

protect yourself against frauds & scams

identity theft/fraud

- Shred anything that has personal information.
- Always check your bank statements, and credit card statements.
- Watch for all bill statements. If you do not receive one, CALL the company.
- Do not respond to any unsolicited e-mails, or phone calls. If someone calls and is requesting information from you, get their name and the department and call them back from a phone number you have or can get from the phone book or Google. DO NOT take a phone number they give you.
- Do not give out personal information to anyone that you have not initiated the call.
- Check your credit report every year. You may receive 1 free report each year from each reporting agency. Space them out throughout the year so that you are watching your account throughout the entire year.
- Guard your credit cards, ATM/Debit cards. Be aware of people around you when you are using one of these cards.
- Use caution with Internet purchases. If you receive a return e-mail after you have just made a purchase wanting you to verify personal information - do not give it. You should be able to forward that e-mail to the "real" company for verification.
- Use credit cards instead of debit cards for Internet purchases.
- Do not give anyone access to your Debit/ATM card and DO NOT give anyone your PIN.

if it happens to you...

Bank Accounts

Contact your bank as soon as you notice anything that does not look correct. This could be an unauthorized ACH withdrawal, Debit/ATM withdrawals you did not do, or checks that you did not write. The Bank will usually require you to close your account, complete appropriate affidavit documents, and you will need to file a police report.

Credit Card or Credit Report

Place a fraud alert on your credit report. Close the accounts that you know or believe have been tampered with or opened fraudulently. File a complaint with the Federal Trade Commission. File a report with your local police or the police in the community where the identity theft took place.

helpful websites

www.annualcreditreport.com
www.transunion.com
www.equifax.com
www.experian.com
www.ftc.gov
www.illinoisattorneygeneral.gov

frauds and scams

Organized crime groups in Nigeria employ hundreds of people who work long hours in public Internet cafes scamming US citizens. These groups are pulling in millions of dollars annually from unsuspecting victims overseas.

Before the “tech” age these groups would run their scams by contacting individuals by letter or fax. Now with the availability of computers and Internet access, things have just gotten easier for them.

The scams are not just limited to Nigeria any longer; they have now branched out to other parts of the world such as the UK, Canada and Jamaica.

The largest risk to individuals, businesses and banks as far as fraud loss is the Counterfeit Check scams. These counterfeit checks are received in a variety of ways, victims negotiate them, the checks are then returned to the paying bank unpaid as counterfeit fraud items. The responsibility of these items ultimately falls on the individual that negotiated it.

scams

Nigerian 419 Scam: This is actually the original scam which most of the others have been developed from. It involves the victim receiving a letter, fax, or e-mail from someone that claims to be a high level government official from a foreign country, commonly Nigeria. Sometimes the scammer will claim to be the wife of a high ranking official who has been assassinated or has died. They will deliver a variety of stories from needing assistance fleeing the country, to wanting to invest in the US. They will say that they need the assistance of someone with a bank account in the US to help them get the money into the country in exchange for a percentage of the money. They will then typically send a check to the victim that they instruct them to cash or deposit and then wire the money by Western Union or Money Gram. The check is a counterfeit and the victim is out the funds.

Lottery/Sweepstakes Scam: This seems to be the most popular one seen. Victims will receive a letter or e-mail that they have won a lottery or sweepstakes. In the letter the victim is sent a check telling them that they need to cash or deposit the check and then wire the money by Western Union or Money Gram to pay for taxes and fees associated with collecting the rest of the prize money.

The letters will typically include a contact phone number and a person's name to call, which of course is the scammer himself on a non-traceable cell phone who is safely outside the US. Many time the letter does not instruct the victim to wire the funds, it will just tell the victim to cash or deposit the check and then to contact them immediately afterwards, at that point the victim will be instructed to wire the funds. The check is a counterfeit and the victim is out the funds.

Inheritance Scam: With this scam the victim is notified usually by email or letter informing them that they are the only survivor of a long lost relative, usually in a foreign country, that has died or been killed and they are now the sole heir to the deceased fortune. Once again they will have a variety of different scenarios where they ultimately will send them a check that they will need to cash or deposit and then wire the funds back to help pay for lawyer fees, taxes, whatever the scenario they have come up with. The check is a counterfeit and the victim is out the funds.

scams (cont.)

Work From Home Scam: The work from home scam is usually found on Want Ads in the papers and job sites on the Internet. The scammer will tell the victim that they are a foreign company that needs help in collecting funds on their accounts from their US clients. The victim is told that all they need to do is receive checks in the mail, deposit them into their account, keep a percentage for themselves and wire the remaining funds to their “employer”. The checks are all counterfeit and the victim is out the funds.

Mystery Shopper Scam: This scam is similar to the Work from Home Scam. The victim is asked to visit a variety of stores and evaluate the customer service, or the displays, or the store in general. The victims are urged to keep their job a secret from anyone, and are sent a check to use for their transactions and to wire the largest portion back by Western Union. The checks are counterfeit and the victim is out the funds.

Internet Auction Scam: This scam is when a victim places an item for sale on the Internet and the winning bidder tells them that they need the item to be shipped to them. They will send the victim a check much larger than the sale price of the item and instruct the victim to wire extra money to the shipper who will be picking the item up. The check is a counterfeit and the victim is out the funds.

Charitable Organization Scam: The scammer for this one will visit various message boards of Christian organizations and gain the trust of an unsuspecting victim. One of the scenarios they may use is they want to invest in their organization. Once again sending a check and having funds wired back to them for a variety of reasons. The check is a counterfeit and the victim is out the funds.

Relative in Trouble Scam: This is a new scam, where the scammer will contact the victim by phone and claim to be a relative, (grandchild, niece or nephew) that is in some type of trouble, either legal trouble, or their car has broken down or they are out of town and have no money to get home on. The scammer will ask the victim if they can wire them funds to help them out and will usually ask the victim not to tell their parents. The victim will go to the bank, withdrawal funds and wire the money. Problem is - it was not anyone they knew.

Jury Duty Scam: This scam involves the scammers contacting victims by phone and telling them that they were supposed to show up for Jury Duty and that they will now be arrested for failing to appear. When the victim tries to tell the scammer they had no idea, they never received any notification the scammer will then tell them they can clear it up by verifying if they have the wrong individual and ask the victim to provide them with their Social Security Number, birth date, birth place, and any other personal information they can get.

As you can see the variety of scams can go on and on. The victims can get roped in, in a multitude of different ways. These scammers are good at what they do and are very convincing. This is their job and they are good at it. The result is the same as you can see, if a check is involved, they are counterfeit and the victim is ultimately responsible for the funds.

If it sounds too good to be true - IT IS.