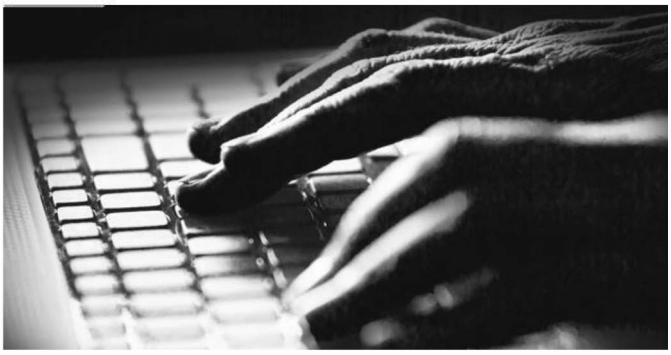
Top 10 Mass-Marketing and Identity Theft Frauds

Homeland Security Investigations

Financial Fraud

Knowing how to spot a Fraud is best way for consumers to protect themselves.



#1 Arrest Fraud: Callers claiming to be from a government agency state that the consumer will be arrested for failing to pay taxes or a fine; but they can avoid arrest by paying over the phone with a prepaid debit card or wire transfer.
Recommended Action: Hang up and contact the agency directly using a phone number from an independent source, such as a past bill or online search.

#2 Business-to-Business Email Fraud: An email is received from a high-level executive in a company purporting to authorize payment for a seemingly legitimate purpose. Actually, this scammer email address is very similar to the legitimate executive's email.
Recommended Action: Before initiating any payments, follow up directly with the executive using a known email address or phone number.

#3 Reverse Mortgage Fraud: Callers offer home refinance assistance that sounds too good to be true.
Recommended Action: Always seek out your own mortgage counselor and refuse to sign anything that you do not fully understand without an attorney present.

#4 Tech Support Fraud: A pop-up window appears that looks like an error message from your operating system or antivirus software. The pop-up warns of a security issue on your computer and directs you to click on a link for assistance.
Recommended Action: Never click on pop-up links. Contact the operating system or antivirus company directly for tech support using the number on their website.

#5 Money Mule Fraud: Emails direct you to move money from your personal bank account for purposes that seem legitimate.
Recommended Action: Always be wary of emails requesting access to your bank accounts. Look for warning signs and conduct your own research before agreeing to participate. Notify the appropriate authorities if you have any concerns.

Homeland Security Investigations

#6 Door-to-Door Fraud: Door-to-door salesperson visits sometimes wearing realistic uniforms / badges.
Recommended Action: Make it a policy to never buy products or services from door-to-door salespeople. If you do decide to make a purchase, contact the company directly to verify the salesperson's credentials.

#7 Medicare / Healthcare Fraud: Alleged Medicare representatives call asking for your Medicare or Social Security number. The fraudster then bills Medicare for products or services that you never received.
Recommended Action: Never provide personal info over the phone, unless you verify the caller's credentials. Review your Medicare Summary Notices for errors and report suspicious behavior to the Medicare Fraud Tip Line at 1-800-HHS-TIPS.

#8 Telephone Fraud: Callers pitch an "unbelievable" opportunity. All they need from you is your personal information.
Recommended Action: Never provide personal info over the phone. Hang up and do not press any buttons on your phone when you receive a robocall. Do not pick up or return a call that appears on the caller ID to be coming from your own phone number.

#9 Romance Fraud: Romance scammers contact their victims through online dating websites or social media. The scammer's intent is to establish a relationship with the victim and use that relationship to dupe them out of money, usually for an "emergency."
Recommended Action: Always be wary about the personal info that you post. Assume that con-artists are trolling even the most reputable sites. If you develop a romantic relationship with someone you meet online, research their identity and be suspicious of any requests for money or personal info.

#10 Sweepstakes Fraud: You are notified that you have won a contest or the lottery; but to claim your prize you first must pay fees or taxes. **Recommended Action:** No real lottery or sweep-stakes will ever request money in advance. Do a quick internet search to verify a sweepstakes if you are concerned about it's legitimacy.