Beware of SCAMS

IMPORTANT INFORMATION
PLEASE KEEP

BRITISH VIRGIN ISLANDS

KEEP YOUR MONEY SAFE - AVOID SCAMs

A scam is a scheme designed to lure you in with the promise of unimaginable wealth only to rob you of your hard earned money. Scams come in many forms and continue to get more and more sophisticated. Scammers are using ever means available to them to capture their intended targets – email, texts, phone calls and social media sites are all used by scammers to reach out to potential victims worldwide.

In today's world it is likely that everyone will be approached by a scammer at some point. Some scams are easy to spot while others may appear to be genuine. Some scams even take place without the victim doing anything at all. Even if you think you could never be tricked into one of these schemes, it is important to always remain skeptical about offers that seem too good to be true. Bogus sweepstakes and lotteries, fake health cures and other products, get-rich-quick schemes and inheritance scams are some of the most common schemes designed to separate you from your money.

Most scams require you to take some action before they can work. You may be asked to send money to someone based on a false promise of huge returns. You may be asked to divulge personal details such as passport or bank account information that is then used by a scammer to defraud you or commit other crimes. The number, variety and complexity of scams continue to grow so individuals need to be more cautious than ever before.

Here are some of the most common scams:

Inheritance Scam – correspondence from someone usually claiming to be a lawyer and offering their services to secure money left to you by a distant relative. They charge you various fees and ask for bank account details to pay in the inheritance. Alternatively, the correspondence could be from someone seeking your help to cash in on an inheritance usually to avoid taxes or other governmental fees with promises of sharing their new found wealth.

Advance Fee Schemes – usually a notification that you have won an unknown lottery or sweepstakes and requesting that you make advanced payments in order to collect your winnings.

Bogus Communications from Regulatory Bodies – correspondence claiming to be from a regulatory or supervisory authority requesting personal information or money.

Identity Fraud – someone impersonates you without your knowledge, often by stealing your bank or personal details, or obtaining them from discarded or lost documents.

Credit Card Scams – usually a telephone call advising you that you have been the victim of fraud and asking you to verify your credit card details.

Stranded Scams – usually an email which appears to be from a person you know claiming to be stranded or in distress and in immediate need of financial assistance.

Rental and Real Estate Scams – victims usually have rental properties advertised online. Scammers contact the victim and agree on a rental price. A counterfeit check is then forwarded for the deposit. The scammer then asks for a refund of a portion of the deposit or the entire deposit before the check is found to be counterfeit. Scammers may also duplicate listings from legitimate real estate websites and defraud potential renters or buyers by posing as a real estate agent.

Counterfeit Check Scams – victims are sent counterfeit checks and asked to keep a portion for services rendered and remit the balance to a third party before the check is found to be counterfeit. Recently law firms have been specifically targeted.

Disaster Relief Scams – scammers solicit contributions purportedly for charitable organizations helping disaster victims. A number of these emerged after the 2010 earthquake in Haiti.

Romance Scams – scammers usually establish relationships with their victims via email or social networks using fake personal details and images of other people. Once trust is established scammers will claim that something terrible has happened to themselves or their family and ask for financial help. Alternatively, the scammer may ask the victim to cash a counterfeit money order and return cash via a money transfer service like Western Union.

Mobile Phone Insurance Scams – a telephone call shortly after buying a new phone offering you insurance coverage.

Missed Call Fraud – victims receive a call on their mobile phone but the scammer hangs up after one ring. If the victim calls back, they are put through to a premium-high rate phone number.

Investment Scams – scammers call potential victims offering shares for purchase in unknown companies with promises of high returns. Scammers have been known to target community or religious groups with these types of scams.

Chain Letters/Ponzi Schemes – scammers guarantee huge returns for reselling certificates or passing on emails for usually a small upfront investment.

Fund Transfer Schemes – money-laundering scams that tempt you to use your bank account by offering a commission. Money-laundering is a criminal offence.

Online Fraud (phishing) – fake bank websites used to get personal information and money from victims.

Work from home scams

Work-from-home scams are often conducted through spam emails, or advertisements on notice boards. Most of these ads are not real job offers. Many of them are actually fronts for a money-laundering scam, an upfront payment scam or a pyramid scheme.

You might receive an email offering a job where you use your bank account to receive and pass on payments for a foreign company. These 'job offers' promise that you will receive a percentage commission for each payment you pass on. Transferring money for someone might be money laundering and you could wind up in trouble yourself for taking part in these 'jobs'. Sometimes, these scammers are just after your bank account details so they can clear out your account.

You might also be offered a 'job' doing something like stuffing envelopes or promotions. You will be required to pay for a starter kit or some other product before you can get started. However, once the money is paid, you may receive nothing at all, or what you do receive could just be instructions for conning other people into joining the same scheme.

Another type of work from home scam involves a job putting together or assembling a product using materials that you have to buy from the 'employer'. After they pocket the money you pay for materials, they may refuse to pay you for some or all of you work because they claim it is not of a high quality.

SCAMS Tips

These are just a few of the many scams that are in circulation. They are all designed with one purpose, to con you out of your money. Scams can cost victims large amounts of money and cause undue distress. The best advice is to ignore all emails, texts, phone calls and the like that appear to be scams. Here are some simple tips to help you protect yourself and your family from scams:

The Basic Rules

- If it looks too good to be true—it probably is.
- Always use your common sense: any offer could be a scam.
- ALWAYS get independent advice if an offer involves significant money, time or commitment.
- Remember there are no get-rich-quick schemes: the only people who make money are the scammers.
- Do not agree to offers or deals straight away: tell the person that you are not interested or that you want to get some independent advice before making a decision.
- NEVER send money or give credit card or online account details to anyone you do not know and trust.
- Check your bank account and credit card statements when you get them. If you see a transaction you cannot explain, report it to your financial institution.
- Keep your credit and ATM cards safe. Do not share your personal identity number with anyone. Do not keep any written copy of your PIN with the card.

Dig Deeper

- Do not let anyone pressure you into making decisions about money or investments: always get independent financial advice.
- Make sure you know how to stop any subscription service you want to sign up to.
- Be very careful about offers for medicines, supplements or other treatments: always seek the advice of your health care professional.
- Beware of products or schemes that claim to guarantee income or winnings.
- Be wary of investments promising a high return with little or no risk.
- Beware of job offers that require you to pay an upfront fee

Protect Your Identity

- Only give out your personal details and information where it is absolutely necessary and where you have initiated the contact and trust the other party.
- Destroy personal information, don't just throw it out. You should cut up, burn or shred old bills, statements or cards so scammers cannot get your personal details from them later.
- Treat your personal details as you would treat money: don't leave them lying around for others to take.

Sending or Transferring Money

- Never send money to anyone you are not totally sure about.
- Do not send any money or pay any fee to claim a prize or lottery winnings.
- Money laundering is a criminal offence: do not agree to transfer money for someone else.
- Make sure that cheques have been cleared by your bank before transferring or wiring any refunds or overpayments back to the sender.
- Do not pass on chain letters or take part in pyramid schemes: you will lose your money and could lose your friends.

SCAM Tips cont.

Telephone Traps

- If you receive an unexpected phone call, always ask for the name of the person you are speaking to and who they represent.
- Do not give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- It is best not to respond to text messages or missed calls that come from numbers you don't recognise.

Dealing with suspicious or unsolicited offers sent by email or SMS

- Do not open suspicious or unsolicited emails (spam): delete them.
- Do not click on any links in a spam email, or open any files attached to them.
- Never call a telephone number that you see in a spam email or SMS.
- NEVER reply to a spam email or SMS (even to unsubscribe).

Internet Tips

- Talk to your internet service provider or an IT professional about spam filtering or, alternatively, purchase spam-filtering software.
- If you want to access an internet account website, use a book marked link or type the address in yourself: NEVER follow a link in an email.
- Install software that protects your computer from viruses and unwanted programs and make sure it is kept up-to-date.
- Beware of free websites and downloads (such as music, adult sites, games and movies). They may install harmful programs without you knowing.
- Check the website address carefully. Scammers often set up fake websites with very similar addresses.
- Never enter your personal, credit card or online account information on a website that you are not certain is genuine.
- Never send your personal, credit card or online account details by email.
- Try to avoid using public computers (at libraries or internet cafes) to do your internet banking.
- Do not use software on your computer that auto-completes online forms. This can give internet scammers easy access to your personal and credit card details.
- Choose passwords that would be difficult for anyone else to guess.

Protecting Your Business

- Never give out or clarify any information about your business unless you know what the information will be used for.
- Never agree to any business proposal on the phone: always ask for an offer in writing.
- Try to avoid having a large number of people authorised to make orders or pay invoices.
- Always check that goods or services were both ordered and delivered before paying an invoice.
- Make sure the business billing you is the one you normally deal with.
- If you are unsure about any part of a business offer, ask for more information or seek independent advice.

For more information contact the Financial Investigation Agency.

BRITISH VIRGIN ISLANDS

Financial Investigation Agency
P.O. Box 4090, Pasea Estate
Road Town, Tortola
British Virgin Islands

Telephone: (284) 494 1335
Facsimile: (284) 494 1435
E-mail: fia@bvifia.org