

KEEPING YOUR PRIVACY PRIVATE



- Install VPN software on your personal computers and smart phones. This hides your browsing habits and protects you from fraudsters who try to access your phone when you are on a Wi-Fi network.
- Install antivirus and anti-malware apps on your personal devices.
- Review every app on your phone and turn off local settings except for app you use regularly that require location information, such as Waze for traffic conditions, weather and apps that provide directions.
- Review and understand privacy settings on your social media accounts, particularly Facebook and WhatsApp. As Fast Company says, “you can’t have privacy and use Facebook.
- Fast Company also recommends using a search engine other than google, because Google’s business model (like Facebook) generates profit by knowing what you do online.
- Be careful not to post identifying information about your family and work on social media accounts. Fraudsters are skilled at combining facts about people to impersonate them online.
- Don’t accept friend requests from people you don’t know, and don’t allow anyone to follow you on twitter.
- Go to your Google account and run a “privacy checkup.
- Remember, while Gmail is secure, it indexes all the text in emails you send and receive to serve up relevant advertising as you surf the web.
- Don’t use social media accounts to log in to other websites.
- Check out as a “guest” when you purchase something on an e-commerce site where you don’t shop frequently.
- For messaging, use Signal or Apple’s messages APP instead of Facebook messenger or WhatsApp.
- Remember, everything you post online creates a digital trail about you, and it will live on the web forever.

FULTON
INDUSTRIAL



**BOULEVARD
IMPROVEMENT
DISTRICT**