

Social Security Column

HOW TO SPOT A SCAM

By Earth M. Nieves

Social Security Public Affairs Specialist of Southern NJ



Now is the perfect time to protect yourself from scams that can damage your finances and reputation. We can work together to keep your personal information safe!

Stay informed of the latest scam trends

Fraudsters continue to change their tactics. Make sure you understand the latest scam trends at www.ssa.gov/scam. Stay informed by:

- Following reliable news sources.
- Subscribing to scam alert newsletters.
- Staying connected with your local law enforcement agencies.

The more you know, the better prepared you'll be to identify and avoid scams.

Think carefully before sharing personal information

Phishing is one of the main ways that scammers attempt to trick people into providing personal information. Pay close attention to emails or messages asking for your username, password, or other personal information.

Scammers pretend to be from familiar organizations to gain your trust. Stay alert when receiving calls that you did not request claiming to be from banks, government agencies, or other well-known companies.

When in doubt, contact the organization directly through official channels to verify that the request is real before sharing any personal information or making payment.

Use strong passwords

Create strong, unique passwords like a phrase with upper and lowercase letters, numbers, and special characters. Don't use passwords that are easy to guess like birthdays or names.

Consider using a password manager to generate unique passwords and securely store them for each of your online accounts.

Be savvy with QR codes

QR codes are increasing in popularity. They're in restaurants, on parking meters, in emails, and on social media.

Scammers have noticed! They are physically placing fake QR codes on top of official ones or creating fake QR codes on social media advertisements to get access to your personal information.

Never scan random QR codes. If the QR code looks odd or altered, do not scan it.

Protect your social media profiles

Take a moment to review the privacy settings on your social media platforms and limit the amount of personal information you share publicly.

Fraudsters may use your social media posts to personalize scams or get access to your accounts without your permission. Regularly check your friends list and remove any unfamiliar or suspicious accounts.

This month, let's make protecting ourselves against scams a top priority. We can significantly reduce the risk of being scammed by staying informed, being alert and careful, and safeguarding our accounts.

We invite you to watch our video at www.youtube.com/watch?v=cyaUWTFLw3c to learn how to identify the red flags. Please share this information with those who may need it – and post it on social media.

###