

WHAT TO DO:

1. Stop. Think. Be skeptical. Do not be pressured into making hasty decisions and check things out before you buy or sign anything right away.
2. Exercise due diligence in selecting investments and the people with whom you deal with. Make sure you fully understand the investment before making the investment. Beware of testimonials which you have no way of checking.
3. Always get information in writing before you give away any money. Take time to do careful research. Remember, if it sounds too good to be true, it's probably a lie.
4. Check out the investment company through some independent agency to make sure it is legitimate. Never invest what you cannot afford to lose.
5. Never send money to pay for taxes/fees/prepaid cards on domestic/foreign text or lottery winnings, which you did not join. Legitimate promos use only 3 or 4 digit phone numbers.
6. Do not be fooled by the promise of large sums of money for your cooperation. Safeguard your personal information. Don't give out private information unnecessarily. As soon as you are convinced that your identity has been compromised, report it to your bank/credit card issuer immediately.
7. Avoid disclosing personal or account details via phone unless you are absolutely certain that the caller has a bona fide need to know. Never respond to scam emails requesting personal details. Delete suspicious emails or email attachments without opening them, even if they seem to have originated from someone you know. Notify the sending company if you receive a suspicious email.

8. Do not click on web links embedded in emails or pop-ups in unfamiliar web sites. Instead, type the URL (e.g. www.pinoycompany.com) or the company requesting for the information.
9. Keep an eye on your credit card every time you use it. Make sure you get it back as quickly as possible. Make sure you shred old receipts and billing statements and destroy old cards properly.
10. Stay calm. Do not immediately follow instructions coming from a stranger for any demand of money or valuables, in exchange for a kidnapped relative or hospitalized family member. Verify first with other immediate family members the veracity of the call received.

*Developed by the Financial Literacy
and Advocacy Division
Financial Consumer Protection Department*

CONTACT INFORMATION

Financial Consumer Protection Department
Supervision and Examination Sector
Bangko Sentral ng Pilipinas
5th floor Multistorey Building
BSP Complex, A. Mabini St., Malate
1004 Manila

Trunkline: (632) 708-7701 local no. 2584
Direct line: (632) 708-7087
Email Address: consumeraffairs@bsp.gov.ph

Financial Education: Building Block
for a Stronger Economy

WATCH OUT FOR

FRAUD AND SCAMS




WATCH OUT FOR FRAUD AND SCAMS

Fraud is an act, expression, omission or concealment that deceives another to the fraudster's advantage¹ while scams are fraudulent business schemes to mislead/swindle/victimize a person or persons with the goal of financial gain².

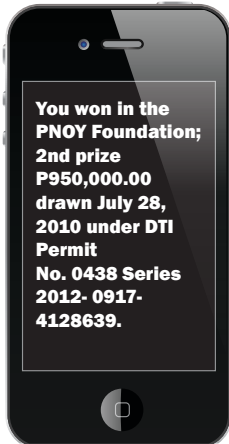
COMMON TYPES OF FRAUDS AND SCAMS

Text Scams

Fraudulent text messages stating that your mobile phone number won in a raffle contest either by a government institution or popular game show.

Sample text message usually say 

To claim the prize, the victim should transmit money to a designated bank account or through a remittance company to pay for taxes and/or remittance fee or send prepaid cell phone load to the scammers' prepaid mobile phone numbers.



Credit Card and ATM Skimming

Illegal copying of information from the magnetic strip of the credit card or ATM through a skimming device. Scammers use the information stolen to: access somebody's account; manufacture counterfeit cards or use in online transactions.

Your card may be skimmed if: (a) used on an ATM terminal with an attached skimming device or if (b) an employee of a gasoline station or a restaurant surreptitiously puts your card into an electronic skimming device.

Ponzi/Pyramiding Scheme

Ponzi scheme organizers lure prospective investors with high returns. The fraudsters normally exist for a limited period of time. They appear to be religiously paying their investors during initial stage. Thereafter, they will quickly disappear, leaving the investors, particularly those downlines, empty handed. The losing investors cannot run after the program managers who are either unknown or whose names and addresses, are usually fictitious.

¹ Source: <http://www.consumerfraudreporting.org/definition.php>

² Source: <http://www.consumerfraudreporting.org/definition.php>

Spurious Investments

Fraudulent commercial documents being sold or traded by individuals or companies and are allegedly issued, secured or guaranteed by the BSP or international banks.

Identity Theft

Fraudsters get the personal information they need to assume your identity through theft. With these information, the perpetrator causes the creation of a financial transaction, e.g., a loan, intermediary account or other financial account, in the victim's name.

Phishing

Emails from your bank or credit card company that looks like the "real thing" and asking for information like PIN, account number, log in IDs and passwords that can be exploited for fraudulent purposes. Phishing may be done using methods other than email. Mobile phone text messages, chat rooms, fake banner ads, message boards and mailing lists, fake job search sites and job offers, and fake browser toolbars may also be used to get information.

Spoofing

A website that appears to be legitimate but it is actually created by a fraudster. The main purpose is to trick the user into releasing sensitive information such as PIN, account number, log in IDs, and passwords that can be exploited for fraudulent purposes.

Nigerian Scams

Emails, fax or letter from strangers or even friends (subject of hacked emails).

These strangers will tell you that they have either large sums of money for remittance or a very good business offer and they need your account to bring the money to the country. They will ask you to either share your bank information or create an account with a particular bank/institution. With the bank information, they will draw up false instruments against your account.

Friends (whose emails have been hacked), on the other hand, will relate a sad story telling they are in need of emergency financial help. They will ask you to send money to a temporary account, which could be easily closed after receiving the money.

Budol-Budol Scam











Victim will be shown bundles of cash to get the victim's trust and then the scammer will ask for cellphone or other important things in exchange for the fake money. The scammer may also leave important things in exchange for cash. Hypnotism is also said to be used for this modus operandi.

Dugo-Dugo Scam

Victim receives a call from someone that a loved one has been kidnapped or has been hurt. The caller will tell the victim to make a money transfer to a stranger or ask for jewelries or other valuable items in exchange for the safety of the kidnapped relative or to pay for the medical expenses of the loved one.

SIGNS OF FRAUD AND SCAM

Be suspicious when:

-  You've been told of winning in a lottery or a raffle that you did not join;
-  You are told to act immediately or lose the opportunity;
-  You've been selected to receive a special offer, incentive or free gift;
-  You must pay for the shipping fee of your prize or gift;
-  You've been promised a high return without any risk or 100% guaranteed return on investment;
-  You've been asked to give through email your personal information such as bank account, credit card numbers, PIN and passwords;
-  The institution provides no written records or information of the transaction;
-  The institution is not registered with or is not regulated by any regulating body;
-  You were provided only with a mobile number as a contact information;
-  The offer provides testimonials that you have no way of checking out.