How to recognize a scam checklist

General scam checklist

If you check any of these boxes, they may be trying to scam you. Make sure you do your research, before deciding, and don't give any money or personal information.

Do they:

- ❑ Offer you a large reward or a lot of money
- ❑ threaten that you will miss out
- ❑ Tell you there is a time limit
- ❑ Pretend to be a company but have no website
- ❑ Will not let you call back again
- ❑ Threaten you with the police
- ❑ Get very aggressive when you hesitate
- ❑ Ask for personal information
- ❑ Ask you to send the product before they send money (cars)
- ❑ Ask you to send gift cards or cryptocurrency

DOs and DON'Ts FOR SCAMS

- ❑ Don't believe everyone who calls with an exciting promotion or investment opportunity.
- ❑ Don't disclose personal information about your bank accounts, credit cards or address over the telephone.
- ❑ Don't be afraid to hang up.
- ❑ Don't be afraid to ask for documentation to verify a product or investment. But remember, even the scammers can prepare paperwork, catalogues and invoices that seem real.
- ❑ Don't be pressured into making a decision. Any real gift or prize will still be available tomorrow.
- ❑ Do take the time to call a friend, relative, banker or a police agency before making a decision to send money.
- ❑ Do call the police to report any suspicious phone calls or mailings.
- ❑ Do take the opportunity to ask the caller questions about their offer or promotion. No legitimate company will refuse your inquiries.
- ❑ Do ask for literature so you can read about the company before making a commitment.
- ❑ Do ask the company for references from other customers who live in your area.

COMMON SCAMS CHECK LIST:

*If you check any of these boxes it may be a scam

EMAIL/TEXT SCAMS

- ❑ The email, or message, may not be addressed directly to you but may say something like "Dear customer."
- ❑ The email, or message, has a sense of urgency and pressures you to act immediately.
- ❑ When you click on the link, you are asked to provide your personal identification number (PIN) or password online. No real company would ask you to do this except on your regular log-in page.
- ❑ There is no padlock or security lock icon on the log-in page indicating that it is a secure site.
- ❑ The website address begins with "http" rather than "https" – the "s" stands for "secure."
- ❑ There is no way to reply or contact the company directly.
- ❑ The website address, email and website are not the same as those of your financial institution.
- ❑ Other links on the page may not work. Sometimes the page can look very similar to the original.
- ❑ Often there are mistakes in spelling and grammar.
- ❑ It asks you to pay a bill you don't remember.
- ❑ The email or message tells you that you have some money waiting for you.

If you checked any of these boxes, do not reply to the email or message or click any links. You can report the email as a phishing scam.

PHONE SCAMS

- ❑ They offer you a big prize or offer, but you must decide now.
- ❑ They try to keep you on the phone.
- ❑ They threaten that you will lose the prize or be arrested.
- ❑ They ask you to send gift cards or digital money.
- ❑ They leave threatening voicemails saying you will be arrested.
- ❑ They pretend to be a family member in trouble in another country.

If you checked any of these boxes, slow down. Ask the person on the phone some questions to confirm their identity and tell them you will call back. Look up the organizations' real number and call to confirm if they had called you. If you believe it is a family member, slow down, ask them questions only they could answer.

ROMANCE SCAMS

- ❑ They are often living and working far from you.
- ❑ They say they are working on an oil rig, or in the army or a doctor abroad.
- ❑ They ask you to pay for a plane ticket for them to come see you.
- ❑ They tell you a sad story about one of their family members needs medical attention, but they do not have the money.
- ❑ They say they need help paying off a gambling debt.
- ❑ They need your help with something and need you to send them money.
- ❑ They ask for personal information.
- ❑ They ask for gift cards or digital money transfers.
- ❑ They may tell you they love you very quickly.
- ❑ They found you on an online dating application or website.

If you checked any of these boxes, slow down. Stop contacting the person and report their account. Do not send them any gift cards or money.

EMPLOYMENT SCAMS

- ❑ You don't remember applying to their company
- ❑ They offer you a large pay cheque for little work
- ❑ They ask you to send money to a client
- ❑ They offer the job without any interview or application
- ❑ They have no website or contact information
- ❑ The company is an overseas company

If you checked any of these boxes, slow down, and make sure to research the company. Go on LinkedIn or Google and look up the company. Do not give any personal information or transfer any money. Real companies will not ask you to transfer money to clients from your personal account.