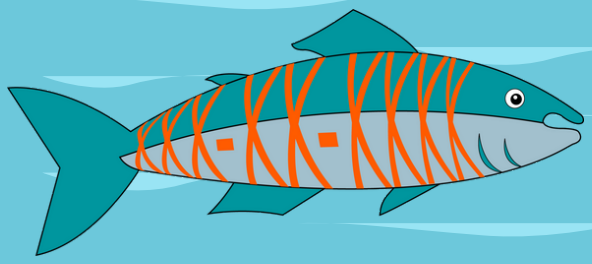

SAMMY SOCIAL

Protect your SSN from Phil!

Educate Yourself on Phishing Techniques

Stay informed about the phishing tactics Phil uses such as fake emails, texts, messages, or phone calls.

Be Skeptical of Unsolicited Requests

Never give out your Social Security Number (SSN) in response to unsolicited emails or messages. Verify the source before sharing any confidential information. No legitimate organization will ask for your fill SSN if they already have it.

Utilize Best Cybersecurity Practices

Use official websites; look for https:// in the URL. Use two-factor authentication on accounts that store your SSN for an extra layer of security. Use strong and unique passwords.

Limit Sharing and Monitor Accounts

Only provide your SSN if absolutely necessary. Ask if it can be omitted or substituted with a different identifier. Regularly monitor bank and credit accounts and look out for unauthorized transactions or changes.

Report Suspicious Activity

If you receive a suspicious email, call, or message requesting your SSN, report it to the appropriate authorities, such as the FTC.

RESOURCES

- ssa.gov/scam
- usa.gov/identity-theft
- ftc.gov

cyberhouserock.info