In the past year, we saw a significant number of data breaches impacting the privacy of individuals. According to the Privacy Rights Clearinghouse, in 2018, 807 publicly disclosed breaches exposed 1.4 billion records. While this is a decrease from 2017's 2 billion records exposed, the problem remains enormous because so many websites, social media outlets, and devices contain our information.

With January 28th being National Data Privacy Day, take some time to consider what types of personal information you should be protecting, and how to do so in a few different ways.

General Personally Identifiable Information

Personally identifiable information or (PII) can be any data that identifies you as a specific individual. This information should be kept private and not shared with others. Examples of PII include your Social Security Number, or your name in combination with your date or place of birth.

Recommendations: Be aware of what you post publicly or submit through applications or services. Consider with whom you share your PII, and give extra scrutiny and consideration as to whether you really need to share this information. If someone contacts you requesting PII through email, social media, or a phone call, do not provide the information. If it is a phone call that you think is legitimate, hang up and call the organization back through a publicly listed telephone number so you can verify the caller is who they say they are.

Information About Your Location

Giving out your location when away from home on social media is a privacy risk. This practice can result in your home being targeted for burglary. Additionally, your family and friends may be targeted by scammers seeking financial assistance on your behalf to help with a non-existent "travel emergency." Three popular methods of this type of location sharing are geotagging (adding a location tag to a social media post or picture), posting a photo in which the background can be easily identified (like Times Square or the Eiffel tower), or "checking in" at a business.

Allowing apps to use your phone's location services has its own privacy concerns, as the app is likely recording or using that data, and may automatically add geotagging to social media interactions in that app as a result!

Recommendations: Customize your location settings to minimize sharing your location with websites and applications, especially on your mobile devices. You can geotag social media posts, pictures, or videos after returning from vacation, going out to eat, or that business trip. Also, check the privacy settings of apps to make sure they don't need access to your location. At a minimum, ensure your social media settings are set to only show your posts and profile to friends.

Security Questions and Social Media

Security questions are a way to authenticate your identity and are an extra layer of security on accounts, which makes it extra important to not post these answers on social media. Posting a picture or writing a post about your first car's make and model, or color of your car, childhood address, favorite

ice cream flavor, mother's maiden name, or elementary school is a bad idea. These are common security questions and by posting this information, you give away the answers, allowing cybercriminals to potentially access your accounts.

Recommendations: When on social media, be aware of what you post (including pictures!) and how it relates to the security questions you selected for your various accounts.

Website/Application Privacy Settings and Permission

All websites and applications have privacy settings. These settings help you control what others are allowed to see, as well as manage your online experience. You should be familiar with these privacy settings and customize them to protect your information. Additionally, when creating an account on a website or application and agreeing to their services, understand what you are giving them permission to do with the data you provide.

Take Responsibility:

Protecting your privacy starts with you. Website owners, websites, and service providers have a responsibility to protect your privacy. However, it is up to you to understand the privacy settings on social media, online accounts, and your devices. Knowing these settings, you will be able to customize them for greater security.

Take ownership of your privacy and read privacy policies and end user license agreements on websites (including social media), and update your settings whenever new privacy features are available.

For More Information:

Privacy Rights Clearinghouse
National Cybersecurity Alliance