Ⅴ. Preventing Financial Fraud (1)

1. Telecommunication-based Financial Fraud

Today, financial fraud includes not only voice phishing using a phone, but also fraud using phishing sites that spread malicious code and attract people to fake Internet banking sites of financial institutions similar to the real site to steal bank account number, password, etc. As such financial fraud is subtly evolving in technique and types.

(1) Voice Phishing

Voice Phishing is a new compound word of voice, private data, and fishing. It is a special fraudulent crime committed in the financial sector that steals properties from other people by deceiving or lying to them. The term 'Voice phishing' was coined because fraud is collecting personal information over the phone.

(2) Messenger Phishing

Messenger phishing refers to fraud that logs in using another person's Internet messenger ID and password, and requests acquaintance such as friends or family members already registered to urgently send money required for medical expenses, traffic accident settlement, etc., through a conversation over the phone or note. If a victim is tricked into sending money, they take it.

(3) Phishing Site and Pharming

① **Phishing Site**: This is a compound word of phishing and site. It is a fake site made very similar to the homepages of banks and public institutions in order to steal financial transaction information. Fraudsters use phishing sites to induce people to disclose their financial transaction information.

② **Pharming**: fraudsterers first infect the user's computer with malicious code to modulate the host file or browser memory. If the computer use access the homepage using 'Favorite' menu or through portal site search, the user is led to the phishing site to disclose their financial transaction information (account password, security code number, etc.) to the fraudsters.

(4) Smishing

Smishing is a compound word of SMS and phishing. It is a new kind of financial fraud that first appeared in Korea in 2012. It is a fraudulent technique that causes micro payment damages by distributing malicious apps or malicious codes to mobile phones using text messages, intercepting mobile payment information, and purchasing game items from game sites.

More Information: Types of Smishing

◇ Fraudsters induce people to install malicious apps or malicious code that pretend to be the website of financial institutions by sending the Internet address through text messages. If the mobile phone user calls to the number displayed on the app, it is led to the phone of fraudster who requests remittances for various reasons (fees, etc.) or it is also led to phishing sites through malicious code.