GUARDING YOUR PRIVACY on Facebook

In an era of information and data collection, it is important that we understand the data that is collected on us and protect what we feel should remain private. We have to be active guardians of our privacy. We must also understand that in some circumstances, providing some data about our self can be an appropriate exchange for specific functionality. Here are a few steps you can take to protect your privacy online.

REVIEW YOUR APPS

The source of the troubles with the Facebook/Cambridge Analytica issue is a Facebook App. Apps give developers access to much of the data that Facebook has about you, including demographic information, likes/interests, friends lists and more. You can protect your privacy by looking at the apps that have gained access to your information and removing those that shouldn't have access to your information.

From the Facebook Dropdown Menu, select settings (or navigate to facebook.com/settings)
…

> Select "Apps and Websites" from the left column menu

> Look at your Active Apps and start with the first app. If you use the app, click on "View and edit" and see what data is has access to. It may need access to some perform its functions. You can edit what it has access to. If you don't recognize the app, remove it from your account.

SECURE YOUR EMAIL ADDRESS

Facebook makes its money through its advertising network. The power of its advertising comes from the information it has on its users. Facebook creates a record for each user that contains demographic information, interests, behaviors and more. Much of the information comes from activities and information you provide during your online experience. However, some comes from comparing your information with other consumer databases, like data from credit reporting agencies. It uses your email address to match your Facebook account to these consumer databases. Using a separate email address just for your Facebook account limits the matches.

LIMIT PERSONAL INFORMATION

Facebook asks you for a lot of information. Oftentimes, it wants you to complete your profile by providing more information. You do not have to provide all this information. Really the only information you have to provide is a valid, email address and birthdate.

Your name must be correct. According to Facebook, your real name is required. That name is what "would be listed on your credit card, driver's license or student ID." Using a fake name would violate their terms and could result in your account being suspended. Appealing a violation is very difficult.

You must provide a valid email address. According to Facebook's Terms of Service, you are required to provide accurate information and up-to-date contact information. In order to protect your privacy, we recommend setting up a secondary email address that you only use for communications with Facebook. This will help to eliminate some of the synchronizations with external databases.

DOWNLOAD AND REVIEW YOUR INFORMATION

Facebook offers users the ability to download all of the information that it has about you. Everything it's facial recognition code to the photos and posts you have uploaded. If you are active on Facebook, this can be a very big file. We encourage you to do this once in a while and review the information that Facebook has on you.

From the Facebook Dropdown Menu, select settings (or navigate to facebook.com/settings)
…

At the bottom of the main section of text, you will see the link to "Download a copy of your Facebook Data." Click on "Download a copy."

INSTALL A PIXEL/COOKIE BLOCKER

Facebook uses pixels and cookies to tailor your ad experience. A pixel is a piece of code on a website that ties your web browsing with your Facebook account. Cookies are small files on your computer that save certain information. Both of these are typically harmless but can pose some privacy issues. They allow Facebook to deliver specific advertising to you based on the sites that you visit.

As someone who does a lot of Facebook advertising, seeing relevant ads is not a problem for me. I have purchased some amazing tools and products from ads that I have seen on Facebook. If this is a problem to you, you can install a pixel or cookie blocker.

One of the best privacy tools available is Disconnect. Disconnect was built on the premise "that people should have the freedom to move about the Internet - and their lives - without anyone else looking over their shoulder." This tool uses Virtual Private Network (VPN) technology to your sensitive online activity from "wireless eavesdroppers." Disconnect encrypts your Internet connection and keeps you safe from hackers on public Wi-Fi. It will also hide your geographic information from websites.

Tools like this are great for privacy but may have adverse effects on the functioning of some of the websites and applications you use.

CLEAR YOUR HISTORY/COOKIES REGULARLY

A final piece of advice that we can offer to help you protect your privacy on Facebook and online is to regularly clear your browser history and cookies. For most websites, as you navigate through the pages, little files are saved on your computer with packets of information. Oftentimes these files, known as cookies, store information to help the website function more effectively. These files can also pose violations to your personal privacy. You should regularly delete these files. You do this through your browser. Instruction on doing depend on which browser you are using.

Clearing your browsing history and cookies:

> Google Chrome - http://bit.ly/ClearCookiesChrome

> Microsoft Internet Explorer - http://bit.ly/ClearCookiesIE

> Microsoft Edge - http://bit.ly/ClearCookiesEdge

> Mozilla Firefox - http://bit.ly/ClearCookiesFirefox

> Apple Safari - http://bit.ly/ClearCookiesSafari

The most important lesson to learn here is that we have to be the guardian of our privacy online. Social network, websites and applications are built daily that want access to your life. In some cases, we may be willing to trade some information for some services, but in all cases, we need to ensure that developers and companies are not misusing our private information online.