Most Prevalent Scams Occurring Today

2015
The Goal of Wire Fraud Scams is to have the victim wire or otherwise send money to the Scammer through non-refundable, non-traceable methods such as Wire Transfer; Money Orders such as Western Union or Money Gram; or using prepaid credit cards such as Green Dot.

These methods of money transfer or the equivalent of cash. Once the money has been transferred, it is nearly impossible to get it back.
The Grandparent Scam
(Relative in Need Scam)

The Scam:
- Scammers search Facebook etc. for information on relatives of older individuals.
- Scammers then call you pretending to be your relative, a friend of your relative, or the authorities, and will ask you to wire money for an emergency.

How to Avoid:
- Safeguard personal information on web, especially on social media such as Facebook.
- Remain Calm, and Verify the Story being told.
- NEVER Wire money!!!!
The Scam:
• The Scammer will call and claim to be from the Internal Revenue Service, and will state that you owe back taxes.
• The Scammer will threaten you with arrest or jail time if you do not comply, or will state that there is already a warrant out for your arrest.

How to Avoid:
• Keep a Cool Head
  • Did you pay your taxes last year? Have you received any other correspondence from the IRS?
• Remember: The IRS, nor any other government agency for that matter, will EVER call you demanding money.
  • The IRS makes all contacts concerning tax matters via U.S. Mail.
• NEVER Wire Money!!!!
Did the government \underline{call} to ask you for \underline{money}?

That was a \underline{scam}.
The government \underline{never calls} to threaten you or demand money.

Check with your case manager before you pay or share personal information.

Report scams to the Federal Trade Commission
\texttt{ftc.gov/complaint}
or 1-877-382-4357
The Scam:
- The Scammer will contact you, often by phone, claiming that there is a warrant out for your arrest.
- The Scammer will often claim that the Warrant is for back taxes owed to the IRS, or for missing jury duty.
- The Scammer will then claim that this “legal issue” can be resolved by your prompt payment of a fine.

How to Avoid:
- Remember: You will NEVER be told or warned that there is a warrant out for you arrest.
- When in Doubt, Check it Out. Contact your local police department.
- NEVER Wire Money!!!!
diana marshall A Law-Suit has been filed and Arrest Warrant issued on your name. This may arise legal consequences at your home and employment place. If you want to resolve this issue, call us back at State Attorney Head office on 717-458-7808
Example of Fake Arrest Warrant
PROTECT YOURSELF AGAINST JURY DUTY SCAMS

DID YOU KNOW?
Court officers will never ask for payment, a credit card or social security number for failure to appear for jury duty. Report suspicious activity immediately to your local law enforcement agency.

DON’T GIVE OUT PERSONAL INFORMATION BY PHONE OR EMAIL
Lottery & Sweepstakes Scams
(Jamaican Lottery Scam)

The Scam:
- The Scammer will contact you and claim that you have won a prize!
- However, to claim the prize, you must first pay taxes, insurance, shipping and handling, etc.

How to Avoid:
- Be Aware: It is against federal law to enter a foreign lottery.
- Remember: You cannot win a contest you did not enter.
- Any legitimate lottery or sweepstakes will not require you to make a purchase or pay for anything up front prior to receiving your winnings.
- NEVER Wire Money!!!!
The Goal of Identity Theft Scams is for the Scammer to obtain enough of your personal information to steal your identity.

Why would someone want to steal your identity?
- To steal your tax refund.
- To set up credit accounts such as credit cards, loans, and mortgages in your name.
- To steal money from your bank accounts.
- To use your name and other information to conduct other illegal activities, such as receiving stolen property.
Phishing
(Method)

The Scam:
- Emails, pop-ups, phone calls, text messages, and look-alike websites.
- Update/validate personal information.

How to Avoid:
- Don’t follow that link!
- Don’t give out your information.
- Remember: Legitimate companies won’t Email to ask for your personal information.
Dear mailbox user,

Your Email Account has been Accessed from an unauthorized area with an unknown IP Address, and it currently being used for suspicious activities. You are hereby advised to re-validate your account to avoid disability of your mailbox.

If this was you kindly ignore, but if not, kindly use the verification link <http://mailupdateportal.ezweb123.com/> to Re-validate <http://mailupdateportal.ezweb123.com/> your account, ignore if your account is not valid, but note that, your mailbox will be disabled if not revalidated with 24 hours.

Thank You.
ICT HELP DESK© 2015 All rights reserved.
To consider you for a future credit line increase, federal regulations require us to have your current income.

Re: Account ending in 7061

Mark D Bauer,

Keeping your account info up to date is always a good idea. Plus, it helps us meet federal regulations, which require us to collect updated income info before reviewing your account for future credit line increases. So please take a moment and update your income in about 60 seconds.

Why update your income info?

• It'll help us better serve your credit needs.
• There's no credit check required for this update.
• It's quick and easy.

Thank you for putting Capital One® in your wallet.

UPDATE MY INCOME
The Scam:
- The Scammer will call and claim to be from Windows, Microsoft, Norton Antivirus, etc.
- Will have you access a program that shows the number of system errors in Windows.
- Scammer will claim that your computer is messed up and in need of repair.

How to Avoid:
- Be familiar with your antivirus and other software.
- DO NOT allow remote access to your computer.
- NEVER trust unsolicited callers.
The Scam:

- The Scammer will create computer program that calls you and leaves a pre-recorded message.
- The message often states that you have been approved for a high level loan at the “gold” or “platinum” level, and that to complete the process and receive your funds, you need to visit a website and enter your personal information.

How to Avoid:

- Hang up on any Robocall that has “Congratulations” anywhere in the first sentence.
- Remember: You cannot be approved for a loan you did not apply for. Be aware of where you have applied for credit.
- Beware of any loan that has a “Gold Level.” It is a loan, not a credit card.
Sample Robocall

“Hello and Congratulations! You have recently applied for a payday loan, and you have been pre-approved for our highest gold level. This entitles you to receive up to $1,500. All funds are deposited into your account within one hour. To receive your funds, simply visit www.wirecashdirect.com and type in your VIP promo code of 7779. Once again, visit wirecashdirect.com and type in your VIP promo code of 7779. This offer will expire within 24 hours. Congratulations Again!”
Put a Stop to Robocalls

Block any numbers that leave a Robocall Message.
Put a Stop to Robocalls

Sign up for Nomorobo

Nomorobo is a Call Screening and Blocking Service that won the Federal Trade Commission Robocall Challenge
Nomorobo is FREE to consumers. Businesses do pay a fee.
For additional information or to sign up, visit www.nomorobo.com
Scam Type #3: Accomplice Scams

Accomplice Scams, which often take the form of Work from Home Scams, are extremely dangerous. Not only can your time and money be stolen, but you can unwittingly become an Accomplice to Fraud and can be found criminally liable for Money Laundering, Receiving Stolen Property, Mail Fraud, and Wire Fraud.
The Scammer will offer you an opportunity, generally via Email, to help transfer money, gold, diamonds or something else of significant value into the U.S. from a foreign country, earning a commission in the process.

Usually, the Scam with either:
- Require the payment of an upfront fee.
- Require that you give the Scammer your banking details, such as the routing and account number.

Comes in hundreds of different variations:
- Soldier found gold in Iraq; Son of a Deposed Dictator; Wealthy Refugee from a War Torn Country.
FROM: CHARLES TAYLOR (JNR).
LONDON, ENGLAND
TELEPHONE: +44 755 2635490.
FAX: +44 2070 2287 93.

DEAR: MR SAMUEL J FETCHERO

MAY I USE THIS OPPORTUNITY TO INTRODUCE MYSELF TO YOU MY NAME IS CHARLES TAYLOR (JNR) I AM THE SON OF FORMER PRESIDENT OF LIBERIA, A COUNTRY IN WEST AFRICA, MY FATHER WHO IS CURRENTLY BEING HELD AGAINST HIS WILL BY THE UNITED NATIONS FOR ALLEGED OFFENCES OF WAR CRIMES. HEIS CURRENTLY FACING COURT TRIAL IN THE HAGUE IN NETHERLANDS MY FATHER IS A GOOD MAN WHO TRIED TO DO SO MUCH FOR OUR PEOPLE LIBERIANS I AM CONTACTING YOU WITH THE BELIEVE THAT WE WILL DEVELOP A CORDIAL BUSINESS RELATIONSHIP WHICH WILL BE BENEFICIAL TO BOTH OF US MY FATHER GAVE ME YOUR ADDRESS WHEN I VISITED HIM ON THE 19TH OF NOVEMBER 2009. HE SAID THAT HE HAVE A LOT OF CONFIDENCE AND TRUST IN YOUR PERSONALITY. MY FATHER KEEP THE SUM OF (ONE HUNDRED AND SEVENTY SEVEN MILLION UNITED STATES DOLLARS) $177,000,000 USD IN A BANKS SECURITY VAULT UNDER THE NAME OF HIS FRIEND A FOREIGNER FROM YOUR COUNTRY: MR SAMUEL J FETCHERO AS THE NEXT OF KIN TO THE DEPOSIT TO AVOID ANY TRACE THIS FRIEND OF MY FATHER DIED ON 25TH JULY 2009 IN A MOTOR ACCIDENT. MY FATHER DIRECTED ME TO USE THIS MONEY FOR INVESTMENT PURPOSES SPECIFICALLY IN YOUR COUNTRY. I PROMISE TO GIVE YOU 30% OF THE TOTAL FUNDS FOR YOUR ASSISTANCE AND 10% OF THE PROFIT AFTER TAX FOR FIVE YEARS.

I AM CURRENTLY ON EXILE HERE IN LONDON ENGLAND AND I HAVE MADE CONTACT WITH THE BANK MANAGER OF THE BANK WHERE MY FATHER DEPOSITED THE FUNDS. I HAVE ALSO INSPECTED THE FUNDS AND CONFIRM THAT IT IS STILL WITH THEM. I WILL GIVE YOU ALL THE DETAILS ON HOW WE WILL CLAIM THESE FUNDS UPON RECEIPT OF YOUR RESPONSE.

I HAVE THE WHOLE DOCUMENTS FOR THE DEPOSIT I THEREFORE SEEK YOUR ASSISTANCE IN TRANSFERRING THIS FUND OUT OF LONDON ENGLAND.

BEST REGARDS.

Charles Taylor

CHARLES TAYLOR (JNR).

NOTE: PLEASE SEND ALL YOU’RE CONTACT INFORMATION THROUGH MY ABOVE FAX NUMBERS, AS SOON AS I RECEIVE YOUR CONTACT INFORMATIONS I WILL SEND ALL THE DETAILS ON HOW WE ARE GOING TO CONCLUDE THIS TRANSACTION.
“Busy Work” Scams

The Scam:
- The Scammer will post on job sites and other classified websites, such as Craigslist and Monster, offering opportunities to Work from Home such as Envelope Stuffing; Crafting; or Data Entry.
- To Get your “kit” or “materials” or to “become a member”, you must pay an upfront fee.
- The Scammer will “overpay” you for your work, and will request that you wire the excess funds back to him. However, the “paycheck” is a fake.

How to Avoid:
- Never Wire Money!!!
- Thoroughly research any Work at Home opportunities.
- If it sounds to good to be true, it is!
- Get any promises, agreements, contracts, etc. in writing!
Beware of Payment Processing Scams

Rarely, the Scammer will actually pay you money to receive funds into your bank account, and then transfer the funds to a different account, keeping a percentage of the transfer for yourself as a “commission.”

Generally, the Target will receive numerous small checks or transfers, and will then transfer one large sum to the Scammer at the end of the day/week.

Often, this is touted as “payment processing” or “check processing.”

In reality, you are illegally laundering money, and could be held criminally liable.
Reshipping Scams

The Scam:
- The Scammer will offer you an opportunity to Work from Home as a “re-shipper,” earning a fee for each package processed.
- The “Job” will entail receiving packages at your address and then reshipping the package as a whole, or “breaking bulk” and resending the packages.
- In reality, the goods you are shipping are generally stolen goods, and you have become an Accomplice to Mail Fraud.
Top Fraud Avoidance Techniques

- Never Wire Money!!!!
- Never give out your personal information unless YOU initiated the contact.
- Always verify whom you are doing business with.
- Shred all documents containing sensitive personal information.
- Safeguard your Social Security Number and Card.
- Monitor your Credit Report.
- Use Direct Deposit whenever possible.
- Register for the Do Not Call Registry at www.donotcall.gov
- Opt-Out of Pre-Screened Credit Offers at www.optoutprescreen.com
ELDER CONSUMER PROTECTION PROGRAM

1401 - 61st Street South
Gulfport, Florida 33707

Telephone: (727) 562-7888
Facsimile: (727) 345-1838

E-mail: ecpp@law.stetson.edu

Website: http://www.stetson.edu/law/elderconsumers

Twitter: @StetsonLawECPP