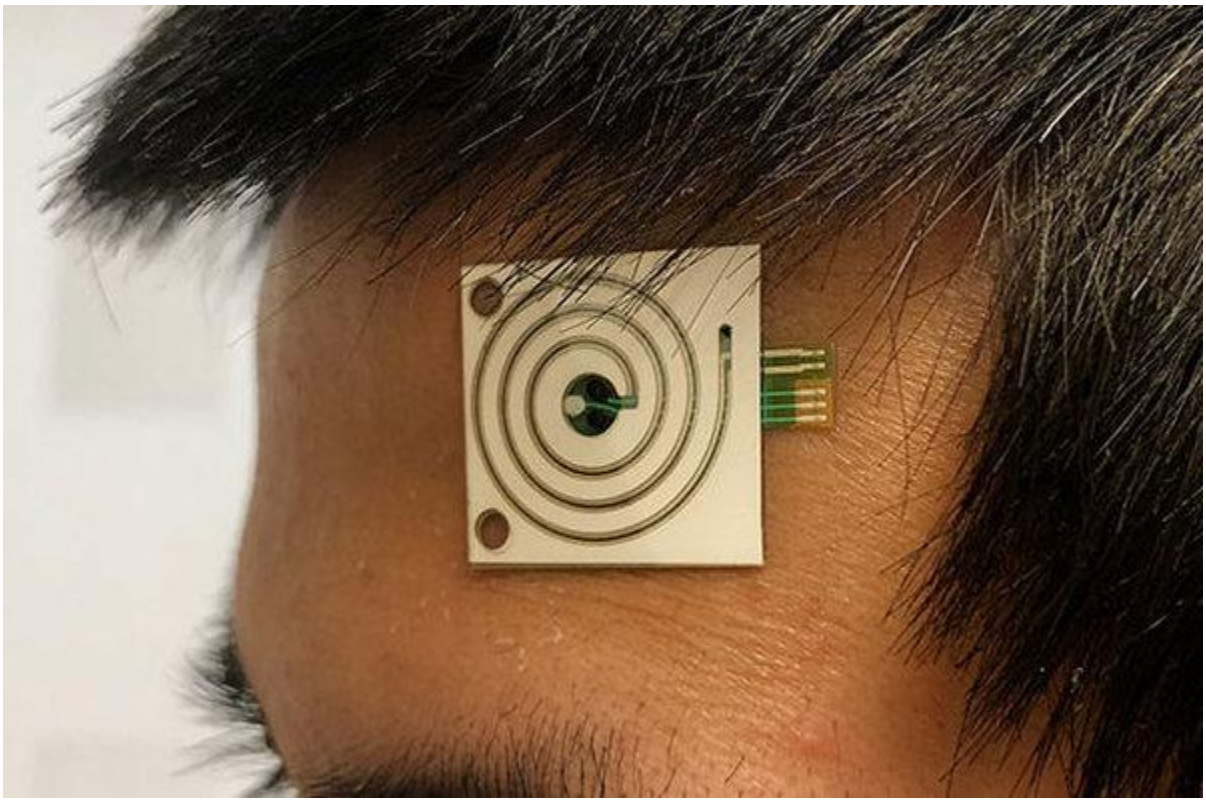
The feature only looks for the password on leaked lists rather than trying to match it to a specific site. The idea isn't solely to prevent a compromised account of the site the user is visiting right now, but rather to also look for cases where people reuse the same passwords.

That's because of the risk that when a site's password database is exposed, hackers will take a user's login details from that site and try it on other popular websites to see if they've reused it.

What's Your Opinion?

Would you find this feature useful? Should it be enabled by default or kept as an optional extra? Is there a risk that the people who most need such warnings will be more likely to ignore them?

COMPLICATED SOLUTIONS TO A SIMPLE PROBLEMS



Berkeley geniuses have invented a patch that analyzes sweat. The

patch **checks your perspiration** for sodium, potassium and glucose levels and figures out what kind of hydration you need
Alternatively, you could just drink water when you're thirsty.

THOUGH FOR THE MONTH!

Everyone has a photographic memory. Some don't have film.
