

HOW TO AVOID THE SWINDLE

- Never provide personal information such as social security, credit card and bank account numbers to anyone over the phone, especially if they called you.
- Beware of anyone who wants you to wire money instead of sending a check.
- In most scams, if you are given a phone number to call, it's probably a disposable — and untraceable — cell phone.
- If you're not sure of the legitimacy of an Internet message from your financial institution, contact the business by some means OTHER than the instructions given on the Internet.
- Review credit account statements regularly to ensure all charges are correct and that there aren't purchases you didn't make.
- Do not be intimidated by any messages that suggest dire consequences if you do not immediately provide or verify financial information.
- Legitimate lotteries and sweepstakes do not require you to pay something upfront or to buy something to improve your chances of winning.
- Sponsors of legitimate contests will readily identify themselves and will send you information if you ask.
- Fraudulent e-mail or fax scams will most likely contain spelling errors and poor grammar.
- Scammers will try to convince you that they are not out to rip you off and might claim that they are working in your best interest.
- Some scammers will become pushy and nasty on the telephone if you resist their offers. Hang up on them.
- Do not rush into making important financial decisions just because you are told that if you don't act NOW the offer will be withdrawn.
- Watch out for phony charities using names that sound a lot like legitimate charities.
- If an offer purports to offer something "for free", it might end up costing you a lot.

REPORTING FRAUD

- If you have disclosed sensitive information in a phishing attack, you should contact one of the three major credit bureaus and discuss whether there's a need to place a fraud alert on your file. This will help prevent thieves from opening a new account in your name. The major credit bureaus can be reached at:
- Equifax
P. O. Box 740250
Atlanta, GA 30374
1-800-525-6285
- Experian
P. O. Box 1017
Allen, TX 75013
1-888-397-3742
- TransUnion
P. O. Box 6790
Fullerton, CA 92634
1-800-680-7289

If you haven't already done so, consider signing up for the **Do Not Call Registry**. Once you are on the national list, telemarketers (with a few legitimate exceptions) are not supposed to call you. You can register via the Internet with the Federal Trade Commission or by calling 1-888-382-1222.

If you receive a visit from someone you think might be a scam artist and would like an officer to respond, call (309) **820-8888**. If you have general questions about e-mails, faxes or phone calls, contact the Bloomington Police Department Public Affairs Unit at (309) 434-2355 or (309) 434-2534. Public Affairs can also be contacted by e-mail at police@cityblm.org.

The FBI/Internet Fraud Complaint Center can be reached at 1-800-251-3221 or at: www.ic3.gov.

The Federal Trade Commission can be reached at: www.consumer.gov or at 1-877-IDTHEFT.

CONS, FRAUDS AND SCAMS



**Bloomington Police Department
305 S. East Street
Bloomington, Illinois 61701**

**Public Affairs Unit
(309) 434-2355
(309) 434-2534
police@cityblm.org**

DEFINITIONS*

Con: Something (as a ruse) used deceptively to gain another's confidence; swindle

Fraud: Intentional perversion of the truth in order to induce another to part with something of value or to surrender a legal right

Scam: Fraudulent or deceptive act or operation

**Merriam-Webster Online*

Cons, frauds and scams can occur over the telephone, through the mail, over the Internet or in person. No one would fall for a scam if it looked like a scam, so perpetrators are very careful to make their con games appear legitimate. Criminals tend to look for easy targets. You can take a few precautions to make yourself a harder target. A good place to start is to heed this advice: ***"If it appears too good to be true, it probably is!"***

Many of the most modern scams, especially those that use the Internet, originate in foreign countries and are virtually impossible to solve. It is also very difficult to identify and prosecute the scammer. Much more certain is the fact that most people who fall victim to them never recover their losses.

NIGERIAN SCAM

It's an old one, but it continues to circulate. You get an e-mail, letter or fax from someone purporting to be a government or business official stating that he has millions of dollars that can not be accessed because of "rules and regulations" in his country, usually in Africa. He wants you to help transfer the money to the U.S. (to your bank account) and for your trouble, he'll give you a big chunk of the money. **What he really wants is your account number so he can raid your account.** Most often, you are asked to transfer (by wire as opposed to sending a check) money to cover all sorts of things, such as paying off government officials, having documents certified or hiring a courier service. You are also asked to keep the plot a secret. People who fall for this scam never see their money again and the promised bounty never existed in the first place.

"PHISHING" SCAM

You receive an e-mail or a "pop-up" window on a website that appears to come from a reputable company. In many phishing scams, it often appears to be the financial institution with which you do business. In other cases, the message appears to come from a government agency or from a well-known credit card company. The message warns of a serious problem that requires your immediate attention. You are then instructed to click on a button to go to the institution's website. In reality, you are being directed to a phony website that may look very legitimate. The fraudulent website instructs you to enter personal and account information in order to "verify" the account. Often, the instructions will be accompanied by a threat that failing to comply will result in suspension of the account. Information provided is used by the scammer to make purchases or open new accounts in your name. **Legitimate businesses will never use the Internet to obtain personal or private information.**

"VISHING" ATTACKS

Vishing is similar to phishing in that consumers are persuaded to divulge personal or private information for the purpose of identity theft. Vishing involves e-mails or text messages, supposedly from a financial institution or credit card company, directing you to a telephone number to re-open your account or reactivate your credit card. Upon making the call, the recipient is greeted with "Welcome to the Bank of..." (the same one they mentioned in the e-mail or text message!) and instructed to provide card numbers and other personal information. The frauds even make their e-mails appear more authentic by advising recipients to never provide sensitive information when requested to do so in an e-mail. **Always call financial institutions or credit card companies using a number you obtained yourself or the one on your monthly statement.**

"BOT-HERDING"

Some computer hackers aren't satisfied stealing from one user at a time. They prefer to direct the unsuspecting to phony web sites or links within e-mails that will allow the hacker to gain control of hundreds or thousands of computers across the country. By going to the phony web site or clicking on the links (for electronic greeting cards, for example), users unknowingly release malicious software onto their computer. The hacker then uses that computer and many others to create a "botnet", a remote-controlled robot network that can be used to launch massive spam campaigns, cripple legitimate computer networks, or steal identities. Many times, computer owners don't even know their computer has been infected. **Do not open unsolicited e-mails, especially those with attachments. Maintain current virus protection programs on your computer.**

LOTTERY/CONTEST SCAM

It begins with a letter, phone call or e-mail claiming you have won a lottery or contest. You are told to contact a claims agent to collect your "winnings", using a telephone number or e-mail address. The claims agent sends you a form to return, along with copies of your driver's license, passport and/or other documents to "verify your true identity". Often, you are also instructed to wire (again, as opposed to sending a check) money to cover taxes and fees. **The scammers now have some of your hard-earned money (which you will never see again) and enough personal information to steal your identity.** Sometimes, you will actually receive a check, but it will be counterfeit and have no value. You will be promised more checks, but they will also be phony, if they arrive at all. In addition, your financial institution might hold you responsible for any cash taken by you when depositing the worthless check(s). Keep this advice in mind: ***"If you did not enter a lottery or contest, how could you win?"***