Social Security Number Safety

If you suspect your SSN has been misused, act quickly by following these key steps:

1. **Contact the Federal Trade Commission (FTC):** Visit IdentityTheft.gov to report the theft and create a personalized recovery plan.
2. **Notify the IRS:** If your SSN has been used for tax fraud, visit the IRS Identity Theft Central or call their support line for help.
3. **Report to the Social Security Administration (SSA):** File fraud reports at oig.ssa.gov or call 1-800-269-0271.
4. **Place a Fraud Alert:** Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion). A fraud alert requires lenders to verify your identity before opening new accounts.
5. **Freeze Your Credit:** This prevents new creditors from accessing your credit file, blocking fraudulent account openings. You can unfreeze your credit when needed.

The SSA and cybersecurity professionals recommend taking the following steps:

- Never carry your Social Security card or share your SSN publicly unless absolutely necessary.
- Be cautious of phishing scams and verify email senders before clicking on links or attachments.
- Monitor your credit and create a “My Social Security” account at SSA.gov.
- Use SSA’s electronic access block to prevent changes to your online account.
- Consider SSA’s direct deposit fraud prevention block to stop unauthorized updates to your payment information.

Free Dark Web Scan:
https://www.experian.com/protection/free-dark-web-email-scan/

https://scan.aura.com/

https://www.keepersecurity.com/free-data-breach-scan.html

https://haveibeenpwned.com/