ePAPER

APCI FEDERAL CREDIT UNION

Protecting Your Data Privacy

Take control of your information

The Basics of Data Privacy

Data privacy is a broad term used to describe the proper way to collect, share, use and retain data. This data may be gathered or managed by companies, government agencies, healthcare providers or other organizations. Data privacy encompasses practices and regulations to safeguard information like names, addresses, social security numbers, financial details, and online behaviors from unauthorized access, misuse, or exploitation.

As the data economy has expanded, lawmakers have introduced more regulations to ensure transparency into how personal data is used and to clearly define individual rights.

Recent legislation, in some countries and states, has introduced the following measures aimed at protecting and empowering users:

- The right to be forgotten, which allows individuals to request the deletion of their stored data.
- The right to access, which allows individuals to request a copy of the data an organization holds about them.
- The right to opt-in or out, which allows individuals to choose whether or not to share their information.

The data you share about yourself holds value to others. It can be used by various entities to market products or services, recommend medical treatments, determine your creditworthiness, and more.

In 2023, Pew Research Center surveyed 5,101 U.S. adults about data privacy and reported the following results:

- 81% expressed concern about how **companies** use the data they collect about them, while 71% expressed concern about how **the government** uses the data they collect about them.

- 67% have little to no understanding about what **companies** do with the data they collect about them, while 77% have little to no understanding about what **the government** does with the data they collect about them.

The survey showed that if you have these concerns, you are not alone. Data privacy remains a significant concern for many Americans. Many feel overwhelmed by the sheer amount of data being gathered daily, with little ability to control or limit it. These concerns are amplified as emerging technologies, including voice-activated devices, wearables, and facial recognition software become more integrated into everyday life.

While data collection has the potential to offer advantages, such as enhancing efficiency, personalizing user experiences, and promoting better healthcare, there are also significant risks.

Data sharing is not inherently negative, as long as you are aware of what information you are providing, to whom, and for what purpose. Fortunately, you can take steps to maintain greater control over your data privacy.

Tips For Better Data Privacy

Protecting your personal information is more important than ever. Whether you are online or using smart devices, keeping your data private can help safeguard you from identity theft, hacking, and other security risks. The following tips can help you maintain your privacy and keep your information secure.

Review privacy policies: Only one in five Americans regularly read the privacy agreements they sign. While privacy policies can be long and tedious, it is essential to understand how an organization collects, stores, protects and uses your personal data. If you are uncomfortable with a company's privacy policy, it is okay to decline.

Limit app permissions: When you grant an app access to your photos, location, camera, contacts, and other personal data, you give that app's owner access to your information. Be selective with what permissions you allow.

For example, it makes sense that an app that uses a map needs your location, but why would a flashlight app need it? Apps can often function without having access to all your data, so you do not have to grant every permission requested.

Protect social media accounts: Cybercriminals frequently gather information shared on social media accounts to commit fraud. Protecting your privacy on social media apps should be a priority. Do not rely on default settings. Customize the security options to match your comfort level.

Secure sensitive documents: Even in today's digital age, physical documents still play a role in our lives. Be sure to safely store paper records that contain personally identifiable information (PII) and always shred any paperwork that contains PII before disposing of it.

Personally identifiable information (PII) includes information that can directly identify you, such as your name, address, phone number or Social Security number. It also includes information that can indirectly identify you, such as your gender, race, or birth date. If cybercriminals can piece together enough PII, they can steal your identity and commit fraud.

Be selective with disclosing PII: It is surprising how often you are asked to provide personal information, especially your Social Security number. Do not hesitate to withhold it if you are uncomfortable. You can also ask the organization why it is needed and how they plan to protect it. This applies to medical offices. According to the Identity Theft Resource Center, in 2019 there were 525 medical and healthcare data breaches, exposing more than 39 million sensitive records.

Consider disabling cookies: Cookies are a small text file used to identify you and track your online behavior. While they can enhance your browsing experience, they also pose a privacy risk. For better security, consider disabling cookies or allowing only certain ones.

Regularly clearing your cookie cache browser history can limit how much data is collected about you. Additionally, there are browser tools that allow you to customize your web browser, which can help enhance your online privacy.

Know your privacy rights and options: Even after sharing your personal data, you often retain some control over how it is used. Many countries have laws that give citizens the ability to influence how companies manage their data in certain situations. In recent years, some states and local jurisdictions have expanded these rights, offering residents greater protections beyond national regulations.

For example, Americans can reduce telemarketing robocalls by registering their phone numbers on the National Do Not Call Registry. By taking steps to limit how your data is used, you can help reduce your exposure to campaigns that seek to collect even more of your information.

Our Privacy Pledge to You

Your trust and confidence are the cornerstone of our relationship. At APCI Federal Credit Union, we value this trust and confidence, and we believe it is our responsibility to safeguard your personal and financial information. We have established the **APCI Federal Credit Union Privacy Notice and Online Privacy Policy** to ensure you the confidentiality you deserve. You have our promise that we will adhere to these guidelines. It is our privacy pledge to you, our valued member.