Facebook says it takes privacy seriously. Oh yeah? It's easy for us to complain about how Facebook shares our information but we give the social network permission by not looking closely at some of the options in settings. Plus, we make some mistakes that make it easy for companies to follow us on and off of Facebook. I'm looking at some privacy settings you should change if you're serious about protecting your information.

TRT 130
STD OUT

SUPER

0-8 Jamey Tucker/whatthetech.tv

ON-CAMERA TEASE

FACEBOOK SAYS IT TAKES PRIVACY AND SECURITY SERIOUSLY. THAT'S HARD FOR SOME OF US TO BELIEVE. I'M JAMEY TUCKER COMING UP WITH SOME OF THE THINGS WE'RE DOING THAT PUT OUR INFORMATION AT RISK.

ANCHOR INTRO

BY NOW WE ALL UNDERSTAND THAT FACEBOOK EARNS REVENUE BY LOOKING AT AND SOMETIMES SHARING OUR INFORMATION WITH OTHER COMPANIES.
BUT SOME OF THE THINGS WE ALL DO, MAKE IT EASIER FOR COMPANIES TO SEE MORE THAN YOU WANT THEM TO SEE.

A LOT OF PERSONAL INFORMATION POSTED ON FACEBOOK GETS INTO THE HANDS OF OTHER COMPANIES BECAUSE WE GIVE THEM PERMISSION. AS OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER SHOWS US, YOU CAN PROTECT YOUR INFORMATION BY CHANGING A FEW SETTINGS.

PACKAGE SCRIPT

If you haven't looked into Facebook's settings in quite a while, I can guarantee you're not going to like some of what you see. Not things Facebook does without permission, but because you're giving them permission.

If you haven't taken Facebook's Privacy checkup that's a good place to start. It'll show you where your information is being shared. There's a lot here so let's hit the high points:

Have you signed into an app or website using your Facebook login? We all have. It's a good idea to review those logins. Under settings and permissions, look at apps and websites. These are all the sites and apps you've connected to your Facebook account. These companies have

access to your Facebook information. You'll see some here you've forgotten about. Many will date back years. review them, and delete any you no longer use.
also under security, look at off-facebook activity. These are companies that share information when you visit their website. You may see hundreds here all sharing your web activity with Facebook such as when you open its website or app, what you searched for, purchased, and added to a wishlist.
you can't pull the information from the past but you can stop sharing in the future
It's also a good idea to check where you're logged in to Facebook. If you see any you don't recognize, you can log out of that device, or all of them. you'll just have to log back in on the devices you use.
Not only will these privacy changes protect your information being shared, but they could also reduce the risks of being hacked. That's What the Tech? I'm Jamey Tucker

ANCHOR TAG

FACEBOOK INSISTS IT DOES NOT SELL ANY PERSONAL INFORMATION. BUT BASED ON THE INFORMATION IT HAS GATHERED FROM ITS USERS, ADVERTISERS PAY META OR FACEBOOK, TO SHOW PERSONALIZED ADS ON FACEBOOK AND INSTAGRAM.

WEB STORY

Facebook says it takes the privacy and security of its users seriously. That may be hard for some people to believe but much of the information gathered and shared with advertisers isn't gathered by Facebook without permission, but by people giving permission to do it. If you haven't taken a look at what information you're sharing with advertisers may want to take Facebook's Privacy checkup.

There's a lot to process so let's hit the high points:

Have you signed into an app or website using your Facebook login? We all have. It's a good idea to review those logins. Under settings and permissions, look at apps and websites. These are all the sites and apps you've connected to your Facebook account. These companies have access to your Facebook information. You'll see some here you've forgotten about. Many will date back years. review them, and delete any you no longer use.

Also under security, look at off-Facebook activity. These are companies that share information when you visit their website. Facebook uses this information to push ads your way that you've shown interest in. You may see hundreds here all sharing your web activity with Facebook such as when you open its website or app, what you searched for, purchased, and added to a wishlist. When I looked under this tab I found a website I visited the site once or twice recently that shared over 29-thousand interactions I had on its website with Facebook. That shouldn't be worrisome if it's a company you frequently do business with, but if it's a company you have no memory of using, it's a good idea to stop sharing with them.

You can't pull information from the past but you can stop sharing in the future.

It's also a good idea to check where you're logged in to Facebook. If you see any you don't recognize, you can log out of that device, or all of them. you'll just have to log back in on the devices you use.

If you use a VPN or virtual private network, don't freak out because of the long list here. Facebook tracks the location of those logins and a VPN, for safety reasons, will log you in from locations around the world to protect your actual location and IP address.

Not only will these privacy changes protect your information being shared, but they could also reduce the risks of being hacked.

www.whatthetech.tv