How to Prevent Financial Fraud

1. Voice Phishing and Some Common Characteristics
   1) Impersonation

      Scammers pretend to be government organizations such as the prosecutors' office, the police, an FSS employee, or an employee of a financial firm
   2) Psychological pressure

      Scammers apply psychological pressure by telling you made-up stories like, "Your information has been stolen," or "You are involved in a crime," or "Your child has been kidnapped."
   3) Manipulation of caller ID

      Scammers manipulate the caller ID on your phone to display the number of a financial company or a public institution so that their victims do not realize it is a phishing call.
   4) Fluent Korean speaking

      In the early days, scammers usually had an impediment in speaking Korean, but recently scammers are speaking in fluent Korean.
   5) Direct withdrawal/Transfer

      Scammers directly withdraw money from the victim's account using the victim's financial transaction information (account number, credit card number, internet banking information, telebanking information, etc.)
   6) Illegally acquired bank account

      A bank account obtained pretending to provide loans or offer a job is used for fraud.

2. Preventing Voice Phishing

1) You should never share your personal information.

If you are asked to provide your account number, credit card number, or internet banking information over the phone or to enter such information on a website because of personal information leakage or involvement in a criminal case, you should never share your personal information.

2) A caller who asks you to go to an ATM is voice phishing scammer.

It is a scam if the caller asks you to go to an ATM for refund of tax or insurance premium. Please keep in mind that you should never follow such a caller's instruction

3) Check whether it is true even when scammers call you with your personal and financial information transactions.

Recently, scammers might often contact you by obtaining your personal and financial transaction information in advance. In such cases, you should hang up and first call the institution where the caller claims to work and check whether the institution calls you or sends text messages or SMS.

4) If you become the victim, promptly request a suspension of payment.

If you fall to the victim of voice phishing, call the National Police Agency call center (☎112) or the call center of a financial firm to request suspension of payment of the damaged account promptly.

5) Note that caller ID (Phone number) can be manipulated

Even if you have signed up for the telebanking pre-designated number system (a system that allows you to use telebanking only with a specific phone number registered in advance), scammers may manipulate the caller ID using an internet exchange. You should not be deceived by the scammers who say "Don't worry, no one except you can use telebanking because you sign up for the telebanking pre-designated number system."

3. Be especially careful about personal information leaks.
    1) Do not disclose your account number, mobile phone number, name, passport number, or alien registration number to unspecified individuals.
    2) Do not disclose your friends' personal information to unspecified individuals without their consent.
    3) Be especially cautious when providing personal account information and real-name information. Since there are no officially registered currency exchange offices in Korea, always exchange money at a bank (extra caution!).