## Common Frauds and Scams

Sophisticated technology allows clever thieves to commit financial fraud in ways never previously imagined. A con artist may call you posing as your banker, or send you correspondence that appears to be from your bank. These criminals infer that your account has already been compromised, and, as part of the bank's "investigation", ask you to provide sensitive personal and financial information. Contact your bank immediately to verify any unusual or suspicious requests.

Here are some tips to help you avoid financial fraud and scams:

1. .Avoid Internet chat rooms and never respond to an unsolicited email
2. Never be pressured to make an immediate decision
3. Never give personal or bank information to an unknown caller, regardless of who he or she claims to be. Don't give in to intimidation or threats.
4. Never pay for something merely because you'll get a "free gift".
5. Use caution when making a charitable contribution, verify the authenticity of the charity.
6. If the offer is an investment, check with your state securities regulator to see if it is properly registered.
7. Don't be fooled by claims of riches from foreign lotteries, sweepstakes, or contests. (Foreign lotteries are illegal!).
8. Beware of offers to help you recover money you may have previously lost
9. Be very cautious in Internet sales and purchases. If selling, clear the check before you send the item to seller. Never accept a check for more than the amount of purchase. The check will be counterfeit and/or worthless. This is the most common Internet scam.

If you believe you may have fallen victim to a scam relating your account with Nara Bank, call us immediately at 213-639-1700.

### Additional resources for consumers:

- National Consumer League's National Fraud Information Center www.fraud.org or 1-800-876-7060
- Annual Credit Report sponsored by the three major U.S. credit bureaus www.annualcreditreport.com or 1-877-322-8228
- www.lookstoogoodtobetrue.com. A website maintained by a joint federal law enforcement and industry task force.
- Better Business Bureau's Wise Giving Alliance www.give.org

## Identity Theft

**Every hour, 1,000 Americans become victims of Identity Theft. And that may be a low estimate. How can you protect yourself? Here are ten easy tips that will help you keep your finances secure.**

1. Place your **outgoing mail** in a secure, locked mailbox.
2. Retrieve your **incoming mail** immediately upon delivery, or use a U.S. Post Office box.
3. Never leave your **purse or wallet** unattended - even for a moment.
4. Guard your **Social Security Number**. Do not use it as your Driver's License number and never give it out unless absolutely necessary (such as for banking business).
5. Memorize your **passwords and PINs** - don't carry them with you.
6. Beware of **fraudulent callers**. Never give your Social Security number, account numbers or any personal information to anyone who calls you. There are numerous scams where callers identify themselves as your bank, credit card company or a fraud investigation firm trying to help you.
7. **Shred** receipts, bank statements, pre-approved credit card offers and convenience checks.
8. Carefully review all **bank statements**, credit card statements and bills.
9. Order your **credit report** annually (visit www.annualcreditreport.com or call 877-322-8228). Review to ensure all the information is correct, especially your name, address, and Social Security number. Look for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause.
10. Report **lost or stolen checks** to your bank and law enforcement immediately.

**At Nara Bank, we're committed to fighting ID Theft. We help catch and prosecute these criminals. For more tips on how to fight financial fraud, contact us or visit the Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft**

## Computer Security

**Account hijacking occurs when a criminal obtains your personal banking information and uses it to take over your bank accounts. An estimated 2 million people are hit with account hijacking each year. Follow these suggestions to help reduce your risk of account hijacking.**

1. When conducting business online, use a **secure browser** that encrypts or scrambles purchase information and make sure your browser's padlock or key icon is active.
2. Be savvy with your **password**. Experts advise a combination of letters and numbers...and avoiding pet names, your home address, and similar easy-to-crack codes.
3. If you receive an **unsolicited email**, or one that you consider suspicious, delete it. Remember: your bank will never email you and ask you to go to another site to "verify information."
4. Install **anti-virus software**. Your computer's anti-virus software is like a vaccine - it works at first, but you need to keep it up-to-date to guard against new strains.
5. Use a **firewall**. This protective wall between the outside world and your computer can help prevent unauthorized access to your computer. Updates are called patches, and you should check regularly with your software company to be sure you have the latest patches.
6. Install **anti-spyware software** and update it regularly.
7. Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send **programs of unknown origin** to your friends or coworkers simply because they are amusing -- they could contain a virus program.

For more information on computer security, visit www.cert.org/tech_tips/home_networks.html

## 금융/신용사기의 유형

기술의 발달로, 예전에는 상상도 하지 못하였던 지능적인 금융관련 사기사건들이 많이 늘어나고 있습니다. 사기범들은 은행원을 가장하여, 고객들에게 전화를 하기도 하고, 은행으로 부터 보내진 것 처럼 위장하여 편지나 이메일을 보내기도 합니다. 이때 마치 고객계좌의 개인정보가 이미 누출된 것처럼 가장하고, 조사를 한다는 명목으로 고객의 계좌정보나 다른 매우 중요한 개인정보을 알아내려하고있습니다. 의심스럽거나 통상적이지 않은 상황에는 반드시 은행으로 연락하여 확인하셔야합니다. 고객님께서 금융사기등 불이익을 피하는데 도움이 될 수 있는 몇가지의 방법들을 나열하였습니다.

10. 알지못하는 곳으로 부터 온 이메일에 답변을 하지마시고, 인터넷 채팅을 피하십시오.
11. 절대로 바로 무슨 결정을 해야된다는 부담을 갖지 마십시오. 시간을 갖고, 다른 사람에게 물어보고 결정을 할 수 있도록 충분한 시간적 여유를 갖으십시오.
12. 은행계좌관련 혹은 다른 개인정보를 알지 못하는 사람 (은행원이나 다른 누구라고 사칭하더라도) 에게 절대로 알려주지 마십시오. 겁을주거나 당황하게 할지라도 절대로 넘어가지 마십시오.
13. "공짜선물" 이나 "상금" 을 타게되었다고 유혹하며 얼마간의 돈을 요구하는 경우 절대로 아무것도 지불하지 마십시오.
14. 비영리기관에 기부금을 낼때 그 기관이 정당한 곳인지 잘알아 보고 조심하여 지불하시기 바랍니다.
15. 투자 권유를 받는 경우, 투자전 주정부의 유가증권 감독기관과 확인하여 등록된 투자기관인지 확인하시기 바랍니다.
16. 외국복권이나, 추첨에 당첨되어 큰돈을 받게 되었다는 등의 허황된 속임수에 넘어가지 마십시오. (외국복권은 불법입니다.)
17. 이전에 손해본 돈을 찾아주는 것을 돕겠다고 하는 제의에 주의하십시오.
18. 인터넷상에서 무엇을 사거나 파실때 매우 조심을 하여야 합니다. 파실때는, 물건을 보내기전 받은 수표가 확실히 결재될때 까지 기다리셔야 합니다. 절대로 물건값보다 더 큰금액의 수표를 받지 마십시오 (더 큰 금액의 수표를 보내놓고 차액을 송금하라고 지시하곤 합니다.) 만일 받으신 수표가 가짜이거나 불법적으로 발행된 것이라면 결재되고 난 후에도 부도처리될 수도 있습니다. 이방법이 가장 흔한 인터넷상사기의 종류입니다.

만일 고객님께서 나라은행계좌 관련된 사기범죄에 피해를 당하셨다면 바로 저희에게 (213 -639-1700) 알려주십시오.

### 소비자 정보를  제공하는 곳들

- National Consumer League's National Fraud Information Center www.fraud.org or 1-800-876-7060
- Annual Credit Report sponsored by the three major U.S. credit bureaus www.annualcreditreport.com or 1-877-322-8228
- www.lookstoogoodtobetrue.com. A website maintained by a joint federal law enforcement and industry task force.
- Better Business Bureau's Wise Giving Alliance www.give.org

## 신분 도용(Identity Theft)

**매시간 1,000 명의 미국인들이 신분도용의 피해자가 되고 있습니다.  아마 이 숫자는 최저예상치일지도 모릅니다.  어떻게 고객님 스스로 보호를 하실 수 있을까요?  고객님의 신분도용 방지와 금융관련 신분보안을 위해 다음과 같은 10 가지 쉬운 방법을 참고하십시오.**

11. 우편을 내보내실때 우체국 우체통을 이용하거나 잠금장치가 되어있는 우편함을 사용하십시오.
12. 우편물을 받으셨을때는 빨리 꺼내시거나, 혹은 우체국 사서함을 이용하십시오.
13. 절대로, 잠시일지라도, 지갑이나 가방을 고객님이 보지않는 곳에 방치하지 마십시오..
14. 소셜번호 보관을 철저히 하십시오. 은행계좌를 여는등 반드시 필요할때 사용하는것 외에는, 신분증처럼 사용하거나, 남에게 알려주거나, 아무데나 놔두지 마십시오.
15. 컴퓨터에 사용되는 비밀번호등은 기록하여 놓지 마시고 기억하여 사용하시기 바랍니다.
16. 사기범들의 전화를 조심하십시오. 전화를 걸어온 사람, 혹은 전화를 걸라고 요구한 사람에게 소셜번호나 계좌번호, 혹은 개인정보를 주지 마십시오. 연방보험국을 사칭하거나,  은행원이라고 하거나, 크레딧카드 회사라거나, 사기사건을 조사하는 기관이라면서 개인정보를 빼내어 벌이는 사기범죄가 많이 일어나고 있습니다.
17. 영수증, 은행 스테이트먼트, 사전승인된 크레딧카드 신청서, 혹은 카드회사나, 모기지회사로 부터 우송되어오는 임시사용 수표등은 은행계좌번호, 카드번호, 개인신분에 대한 많은 정보를 담고 있습니다. 잘 찢어서 정보들이 보이지 않게해서  버리시기 바랍니다.
18. 은행 스테이트먼트, 카드사용명세서, 고지서등를 항상 잘 살펴보십시오. 사용하시지 않거나 잘못 된 내역에 대해 배상받을 수 있는 기간이 정하여져 있으므로, 더큰 피해 방지를 위해 정기적으로 살펴보시는 것이 매우 중요합니다.
19. 크레딧리포트를 일년에 한번씩은 신청하셔서 (visit www.annualcreditreport.com or call 877-322-8228) 신용기록이 정확한지, 특히 이름, 주소, 소셜번호등이 정확하게 기재되었는지, 다른 번호나 다른 이름 다른 주소가 기재되어있지는 않은지 살피시기 바랍니다. 혹 본인이 하지 않은 신청기록, 낯선 채무기록이 있는지, 알지 못하는 신용기록 조회내역, 채무불이행, 혹은 지체된 지불등이 있는지도 살피십시오.
20. 수표분실, 도난을 당하셨다면, 경찰과 은행으로 신속히 신고하시기 바랍니다.

**나라은행은 신분도용범죄퇴치를 위해 최선을 다하고 있습니다. 이런 범행들을 찾아내고 잡을 수 있기위해 노력하고 있습니다.  금융사기에 대한 더 많은 정보를 원하신다면,  Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft 을 방문하시기 바랍니다**.

## 컴퓨터의 보안장치

**사기범들은 고객님의 개인정보를 입수하여 은행계좌들을 탈취하여 자기들의 계좌처럼 사용하여 잔고를 다 빼가거나 다른 정보들을 입수하는데 사용합니다.  이와같은 수법으로 매년 약 2 백만명이 계좌를 탈취당하고 있습니다.  계좌탈취의 위험을 방지하는데 도움이 되는 몇가지를 아래와 같이 소개해드립니다.**

8. 기업용 거래로 인터넷을 사용시에는 암호화 되었거나 철저히 보안장치된 브라우져를 사용하여야 하며, 브라우져의 잠금장치가 작동하는지 확인하여야 합니다.
9. 비밀번호 (Password)  를 너무 쉽게 만들지 마십시오.  전문가들은 글자, 숫자, 부호를 섞어서 만들기를 권유하고 있습니다. 또한 소지하고 있는 애완동물의 이름, 집주소 등 쉽게 알아낼 수 있는 비밀번호는 피하라고 권고하고 있습니다.  비밀번호를 공유하여 서로 같이 사용하는 것을 금하여야 하며, 정기적으로 바꾸게끔 하여야 합니다.
10. 잘 모르는 곳으로 부터 받은 이메일이나, 혹은 의심스럽다고 여기는 이메일은 컴퓨터에서 지워 버리십시오. 은행은 고객님께 고객님의 신상정보를 확인하기 위해 다른 웹페이지로 접속하시라는  이메일을 보내지 않는다는 것을 기억하시기 바랍니다.
11. 안티바이러스 프로그램을 반드시 설치하십시오. 컴퓨터에 설치된 안티바이러스 프로그램은 면역주사와 같아서 첫번째 발병시에는 면역역할을 할 수 있지만, 새로운 바이러스에 지속적으로 대항하기위해서는 항상 최근것으로 바꾸어 주셔야 합니다.

12. 방어벽 (firewall) 을 이용하십시오. 외부와 고객님의 컴퓨터 사이에 설치된 방어벽은 고객님의 컴퓨터에 허락되지 않은 외부로 부터의 접속을 막는데 도움을 줄 수 있습니다. 최근것으로 바꾸어주는 것을 패치라고 하는데, 프로그램 회사와 정기적으로 확인하여 항상 최근 패치가 설치되어 있도록 하여야합니다.
13. 안티스파이웨어를 설치하고, 정기적으로 최근것으로 바꾸어 주어야 합니다.
14. 확실하고, 확인되지 않은 프로그램은 절대로 사용하면 안됩니다. 단순히 흥미롭다는 이유로 알지못하는 곳으로 부터 들어온 프로그램을 다른사람에게 보내지 말아야 합니다. 바이러스 프로그램일 수도 있어서 본인의 컴퓨터 뿐 아니라 다른사람들의 컴퓨터까지 바이러스를 전염시킬 수 있기 때문입니다.

컴퓨터 보안에 대한 정보를 원하시면 www.cert.org/tech_tips/home_networks.html 로 방문하십시오.