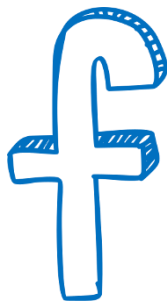


Who Knows? Facebook Knows!



Have you been shopping online and then noticed that ads start appearing on your Facebook that are directly related to what you have just been shopping for? This is no coincidence and is known as Targeted or Interest Based Advertising. Statistics prove that you are much more likely to buy something this way than from a random ad.

Personally I don't mind this but if you find this just too weird then follow these steps for you to disable 'Interest Based Advertising'. For a laptop or desktop computer:

- Log in to your Facebook account.
- Click the down arrow located on the right side of the blue bar at the top of the window.
- Click Settings.
- Click the Ads link located in the left-hand column.
- Click Ad settings to expand that section. You should now see three settings listed in that section.
- Change the first two settings to Not allowed, then toggle the third setting to No One.

If you want to know how to do it on a mobile device like a tablet or phone then let us know. There are more steps but it is still easy enough. *Damon*

Private Searching



If you're interested in testing a privacy focussed internet search engine try duckduckgo.com. Your search results are likely to be lower quality than Google search results, however if privacy is your thing, then DuckDuckGo has no advertising trackers or ad targeting, and does not store your search queries.

OPINIONS ON INTERNET PRIVACY

THE NIHILIST:

JOKES ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.



THE EXHIBITIONIST:

MMMM? I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.



xkcd.com/1269/

CC BY-NC 2.5

...a little CRC



MY GOV TAX SCAMS

Tax time is here, and we see a surge in scammers impersonating myGov or the Australian Taxation Office (ATO) to trick you into giving them money or personal details. These scams can come through as emails, text messages and fake myGov login pages. Usually these scams will say you're entitled to a tax refund or that you need to pay a debt. They are also made to look very real through the sophisticated use of myGov and ATO logos, information and even email addresses which makes it easy for anyone to fall victim.

How do I stay safe?

- myGov will never send you a text, email or attachment with links or web addresses that ask you for your login or personal details. Do not click on links in emails or text messages claiming to be from myGov.
- Always login to your official myGov account to check your tax, lodge your return, and check if you owe a debt or are due a refund. Do this by manually typing my.gov.au into your internet browser address bar.
- You can also check the status of your tax affairs at any time by calling the ATO on 13 28 61.
- Have a strong password on your myGov account and add a security code to your login process to provide an extra layer of protection. This makes it harder for a hacker to get any further if they crack your password.
- Unfortunately these scams continue well beyond the 30 October deadline for tax returns, as scammers know many people are waiting for a refund or debt owed. Watch out for scams throughout the year.

More information: ato.gov.au/scams
staysmartonline.gov.au

Monday, Tuesday, Wednesday 10 am to 5 pm • Thursday 10 am to 6 pm • Friday 9 am to 6 pm