CYBER PRIVACY why it should matter to you

NUHAN B. ABID

You've heard the age old adage "don't talk to strangers", but funnily enough in the internet we end up talking a lot to strangers. In fact on the internet, information we'd formerly be conscientious about, like our daily activities that we'd probably once keep private in a diary, are now openly share without so much as a second thought. Given the massive boom in social media, and how easily we let our information be accessed, it's no surprise that data we share can be misused. And that brings us to our topic of today, cyber-privacy.

WHAT IS CYBER PRIVACY, AND WHY IS IT IMPORTANT?

Do you like leaving your door open when you leave the house? You do that, and you're basically saying "hey, come in" to any passerby on the street. Now some of them might be harmless, but you'll probably be missing something because it got stolen by a random intruder.

That's effectively the equivalent of what happens to your data when you post it online without taking any steps to prevent it from being stolen. I shouldn't have to tell you why it's important to protect it, since after all, letting people steal your information without your consent should feel wrong to you.

By now, you've potentially heard about the Cambridge Analytica scandal, where information belonging to millions of users on Facebook was leaked to the aforementioned data analyst group, who in turn sold it off for profit, despite their supposed agreement to protect your data as per their "Terms of Service".

Forget just basic ethics, your data could be potentially accessible for misuse, ranging from identity theft to having your critical personal information (like home address, credit card numbers etc.) leaked online. And this is why cyber privacy is important, since it means you're actively taking steps to keep your data secure, private and away from prying eyes.

WHERE IS YOUR DATA BEING USED AND WHY?

If you're wondering why your data is valuable, it's because it can be used to personalise and target advertisements at you. Social media companies earn revenue from advertisements, i.e. they place ads in your feed so you can engage with them. "Personalised ads" mean that they're specific to your tastes and interests, so you're more likely to engage with them.

Ironically, despite the value of your data to you, on average it isn't worth much to a company. In the first quarter of 2014, Google's ad revenue per user data showed an average of USD 45 for each individual data profile. Of course, considering how many people use Google itself, you can clearly see where the money is being raked in.

Almost everyone uses a smartphone these days, which include several apps ranging from social media to texting to games and whatnot. For these apps to actually run, they usually need permissions from your device. They usually show you this when you install said apps, although most users maybe skim over them or don't really understand what they mean.

Some permissions may be justified, for example Snapchat – which you probably use to take pictures – will need access to your phone's camera so it can do so. But then again, some apps may have undesirable permissions that you don't want to give because it looks off or doesn't actually appear to need them. For example, you might have downloaded a game from the app store but then realised it wants permission to dial or get your location data, despite the game not really needing either. You can disable them if you feel like they don't require this and are being needlessly intrusive which may potentially threaten your data. This is usually a red flag anyway for unwanted data collection.

The Facebook app is another example of a highly intrusive app, as it is one of those apps that refuse to function with some permissions turned off. And while Zuckerberg can deny it all he wants – even in front of the US Congress – that your data isn't being collected for use, it's not entirely true. They admit to personalising ads for you, and you can check this by going to your account settings and ad preferences. There you can actually see what they believe you have interests in, your political affiliation and demographic status, and that'll give you an idea of what they might want to show you as ads.

In fact, if you want to check what data the two biggest internet giants have on you, you can. Dylan Curran recently posted a Twitter thread that went viral – breaking down exactly what kind of information is collected by sharing the data Facebook and Google had on him. While you can search him and see for yourself the details of what that data entails, we'll try and just summarise it here to give you an idea.

Google has all your search history on itself and YouTube dating back several years, all your app history and of course, an ad profile. Google also has your location history of everywhere you've been with your phone. Facebook stores your entire contacts list from your phone, as well as files you've sent/received, along with all your messages on Messenger. And of course, that's not even the end of it. You can check your own by going to google.com/takeout or https://www.facebook.com/help/131112897028467; be prepared to see what they have on you. It's a lot and it's disturbing to know how much your privacy is violated on a day to day basis in exchange for conveniences. It's even freakier when you realise that in the wrong hands anyone can know almost everything about your life from your data if they just get access to your Google/Facebook accounts.

SO HOW DO I KEEP MYSELF SAFE(R)?

The honest truth is you probably can't ever achieve complete privacy in the digital age. It's knowing about how to make safe trade-offs in your internet use. Some key tips:

1. Don't use apps without checking their permissions; turn them off if you feel like they don't need some of them.
2. Don't connect any random third party app to Facebook, *especially* those Facebook quizzes – those are prime data mining grounds. In fact, using one of those apps is how the Cambridge Analytica scandal happened – they took a lot of data from one such quiz.
3. Don't post any content you don't want publishable online. These include private photos you'd prefer not to be online, or critical information like your credit card details on places that do not need them.
4. Do not fall for phishing scam sites. Phishing refers to tricking you into giving up details like your username/passwords/credit card details by posing as legitimate entities. Scammy looking emails don't always go to spam, check the email address; Google/Outlook/your email provider of choice always have special emails that you can easily identify, they won't use generic looking emails from themselves.

   Always check the URL to see if the website is legitimate, and not a clever copycat; oftentimes the URL are common typos that take advantage of people's mistakes and then trick them into giving up data with a site that looks the same.
5. Following up on the last point, if you have to divulge information as sensitive as credit card details, always check if the website has an https connection, emphasis on the "s". That implies a secure encrypted connection, and you can check that also with an icon of a lockpad in the URL bar.
6. If you're especially paranoid after reading all this, drop using Google and Facebook entirely, switch to using a VPN to disguise your online browsing habits, and use Tor browser to maintain even more privacy. Similarly, DuckDuckGo is an alternative search engine to Google that won't track your searches.

If after all this, you're not convinced and think this isn't enough, just disconnect your computer, crush it into dust, run away, and move into a secluded forest in the middle of nowhere. At least that way, no one's going to steal your data and track you.

In the end, cyber privacy remains an important topic in daily discussion, and one for lawmakers to take seriously. The best way to stay safe is to try and be smart about what you use on the internet, and hope that the ones you do trust to keep your data don't accidentally leak it.

Nuhan B. Abid is someone who actually thinks puns and sarcasm are top class forms of humour. Tell him that 'sar-chasm' is TOTALLY the best thing ever at nuhanbabid@hotmail.com