

## **New Year, New You, Same Scams**

As we bring in the new year with resolutions and aspirations, it's crucial to remain vigilant against scams that target the enthusiasm of embracing a "New Year, New You" mindset. From enticing shopping deals to subscription traps, scammers are adept at exploiting the desire for self-improvement. Here are some details to help you recognize and avoid common scams you could be approached by in the new year.

## **Popular New Year Scams:**

- **Fake Wellness Products:** Scammers capitalize on health-related resolutions by promoting fake or unverified wellness products.
- **Bogus Gym Memberships:** Fraudulent fitness centers may offer irresistible New Year discounts, only to disappear with your money. Research and choose reputable (local) gyms with a proven track records.
- **Subscription Traps:** Some scammers lure individuals into free trial subscriptions that later turn into expensive recurring charges. Always read the fine print before signing up for any trial offers.
- **Phishing Emails and Texts:** Be wary of unsolicited messages claiming to offer exclusive New Year discounts or personalized resolutions. Clicking on links in these messages could lead you to a phishing site or even install malware on your device.

## **Red Flags to Watch For:**

- **Too Good to Be True Offers:** Be skeptical of deals or products that promise extraordinary results or amazing discounts. Verify the legitimacy of offers before making any purchases.
- **Unsolicited Communication:** If you receive unexpected emails or texts promoting New Year deals, especially if they request sensitive information or immediate action, it's likely a scam.
- **Hidden Fees in Subscriptions:** Read the terms and conditions of any subscription or trial carefully to uncover hidden fees or auto-renewal clauses that could catch you off guard in the future.

## **Tips to Avoid New Year Scams:**

- **Verify Sellers and Brands:** Research unfamiliar brands or sellers before making any purchases. Look for reviews and ensure they have a legitimate online presence.
- **Use Secure Payment Methods:** Always opt to use secure payment methods when making online purchases. Avoid sharing sensitive information via unsecured channels as this could lead to a compromise of your sensitive information.
- **Read the Fine Print:** Before subscribing to any service or purchasing a product, thoroughly read the terms and conditions to understand the full scope of their commitment.
- **Stay Informed:** Keep yourself informed about popular scams and regularly check official sources for updates on the latest tactics scammers are using.