CMSGu2022-01

National Computer Board

## Mauritian Computer Emergency Response Team

**Enhancing Cyber Security in Mauritius**

# Guideline on spotting Online Scams

CERT-MU

**National Computer Board**

**Mauritius**

**Version 1.0**

June 2022

Issue No. 1

# Table of Contents

# 1.0 Introduction

## 1.1 Purpose and Scope

The purpose of this guideline is to help the community to spot online scams, be it through emails, SMS or social media.

## 1.2 Audience

The targeted audience for this document includes everyone who uses the Internet, including corporates and home users.

## 1.3 Document Structure

This document is organized into the following sections:

*Section 1* provides the purpose, scope, target audience and structure of the document.

*Section 2* presents a background on online scams.

*Section 3* outlines the common types of online scams.

*Section 4* gives a description on how to identify online scams tell tales.

Section 5 explains how you can protect yourself against online scams.

*Section 6* concludes the document

## 2.0 Background

Online scams are a type of fraud where cyber criminals use lies and deceit to fool people into divulging confidential information. Victims usually receive nothing in return and, in fact, lose large sums of money. Online scams are getting overly sophisticated and difficult to spot so it is important to know how to identify them,

Moreover, the COVID-19 pandemic has provided scammers with new opportunities to defraud consumers. Some of the most well-known scams, such as the Nigerian letter scam, continue to defraud thousands of people a year, despite widespread warnings.

## 3.0 Types of scams

Below are the most common types of online scams.

### 3.1 Advance fee fraud

**Be careful with this message.** Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

HEAD FOREIGN PAYMENT DEPARTMENT
UNITED BANK FOR AFRICA {U-DIRECT BENIN}
INTERNATIONAL REMITTANCE DEPARTMENT
Federal Ministry Of Finance,COTONOU- Benin
Our Ref-UBA/BD/PEMU/FGN/MIN/04-09
Direct Phone No: +22964034335

Attention Dear Customer Funds Beneficiary

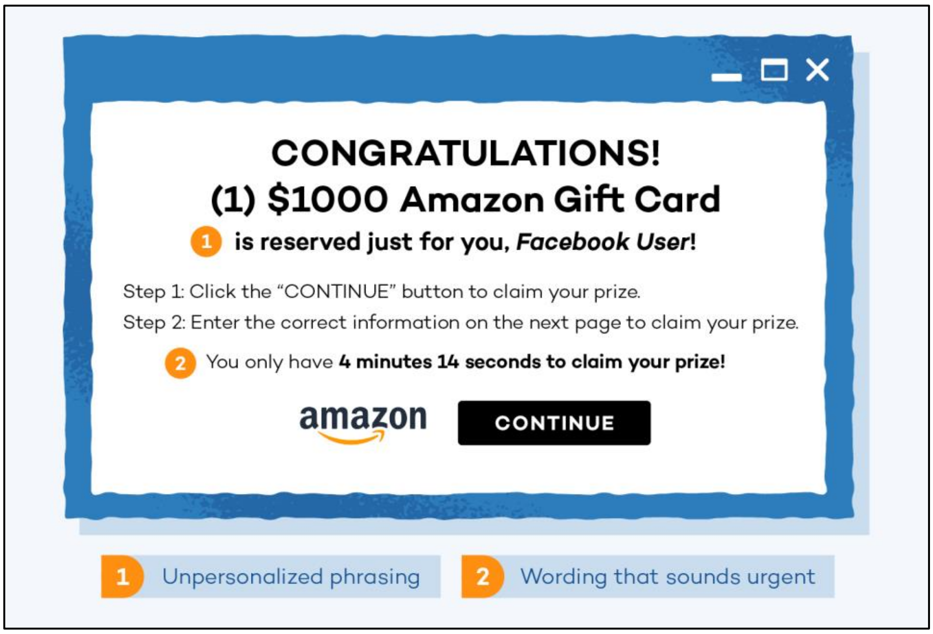
We are still waiting to receive the Money Gram or western union payment information's of $82.00 Usd, from you today, to enable us process on your total Compensation funds payment wire transfer direct into your Bank Account. Make sure you send it today, to avoid cancellation on your payment file, because your delay is getting too long, and you are warned to stop forwarding Our email to the impostors hackers, to avoid them knowing the status of your total Compensation funds payment wire transfer.

I told you earlier-stage that once we receive the payment fee confirmation from the Origin Country as we instructed you, your total Compensation of $7.5m usd funds payment wire transfer will commence successful direct into your Bank Account, and all the Proof documents will be forwarded to you together with your Compensation funds payment transfer slip.

- A scammer requests fees upfront or personal information in return for goods, services, money or rewards that they never supply.
- Scammers invent convincing and seemingly genuine reasons for requesting payment, such as to cover fees or taxes.

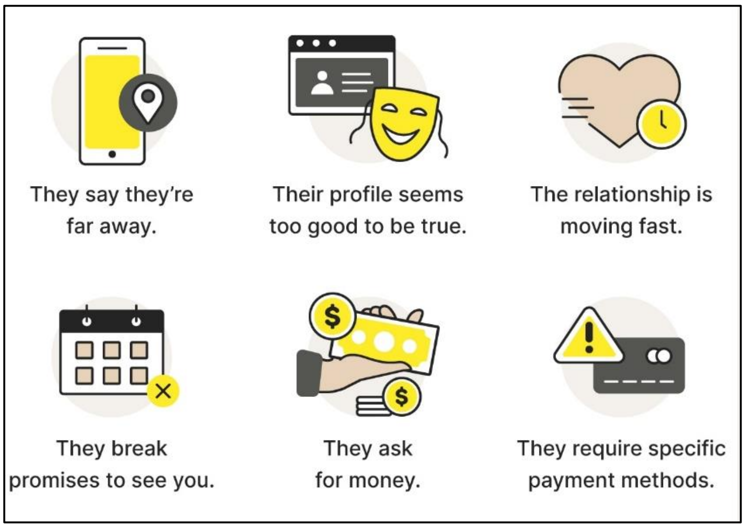
- They often ask for payment by international wire transfer.
- These scams are commonly mass-marketed with scammers sending them out to thousands of people all over the world at the same time, usually by mail or email.

### 3.2 Lottery, sweepstakes and competition scams




- An email, letter or text message from an overseas lottery or sweepstakes company arrives from out of nowhere.
- It says you have won a lot of money or fantastic prizes in a lottery or sweepstakes competition you did not enter.
- These scams try to trick you into giving money upfront or your personal details in order to receive the prize.
- Scammers typically claim that you need to pay fees or taxes before your winnings or prize can be released.
- You may also have to call or text a premium rate phone number to claim your prize.
- Remember you cannot win a prize if you haven't entered.

### 3.3 Dating and romance scams



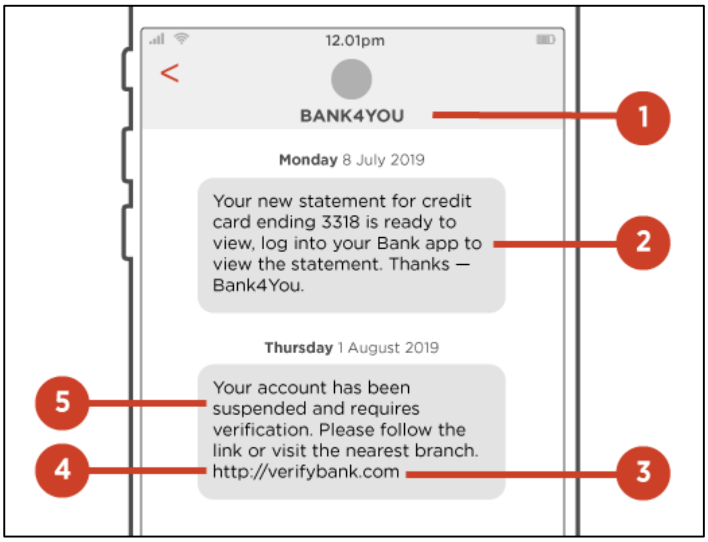

- Scammers create fake profiles on legitimate dating websites.
- They use these profiles to try to enter into a relationship with you so they can get a hold of your money and personal details.
- The scammer will develop a strong rapport with you then ask for money to help cover costs associated with illness, injury, travel or a family crisis.
- Scammers seek to exploit your emotions by pulling on your heart strings. Sometimes the scammers will take months and months to build up the rapport.

### 3.4 Phishing scams

- Phishing emails are commonly used by scammers to trick you into giving them access to your computer.
- They 'fish' for your personal details by encouraging you to click on a link or attachment.
- If you click, malicious software will be installed and the hacker will have access to files and information stored on your computer.
- A phishing email often appears to come from an organisation that you know and trust, like a bank or financial institution, asking you to enter your account password on a fake copy of the site's login page.
- If you provide your account details, the scammer can hack into your account and take control of your profile.

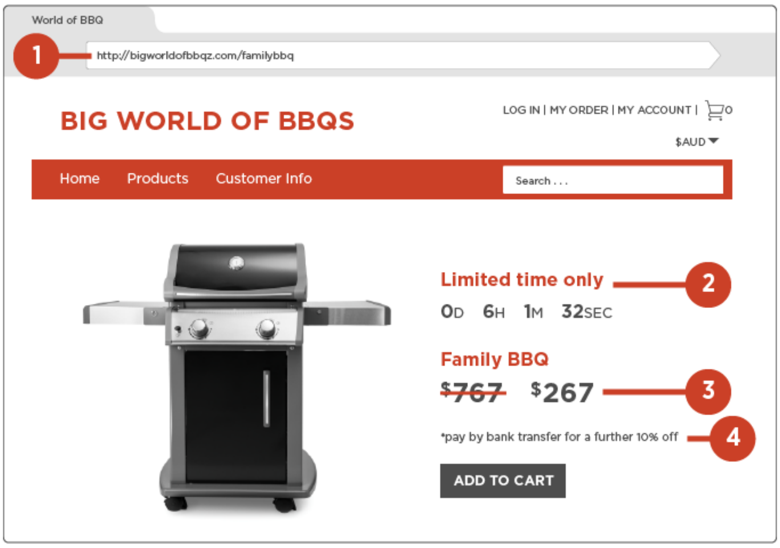
### 3.4.1 Bank SMS

You receive a new SMS from your bank. After looking at it closely, you realise that although the previous SMS was real, the new SMS is a scam.




1. Scammers can make messages look real.
2. It is different in style from the first SMS.
3. It has a malicious link.
4. It is not secure.
5. It has a sense of urgency.

### 3.4.2 Online shopping, classified and auction scams




1. It is not secure.
2. It has a sense of urgency.
3. The deal is too good to be true.
4. It is using a non-secure payment method.

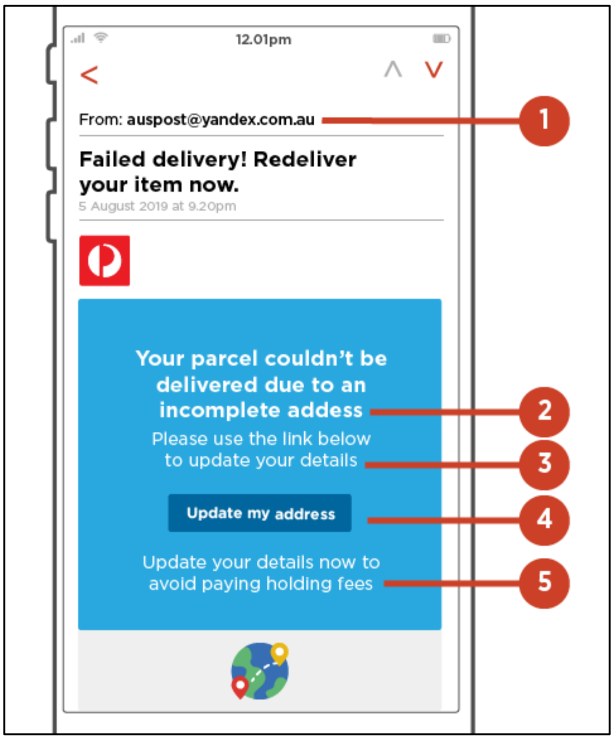
- Scammers like shopping online for victims. Not getting what you paid for is a common scam targeting online shoppers.
- A scammer will sell a product and send a faulty or inferior quality item, or nothing at all. They may also pretend to sell a product just to gather your credit card or bank account details.

- These scams can also be found on reputable online classified pages.
- An online auction scam involves a scammer claiming that you have a second chance to buy an item that you placed a bid on because the winner has pulled out.
- The scammer will ask you to pay outside of the auction site's secure payment facility.
- If you do, your money will be lost and the auction site will not be able to help you.

### 3.4.3 Classified scam

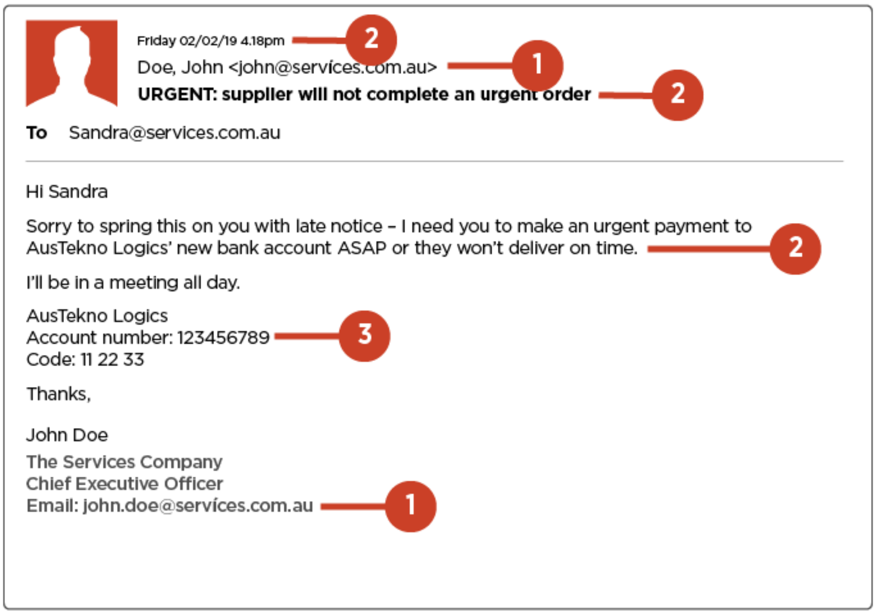

1. There is no evidence of the puppy.
2. It is too good to be true.
3. There are other up-front costs to consider.
4. The payment method is not secure.

### 3.4.4 Mail delivery scam



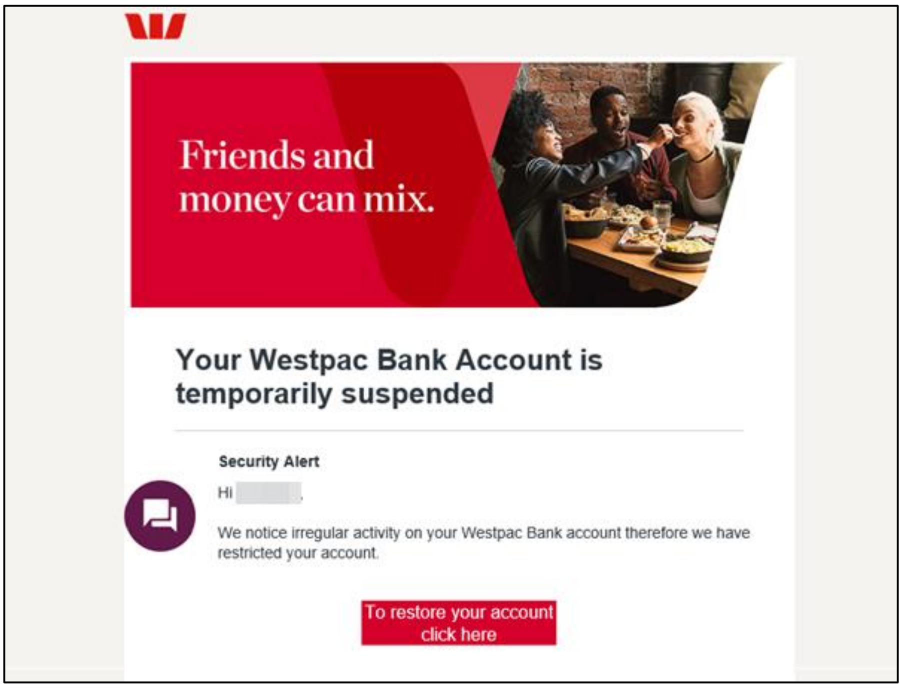

1. You cannot confirm who it is from.
2. It has spelling and grammatical errors.
3. It has a request for you to do something.
4. It has a malicious link.
5. There is a sense of urgency.

### 3.4.5 Business email compromise scam



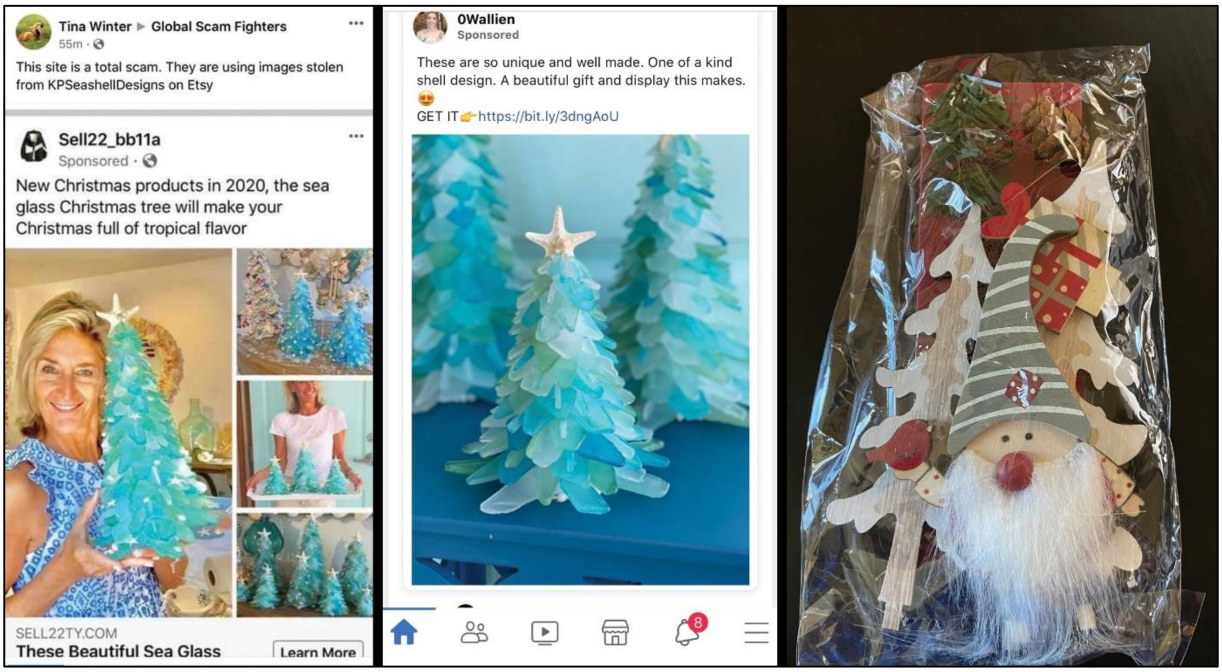

1. You cannot confirm who it is from.
2. It has a sense of urgency.
3. Some things have changed.

## 3.6 Banking, credit card and online account scams




- Scammers send emails or text messages that appear to be from your bank, a financial institution or an online payment service.
- They usually claim that there is a problem with your account and request that you verify your details on a fake but convincing copy of the bank's website.
- Card skimming is the copying of information from the magnetic strip of a credit card or automatic teller machine (ATM) card.
- Scammers skim your card by putting a discreet attachment on an ATM machine. They may even install a camera to capture your pin.
- Once your card is skimmed, scammers can create copies and make charges to your account.

## 3.7 Small business scams

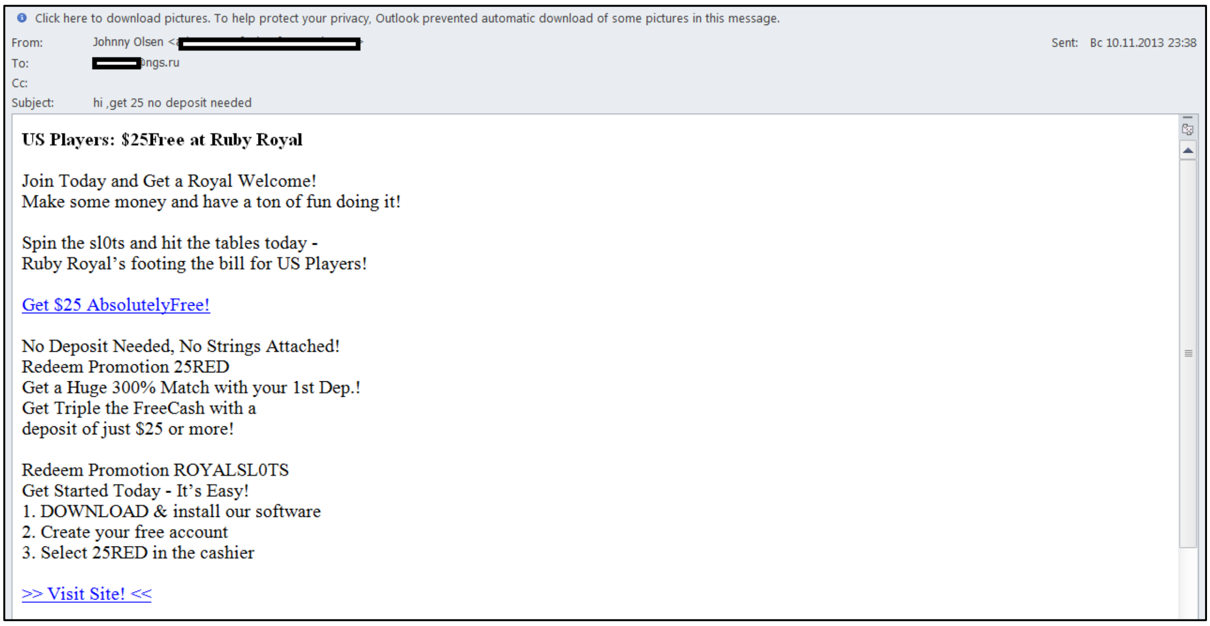



- If you own a small business you can be targeted by scams such as the issuing of fake bills for unwanted or unauthorised listings, advertisements, products or services.
- A well-known example is where you receive a bill for a listing in a supposedly well-known business directory.
- Scammers trick you to sign up by disguising the offer as an outstanding invoice or a free entry, but with a hidden subscription agreement in the fine print.
- Scammers can also call your business pretending that a service or product has already been ordered and ask for payment over the phone.

### 3.8 Job and employment scams


- These scams involve offers to work from home or set up and invest in a business opportunity.
- Scammers promise a job, high salary or large investment return following initial upfront payments.
- These payments may be for a business plan, training course, software, uniforms, security clearance, taxes or fees.
- These scams are often promoted through spam email or advertisements in well-known classifieds, including websites.

## 3.9 Golden opportunity and gambling scams



Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Johnny Olsen <[redacted]

Sent: Вс 10.11.2013 23:38

To: [redacted]ngs.ru

Cc:

Subject: hi ,get 25 no deposit needed

**US Players: $25Free at Ruby Royal**

Join Today and Get a Royal Welcome!
Make some money and have a ton of fun doing it!

Spin the sl0ts and hit the tables today -
Ruby Royal's footing the bill for US Players!

Get $25 AbsolutelyFree!

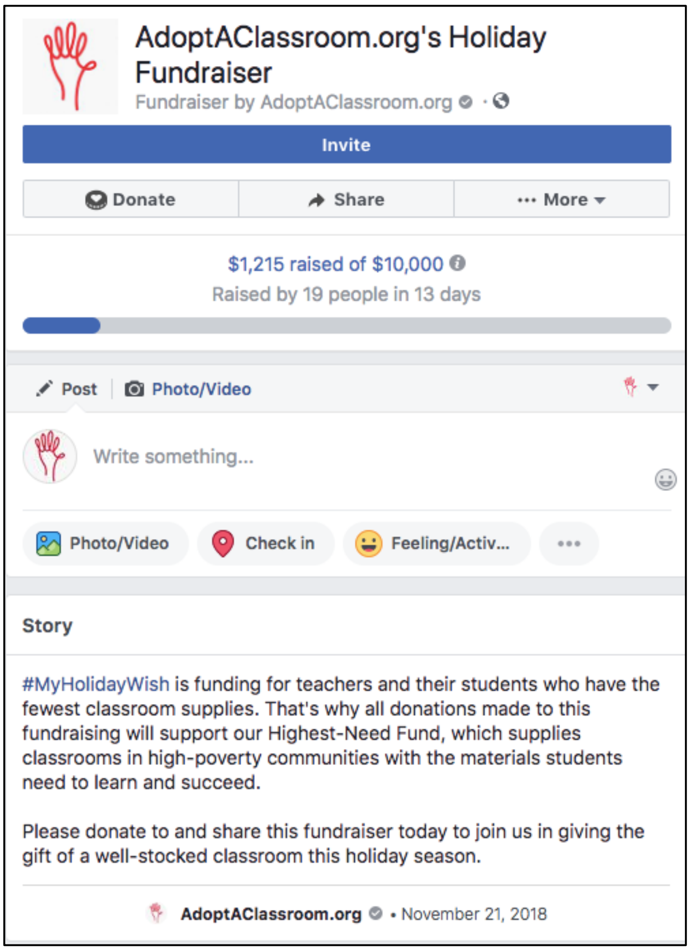
No Deposit Needed, No Strings Attached!
Redeem Promotion 25RED
Get a Huge 300% Match with your 1st Dep.!
Get Triple the FreeCash with a
deposit of just $25 or more!

Redeem Promotion ROYALSL0TS
Get Started Today - It's Easy!
1. DOWNLOAD & install our software
2. Create your free account
3. Select 25RED in the cashier

>> Visit Site! <<

- Scams often begin with an unexpected phone call or email from a scammer offering a not-to-be-missed high return or guaranteed investment in shares, real estate, options or foreign currency trading.
- While it may seem convincing, in reality the scammer will take your money and you will never receive the promised returns.
- Another scam promises to accurately predict the results of horse races, sports events, stock market movements or lotteries.
- Scammers promise you huge returns based on past results and trends. In order to participate, you may be asked to pay for membership fees, special calculators, newsletter subscriptions or computer software programs.

## 3.10 Charity and medical scams




- Scammers are unscrupulous and take advantage of people who want to donate to a good cause or find an answer to a health problem.
- Charity scams involve scammers collecting money by pretending to work for a legitimate cause or charity, or a fictitious one they have created.
- Often scammers will exploit a recent natural disaster or crisis that has been in the news.
- They may also play on your emotions by claiming to collect for a cause that will secure your sympathy, for example to help sick children.
- Medical scams offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions.
- The treatments are often promoted using false testimonies from people who have been cured.

### 3.11 Cryptocurrency investment scam


- Cryptocurrency investment scammers may advertise or post on social media offering great returns from cryptocurrency trading.
- If you click on the advertisement or post, the scammer will contact you or you will be directed to a fake website.
- The scammer will offer to make an investment on your behalf, or provide details of an app or website through which you can invest.
- Cryptocurrency scammers also commonly use platforms such as Discord and Telegram to contact people.
- The scammers will encourage you to buy cryptocurrency through an exchange or request you send money to a company for them to do so on your behalf.
- They will then claim to either trade on your behalf, or coach you through making trades yourself.
- You will be able to see the profits you have made on a webpage, app or custom platform.
- The data you can see will be fake and will show you profiting (or losing as a way to get you to invest more money).
- Eventually you will be unable to withdraw any money.
- The scammers will make excuses for delays in withdrawals, you are banned from the platform or the trading platform is closed.
- When you try and find out what has happened, the scammers cannot be contacted and your money is gone.

# 4.0 Common online scam signs

You can learn to recognize an online scam much faster if you can spot its key features. Every scam has a few standout characteristics in common, as listed below:

- Unexpectedly contacts you
- Provides vague contact details
- Tries to gain trust
- Emotional
- Pressurizes you for action
- Asks for personal information
- Overpays you
- Promises something
- Wire transfer request
- Pretends to be a family member
- Offers something you want
- Offer too good to be true
- Pretends to be a business or the government
- Masquerades as your employer
- Asks you to keep it secret

## 5.0 How to protect yourself against scams

As tricky and brilliant as online scams can be, it is easy to protect yourself. Take the steps below to thwart most email, text, or phone scams.

- Look for signs of deceit such as misspelled words or poor grammar. Legitimate organizations pay attention to these details.
- Do not click links in emails or texts.
- Do not log into an account from an email or text.
- Do not call a number from an email. Look it up instead.
- Secure your online accounts using two-factor authentication and a secure connection.
- Pay by credit or debit card. They have protections built-in to get your money back.
- Block unwanted calls and text messages.
- Do not give your personal or financial information in response to a request that you did not expect.
- Resist the pressure to act immediately.
- Know how scammers tell you to pay.
- Stop and talk to someone you trust.

## 6.0 Conclusion

As online scammers get smarter, they cheat innocent internet users out of an ever larger slice of the financial pie. However, it is not hard to defend yourself against online scams. The trick is to be vigilant with anyone who approaches you, especially via social media, email or SMS. Do not ever give out information or pay money, even as a refund, unless you can independently verify the source.

# References


- https://www.hp.com
- https://www.scamwatch.gov.au
- https://nt.gov.au
- https://consumer.ftc.gov
- https://www.investopedia.com
- https://www.which.co.uk
- https://us.norton.com
- https://www.pandasecurity.com
- https://www.hp.com