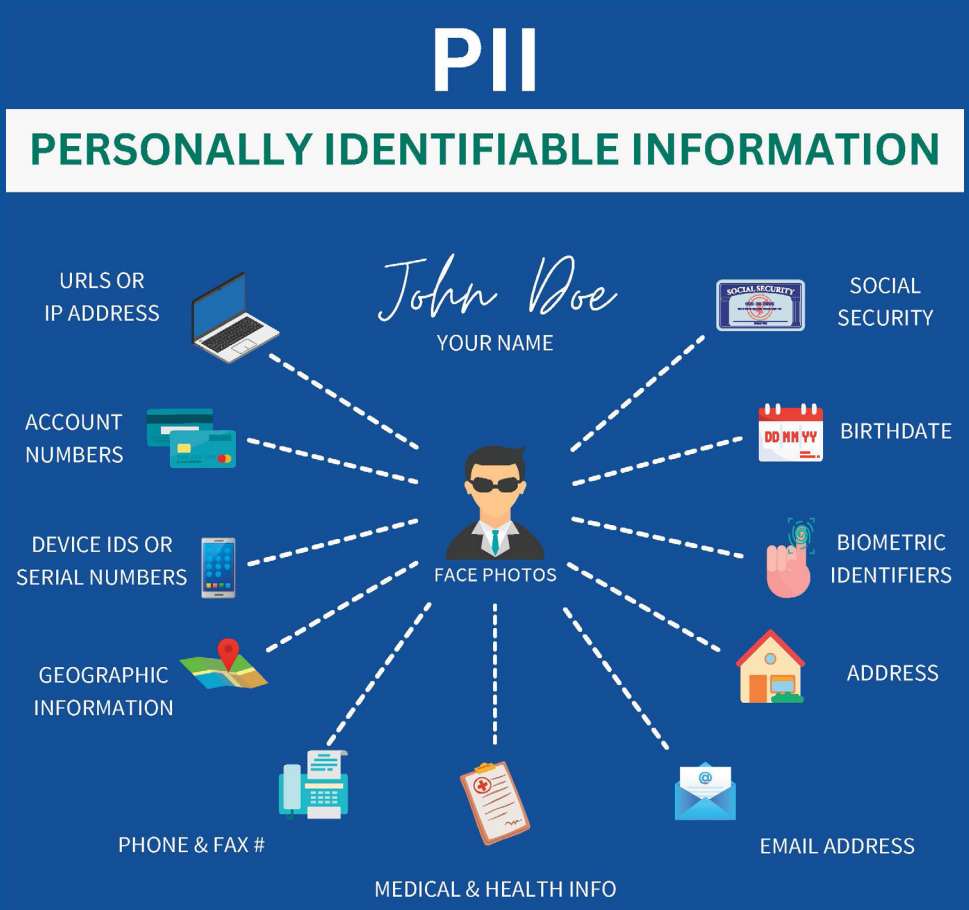
Lumena Financial Strategies

9635 Granite Ridge Rd., Suite 100
San Diego, CA 92123
P (619) 295-9930 | F (619) 295-9947
team@lumenafinancial.com



In today's interconnected world, the internet has become an integral part of our daily lives. While it offers immense convenience and countless opportunities, it also exposes us to potential risks, especially when it comes to safeguarding our personally identifiable information (PII). PII refers to any data that can identify an individual, such as name, address, social security number, email, or financial information.

Protecting your PII is crucial in safeguarding your identity and ensuring your online safety. By following the best practices outlined on the reverse side of this flyer, you can significantly reduce the risk of falling victim to identity theft, data breaches, and other cybercrimes.

You have probably heard about recent, large data breaches on the news or you may have received a letter stating that your PII may have been exposed. While you cannot always avoid data breaches through third-parties, you can take steps to make it harder for your PII to be exposed.

Stay vigilant, be cautious with your data, and always prioritize your privacy and security while enjoying the benefits of the digital world. Remember, if it sounds too good to be true, it is. Taking proactive steps today can save you from potential headaches and financial losses tomorrow. Stay safe, stay secure!

Ten Helpful Tips

- **Be Cautious Online:** Exercise caution when sharing personal information online. Avoid posting sensitive details, like your full birthdate, home address, or financial information on social media platforms or public forums. Cybercriminals can use this information to impersonate you or gain unauthorized access to your accounts.
- **Strong Passwords and Two-Factor Authentication (2FA):** Create strong, unique passwords for each of your online accounts. A strong password should be a mix of upper and lowercase letters, numbers, and special characters. Or consider using a passphrase instead of a password to make it event harder for people to guess and easier for you to remember! Additionally, enable two-factor authentication whenever possible. This extra layer of security ensures that even if your password gets compromised, an additional verification step will be required before accessing your account.
- **Update and Secure Devices:** Keep all of your devices including smartphones, computers, and tablets, up to date with the latest software and security patches. Install reputable antivirus and anti-malware software to protect against potential threats.
- **Secure Wi-Fi Networks:** Secure your home Wi-Fi network with a strong password and encryption. Avoid using public Wi-Fi for sensitive activities like online banking or accessing confidential documents and accounts. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your internet connection.
- **Be Wary of Phishing Attempts:** Phishing emails and messages are designed to trick you into revealing your PII. Be cautious of suspicious emails, especially those requesting sensitive information or containing urgent, unsolicited offers. Verify the sender's email address and never click on links or download attachments from unknown sources.
- **Review Privacy Settings:** Frequently review the privacy settings on your social media accounts and other online platforms. Limit the amount of personal information visible to the public, and only accept friend requests or connection requests from individuals you know.
- **Avoid Oversharing on Social Media:** Think twice before sharing too much personal information on social media. Even seemingly harmless details can be used by cybercriminals to build a profile and attempt targeted attacks.
- **Use Encrypted Communication:** When exchanging sensitive information, use encrypted communication channels like secure messaging apps or end-to-end encrypted email services to ensure that your data remains private.
- **Regularly Monitor Financial Accounts:** Monitor your financial accounts regularly for any unauthorized transactions. Report any suspicious activities to your financial institution immediately.
- **Dispose of Data Properly:** When disposing of physical documents or electronic devices that contain personal information, ensure you do so securely. Shred paper documents and perform a factory reset on electronic devices to wipe all data. We offer a secure on-site shredding event annually around Earth Day as a free benefit to our clients!