
Tips for Minimizing Risk to Your Identity

Below we have noted tips to help you minimize your risk of exposing your identity. These practical steps are easy to follow and are a great way to begin incorporating consideration for the way you can prioritize safeguarding the privacy of your information into everyday activities.

- Guard your personal information—always question when someone asks for it, whether in person, by phone, or by email.
- Leave at home any sensitive documents you will not need that day (credit/debit card, checkbook, etc.).
- Cross-cut shred everything containing sensitive information before throwing it away.
- Be cautious when responding to promotions. If it seems too good to be true, it probably is.
- Teach children not to give out personal information over the phone or on the internet.
- Beware of phishing emails. Anyone asking you to provide personal information by email, visiting a website, or calling a number could be fraudulent.
- Use social media sites carefully. Fully explore and activate the security features each site offers.
- Don't reveal too much about yourself on the internet, whether through text or photos.
- Use only your secure personal computer to access websites that require you to enter personal identifiers.
- Remove and destroy the hard drive of your old computer before selling or recycling.
- Use complex, and different, passwords for all your accounts you access online.
- Beware of job offer scams. Be certain that the employer or business is legitimate.
- Deposit outgoing mail in post office collection boxes rather than an unsecured mailbox.
- Do not ignore unexpected mail from debt collectors or creditors. They could be alerting you to a fraud problem.
- When choosing personal identification numbers (PINs) do not choose obvious numbers (date of birth, street number, etc.).
- Shield the entry of your PIN number while at an ATM or store checkouts to prevent “shoulder surfers” from obtaining your PIN.
- Review account statements upon receipt. Report discrepancies immediately to the company that issued the statement.
- Contact your financial institution if you did not receive an expected monthly account statement.
- Cancel old, inactive accounts you do not currently use to prevent an unauthorized re-activation by a thief.

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.