

GOVERNMENT UNVEILS PLANS TO ROOT OUT VISHING

The government unveiled its plans to root out vishing (or voice phishing) scams through close coordination between the financial, communications and investigative authorities on June 24.

BACKGROUND

The government has been pursuing policies to promote inclusive finance and human security along with innovation-led growth. The advancement in digital technologies has led to a rise in vishing scams using new and more sophisticated tricks and technologies. With the widespread usage of smartphones, illegitimate use of burner phones and apps has been on the rise as well. Vishing is a crime that brings ruin to families and undermines trust in our financial and telecommunications systems. With more sophisticated tricks and tools, it requires strong, comprehensive and persistent responses from the government.

KEY MEASURES

The government-wide collaboration in finance, communication and investigation will help strengthen vishing prevention measures from prevention to detection to punishment and in terms of assisting victims and raising public awareness.

I. DEVELOP COMPREHENSIVE PREVENTION SYSTEM

- Prevent the use of mobile phones in vishing scams
- Require financial companies to adopt Fraud Detection System (FDS) to closely monitor suspicious transactions linked to vishing, and have them utilize big data and AI to share information with relevant public institutions
- Strengthen duties and responsibilities of financial companies and telecommunications service providers in preventing vishing scams
- Prepare plans to improve the personal authentication and ID verification system in the third quarter
- Implement pilot projects and R&D to develop new digital technologies to be applied in vishing prevention

II. BOLSTER CRACKDOWN & PENALTY

- Strengthen crackdowns on financial scams including vishing: (a) set up close cooperation network with overseas investigative authorities while increasing crackdowns on smishing and other newly emerging types of fraud
- Make statutory punishment on vishing more severe

III. STRENGTHEN COMPENSATION REQUIREMENT OF FINANCIAL COMPANIES

- Establish basic principles on the responsibility of financial companies by having financial companies bare the compensation responsibility as long as there is no intent or negligence involved on the part of the consumer
- Have financial companies develop a variety of insurance products on vishing and allow consumers to sign up for vishing insurance at easily accessible locations, such as telecom vendors or bank branches

IV. MAINTAIN STRONG INTER-MINISTERIAL COOPERATION

- Support cooperation between financial companies and telecommunications service providers in providing call block services for overseas incoming calls and altered phone numbers
- Set up hotlines between Korea Internet & Security Agency, Financial Supervisory Service, investigative authorities and telecommunications companies to effectively respond to new types of vishing scams
- Detect and prevent false reports through close cooperation between law enforcement and financial companies

V. INCREASE PUBLIC AWARENESS

- Make more public service advertisements in public transports, telecom vendors and banks, and through TV broadcasts and Youtube channels
- Have financial companies make more announcements on their vishing prevention measures
- Send public alert text messages to provide information about widely used vishing tricks and to raise public awareness on vishing prevention

EXPECTATION

The comprehensive measures to root out vishing will help build a more accountable and trust-based digital economy, allowing individuals to use financial and communications services in a safer and more convenient environment.

Individuals should practice caution with private data and be well aware of the threat of vishing and other types of financial scams as well as of personal identity theft or malware infection using smartphones.

#

For any inquiry, please contact Foreign Press & Relations Team at fsc_media@korea.kr.