Little Black Book of Scams & Frauds

PART 5

HSBC | Malta Foundation

ĠEMMA

know, plan, act.

CONTENTS

FOREWORD

In such a fast-changing world, one can only safeguard against falling prey to scammers if one remains vigilant and takes precautions in financial interactions.

In this booklet, supported by HSBC Malta Foundation, HSBC Malta has compiled essential information to help the reader expand his or her knowledge, helping them remain safe in a possible interaction with a fraudster. You can read about how a scam works, how you can protect yourself against scams, and a handful of case studies. These are followed by a discussion of red flags and notes to help you remain alert should you be approached by a scammer.

HSBC | Malta Foundation

HSBC Malta Foundation has made continuous efforts to raise people's awareness of the possible threats of financial fraud and to improve financial literacy, also through its long-term partnership with ĠEMMA. As part of these efforts, the bank has curated a regularly updated online Fraud Guide on its website where people can learn about the most common scam types and measures which can be taken to protect oneself from both online and offline fraud. The website is available at **https://www.hsbc.com.mt/help/security/fraud-guide/**

Mark Drago
Head of Financial Crime Compliance
HSBC Bank Malta p.l.c.

INTRODUCTION

These are just few of the headlines that peppered Maltese newspapers in the past months. Indeed, 2021 is the year of scams and fraud in Malta.

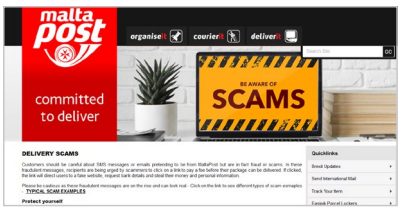

TIMES OF MALTA

Latest National World Opinion Community Sport Motoring Business

Police trying to uncover scam origin as more than 200 defrauded in two months

Scams currently coming mainly through postal operators, bank notifications

13th June 2021




Lovin Malta

News Euro 2020 COVID-19 Sexual Health Ewropej

'I Wondered What I Had Done': People Are Falling For A Scam Call Pretending To Be The Maltese Police

1st July 2021


Home > Local > News > MaltaPost warns about delivery and shopping scams

MaltaPost warns about delivery and shopping scams

Monday, 24 May 2021, 10:59 Last update: about 2 months ago

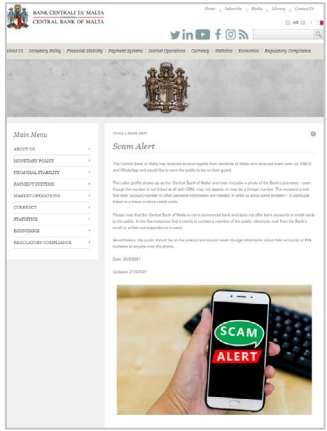
24th May 2021


MBW Malta Business Weekly

Economy Finance Manufacturing Technology

'Remain vigilant and do not give any personal details' Cybercrime unit

3rd June 2021


BANK CENTRALI TA' MALTA
CENTRAL BANK OF MALTA

Main Menu

Scam Alert


the malta independent online

LOCAL WORLD OPINION SPORTS BUSINESS ARTS LIFE VIDEOS NEWSPAPER

40 people scammed out of €50,000 in 24 hours

Thursday, 24 June 2021, 18:05 Last update: about 13 days ago

24th June 2021

Another 40 people have fallen victim to email or SMS scams, with scammers pulling just over €50,000 out of the bank accounts of these victims in just the last 24 hours.

Police said in a statement that it was receiving record amounts of reports of such scams, and made a renewed appeal for the public to be cautious about where they enter personal details.

These scams see criminals using portals built to seem like local entities such as postage operators or banks to induce people into sharing personal details with them – usually by asking them to insert their bank details to pay a small fee to release a mail package or to confirm their details with the bank.

From our 8 European hubs

SHIP

ĠEMMA set financial abuse, of which scams and frauds are one important channel, as one of the core financial capability education competencies that need to be addressed in Malta. The decision to invest in financial capability education is a correct one – as evidenced by research carried out by ĠEMMA in February 2021 on scams and frauds:

- 62% of mobile owners do not have an antivirus installed on their mobile.
- 35% of respondents were confident in recognising a scam. The confidence decreases with age, but increases with the level of education.
- 84% indicated that they have not been scammed in the past two years. Among those who were scammed, 32% experienced a financial loss.
- 50% of respondents indicated that their scam began from an online advert on a website; other main factors that led to a scam related to an online advert on social media and e-mail (with 24% and 17% responses respectively).
- 39% did nothing after being scammed; only 10% stated that they reported the scam to the Malta Police Force.
- 74% of interviewees do not seek information on scams; those aged 25 to 44 are the most inclined to seek information on scams.

In summer 2020, ĠEMMA entered into a strategic partnership with the e-Skills Malta Foundation to disseminate joint financial capability education knowledge and information on scams and fraud on a national level. During this partnership 4 issues of the **'Little Black Books of Scams and Fraud'** were issued, as well as infographics on protection measures that one should be aware of, relating to 35 different **scams and fraud**. During the past 12 months, ĠEMMA has also carried out two **webinars on scams and fraud**.

This is the 5th issue in ĠEMMA's 'Little Black Books of Scams and Fraud' series that is being published. For this 5th issue, ĠEMMA partnered with the HSBC Malta Foundation. The scams and frauds presented in this issue are real cases. Whilst for privacy matters no personal information is given, the 12 cases presented show the range, scope and sophistication of scams and frauds experienced in Malta. The 12 scams and frauds are:

- A dream holiday
- The mule: selling a motor-bike
- Cheque fraud
- Elder abuse: use of a mother's power of attorney to secure a loan
- Elder abuse: misuse of power of attorney to pay a deposit
- Romance scam
- Online 'bargains'
- Computer scam
- UK car import scam
- Unsolicited email to change contact details
- Virus infection on computer
- Offshore investment scam

The Little Black Books of Scams and Fraud are an important tool for you to learn about scams and fraud, including:

- the most common scams to watch out for
- the different ways scammers can contact you
- the tools scammers use to trick you
- the warning signs
- how to protect yourself, and
- where you can find help.

Scammers are criminals who have invested in tools and expertise in order to catch you out. We encourage you to:

- stop and think if you are faced with a situation where you are requested to part with your money;
- back off and trash the e-mail or hang up the phone when you are being rushed to make a decision;
- report a scam or fraud to the police or your bank if you come across one or fall for one.

The purpose of our Little Black Books series is to make you familiar with the many scams and frauds that are perpetuated, equip you with some knowledge on how to protect yourself, present you with resources you may look up, and where you should report should you need to do so.

ĠEMMA strongly recommends that should you come across a scam or fraud – or you become a victim of one – report it. It may be too late for you to recoup your money, but in reporting it you may protect others from falling for the same scam.

We encourage you to share this e-book with your family, friends and colleagues.

How A Scam Works

Most scams follow the same pattern. So, understand this pattern and the scam will be easier to spot. The way a scam works is described here.

(a) The Scammer's Approach

A scammer will approach you with a story designed to make you believe a lie. She or he targets your emotions and behaviour – offering you a chance to make money, to find a partner, to help somebody in need. Invariably, the scammer will dress him/herself as a government official, a company – including branding names you are familiar with, an expert investor, a government official, a lottery officer, an attractive lady or gentleman.

The scammer will use any one of these approaches:

Online	
Email	Still the favoured method, cheap, and a good way to communicate with many persons.
Social media (Facebook, Instagram, etc.), Dating sites, Online forums	These are platforms you are actively running or browsing. You may approach a person and establish contact, or the scammer will befriend you.
Online shopping, classifieds, and auction sites	These are used by scammers to trick you, with initial contact often made through reputable and trusted sites or fake websites that look like the real thing.

Over the Phone / Mobile	
Phone calls	Calls are made by scammers to homes and businesses in a wide variety of scams: from threatening tax scams to offers of prizes or 'help' with computer viruses.
SMS	Scammers tend to send a whole range of scams including competition or prize scams.

Knocking at your Door	
Door-to-Door	This usually involves the scammer promoting goods or services that are not delivered or are of a poor quality.
Charity / Church / Town Band Representative	The scammer seeks donations setting out a heart-rending story or for a social / religious project underway for which funds are being raised.

(b) Communicating and Grooming You

The scammer's tools are designed to get you to lower your defences, build trust in the story and act quickly or irrationally, and proceed to the final stage – making you send the money or provide personal information. The scammer's tools include:

- Spinning elaborate, yet convincing, stories to get what they want.
- Using your personal details to make you believe you have dealt with them before and make the scam appear legitimate.
- Contacting you regularly to build trust and establish a relationship.

- Playing with your emotions by using the excitement of a win, the promise of love, sympathy for an unfortunate accident, guilt about not helping or anxiety, and fear of arrest or a fine.
- Creating a sense of urgency so that you will not have the time to think things through and make you react on emotions rather than logic.
- Similarly, using high pressure sales tactics saying it is a limited offer, that prices will rise, or the market will move and the opportunity will be lost.
- Having all the hallmarks of a real business using glossy brochures with technical industry jargon backed up with office fronts, call centres and professional websites.
- Creating counterfeit and official-looking documents – documents that appear to have government approval or are filled with legal jargon can give a scam an air of authority.

(c) Sending the Money

Asking for money may be set at the point of contact or after months of careful grooming. Scammers have their preferences for how you send your money. Methods vary: wire transfer, credit / debit card, bank transfer, Bitcoin, etc.

THE 10 COMMANDMENTS TO PROTECT YOURSELF

AGAINST SCAMS AND FRAUD

ĠEMMA strongly advises you that you follow these 10 Commandments religiously at all times to protect yourself from scams and fraud:

1 **Watch out for scams.**
Scammers target you anytime, anywhere, anyhow.

2 **Do not respond.**
Ignore suspicious emails, letters, house visits, phone calls or SMS messages – press 'delete', throw them out, shut the door, or just hang up.

3 **Do not agree to an offer straightaway.**
Do your research and seek independent advice if it involves significant money, time or commitment, and get the offer in writing.

4 **Ask yourself who you are really dealing with.**
Scammers pose as people or organisations that you know and trust.

5 **Do not let scammers push your buttons.**
Scammers will play on your emotions to get what they want, including adopting a personal touch. Alternatively, they seek to rush you into making a quick decision before you look into it. Remember there are no guaranteed get-rich-quick schemes!

6 **Keep your computer secure.**
Always update your firewall, anti-virus and anti-spyware software, and buy only from a verified source.

7 **Only pay online using a secure payment service.**
Look for a URL starting with 'https' and a closed padlock symbol.

8 **Do not hand over money and information to someone you do not know and trust.**
Any request for payment by an unusual method such as wire transfers, reloadable cards, or gift cards that are nearly impossible to reverse or track is a tell-tale sign that it is part of a scam. And if you do hand money ... it is rare to recover it.

9 **Protect your identity.**
Your personal details are private and invaluable. Keep them that way and away from scammers.

10 **If you have spotted a scam, spread the word.**
Tell your family and friends, and report it to: computer.crime@gov.mt

In addition to these 10 Commandments, keep in mind the following:

- It is NOT always true that companies, businesses and enterprises are always legitimate. Scammers can easily pretend to have approval and registrations when in fact they do not.
- It is NOT always true that all websites are legitimate. It is easy and cheap to set up a website. And an enterprise's website can be easily copied by scammers who will want to trick you into believing it to be genuine.
- It is NOT always true that scams involve large amounts of money. Sometimes scammers target many people and try to get a small amount of money from each person.
- It is NOT always true that scams are always about money. Some scams are aimed at stealing personal information from you.

Dream holiday

Mr Stivala, a successful businessman, was already dreaming of his winter skiing holiday even though it was still summer. He wanted to give his family a surprise: a skiing holiday in the Swiss Alps – a surprise for his wife for their tenth marriage anniversary, and for the kids for their Christmas school holidays.

While searching the internet, he received a pop-up advertising a charming chalet in Saint Moritz: three bedrooms, large kitchen dining, private hot tub. Mr Stivala, attracted by the stunning pictures of the chalet and the surrounding area, clicked on the link. He was redirected to a website to check for availability and prices.

Mr Stivala entered the check-in and check-out dates and waited eagerly for the website response. Yes, the dates were available. The cost, inclusive of 10 days ski-pass for all the family with a personal trainer, was €15,000. This was within Mr Stivala's budget so he sent a message on the website contact

page stating that he was interested, however he wanted to verify the payment methods as the website was showing only payment by bank transfer.

A few hours later, Mr Stivala received a phone call allegedly from the owners of the chalet. On enquiring whether he could pay the deposit and, subsequently, the full payment via credit card, he was told that they would only accept payment via bank transfer as they did not have any arrangements with any card processor or other online payment processors.

Mr Stivala considered this to be a bit strange and asked whether the chalet was advertised on any dedicated booking sites (such as booking.com). He was told that yes, the cottage was advertised on booking.com. An email was sent with a link to the bookyourholiday.com page where the chalet was being advertised.

Mr Stivala clicked on the link in the email received and he was redirected to the booking.com page hosting the details of the same chalet. The pictures and the details, including the contact details, tallied with those he saw on the original website. He felt reassured so he phoned on the telephone number provided. The call was answered by the same person he talked to before. The two agreed on a deposit of €4,500 with the remaining balance to be paid two weeks before the check-in date.

The deposit was paid via wire transfer to the account shown on the website. Two weeks before the holiday was supposed to commence, Mr Stivala paid the rest of the money and received a thank you note together with a map and all the activities planned for that period. He was also advised that instructions on how to do the check-in and pick up the keys would be sent via email 24 hours before check-in date.

Unfortunately, the email with these instructions was never received. Emails and calls to the same address and number remained unanswered.

Red flags

- Advert pop-up
- Not accepting credit card payments/ other normal payment processors but only wire transfers
- Accent of the person answering the phone call. Does it make sense?
- Paying the full amount two weeks beforehand

Notes:

- Websites can be easily copied and replicated, including using domain names very similar to the original websites (e.g. b00kyourholiday.com to mimic bookyourholiday.com).
- Fraudsters can register and create new websites very easily, using images with the same look and feel as genuine ones.
- Check when the domain name was registered. Often, such fake websites will be closed off and so new websites and names will need to be created. You should be wary of websites offering deals that have been created very recently.
- If you are directed to another well-known website to verify, then do not use links received via email but go directly to the proper website (in such cases use the *proper* bookyourholiday.com) and do a search using the portal's search function.
- Be wary when rental agencies do not accept credit card but only allow wire transfers. Although this could be genuine, the majority of such rental services do accept payment via card or other payment processors. This gives you more protection on your booking or purchase.
- Asking for full payment two weeks before check-in allows time to the fraudsters to move money from one account to another and hide their tracks as it will only be several days later that the victim will realize this was a fraud – with very low chances to stop the payment or ask for a recall of funds.

MULE

SELLING MOTOR BIKE

Mr Pulis wanted to sell his 10-year-old motor bike. He put up an advert on one of Malta's buying/selling websites. After a few days he received a phone call from the U.K. The caller said that he was interested to buy the bike and asked for details on the condition, mileage, etc.

Mr Pulis confirmed the price of €1,000. He informed the caller that he had no know-how to transport the vehicle to the U.K. The caller assured Mr Pulis that he would be taking care of the shipment and that all Mr Pulis had to do was to follow some instructions he will be provided after the deal is done.

Agreement was reached, and the purchaser asked Mr Puilis for his International Bank Account Number (IBAN). A couple of days later, Mr Pulis received an SMS from his bank alerting him to an inward payment of €10,000.

Mr Pulis phoned the buyer straightaway and told him that he must have made a mistake when making the transfer as he had added an extra zero to the amount. Mr Pulis was told to keep €1,000 for the motorbike. As to the remaining €9,000, he was advised to withdraw the money in cash and transfer €500 to a certain company that would be taking care of the shipment and return the €8,500 to the buyer. Both transactions were to be made via a money transfer agency and not through a bank. Full details on how to make the transfers were provided.

Mr Pulis did as requested but he never heard again from the buyer or the shipper. He just kept €1,000 and his bike.

Red flags:

- Foreigner/s seeking to buy vehicles from Malta – especially if the vehicles are more than 10 years old
- Receiving a lot more money than the price you demanded
- You are asked to return the difference via a different channel and via a less traceable money transfer bureau

Notes:

- In this case, Mr Pulis was being used as a "money mule". Most probably, the €10,000 received in his account were the proceeds from another fraud or scam, in which the victim had been asked to send money to Mr Pulis' account. This is commonly done by fraudsters to avoid using their own accounts to receive fraudulent funds, so that when a victim reports the fraud and provides the relevant details of the transactions, the beneficiary's account (in this case, Mr Pulis') would be the first account that the banks and law enforcement officers will look at.
- This is only one way of recruiting mules. Although the actual fraudsters had to forgo €1,000 from the whole fraudulent amount, recruiting mules or creating fake bank accounts or recruiting mules with commission is very often more difficult and more costly.
- Although, in this case, Mr Pulis was a victim, such "mules" may get into serious problems with the authorities and the banks because the act of receiving funds from "unkown" third parties and passing the money back to other unknown persons may be viewed as money laundering, which is a criminal offence. Banks may also close off the relationship with the unwitting victim.
- People are prone to make mistakes when transferring money, but returned funds should be sent to the original sender using the same method and the same account number of the original transaction.

CHEQUE FRAUD

Mr and Mrs Demicoli ran a small B&B business. They advertised their rental property online. One day they received a call from an Italian school teacher who enquired regarding the hosting of five 18-year-old students for two months during the summer months. The students were seeking to learn English in one of the English language schools in Malta.

The Demicolis agreed and confirmed the rental fee at €5,000. They also agreed on a deposit of €1,000. The school teacher accepted and advised that he would be sending a cheque to cover the deposit, with the remaining payment to be done in two tranches, one at the beginning of the students' stay and the rest after the first 30 days.

Some days later the Demicolis received a foreign currency cheque for €5,000 instead of €1,000. Mr Demicoli phoned the teacher who replied that he had made a mistake. To put Mr Demicoli's mind at rest, he confirmed the booking and asked him to deposit the cheque in his (Demicoli's) account and to transfer the extra €4,000 to the school's bank account. The Italian teacher duly provided Demicoli with the school's IBAN number.

Next day, Mr Demicoli deposited the €5,000 cheque into his current account via his bank's ATM, and in the evening he transferred the extra €4,000 to the school's account as directed by the Italian teacher.

Three weeks later, Mrs Demicoli replied to a call from her bank advising her that the deposited €4,000 cheque was returned unpaid by the Italian bank. The Italian bank representative told her that the cheque was a very good counterfeit indeed.

Red flags

- The cheque amount you receive is more than expected or more than you asked for.
- You are asked to return the difference *before* the cheque is cleared – foreign cheques may take longer to clear, sometimes weeks.
- You are asked to return the difference via a bank transfer.

Notes:

- Never accept a cheque with a value that is more than that agreed. Send it back to sender.
- Verify whether the address provided is one you would expect – in this case, the address of a school.

ELDER ABUSE

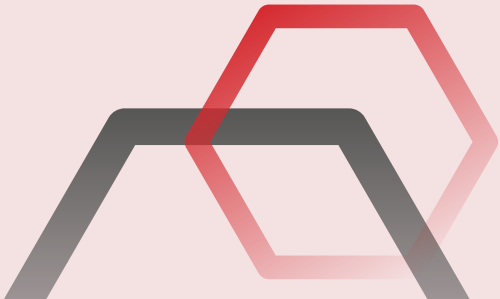
USE OF MOTHER'S POWER OF ATTORNEY TO SECURE A LOAN

Mrs Vella, a widow of 85, lived on her own in her small village house of character. However, she was not able to travel by bus to do certain errands such as withdrawing money from the bank, paying bills or renewing the application for free medication.

She had three sons, all of whom were married and with children. Although they gladly took it in turns to pick her up, drive her around and take her back home, she felt that she was putting too much pressure on them.

One day it was the turn of her youngest son to drive her to the bank to withdraw her pension from the bank. Whilst in the car, she told her son about her concern. He suggested that she should go to a notary to draw up a power of attorney that would allow her three sons to do the errands for her. Mrs Vella agreed to the idea.

All three sons were present when the notary drew up a general power of attorney. The notary explained the duties and rights involved in a power of attorney. Mrs Vella fully trusted her three sons and duly signed the POA. At last this would save her sons a lot of time and hassle.



Six months later, her eldest son, who was a businessman, ran into some liquidity problems and the bank would not increase his overdraft limit. He could not meet the repayment schedule, so the bank could only agree to an increase in the limit if he provided adequate security.

Mr Vella needed the cash badly for his business. A solution came into his mind: using the general power of attorney and put his mother's house as security.

Notes:

- In this case, although all the three sons could check the bank balances, what the eldest son did could not be discovered unless there was an issue with the repayments and the bank wanted to start proceedings to get hold of the security, or if the property was sold by Mrs Vella (or by her heirs after her demise). In such cases the bank asks for the overdraft to be paid in full before the security is released.
- A general power of attorney is a very powerful instrument as it enables the attorney to do anything with the mandator's assets.
- Preferably, powers of attorney should not be general but specific, and include certain limits to the powers.
- Consider requiring certain transactions to be signed by two or more persons jointly.

ELDER ABUSE

MISUSE OF POWER OF ATTORNEY TO PAY DEPOSIT

Mrs Cassar, a spinster aged 78, needed help to be able to do her daily needs, such as cooking, buying groceries and washing. She could not continue to live on her own in her father's farmhouse. She had two brothers and three sisters, all married, who lived in the same village.

Mrs Cassar had worked very hard during her life and managed to save a considerable amount of money in the bank: more than €400,000.

One of her brothers finally convinced her to move in with them. They agreed on a payment of €50 per week as a cover for the food. A power of attorney was drawn up whereby her niece could withdraw money from Mrs Cassar's bank account for medicines, etc.

After a couple of years, Mrs Cassar's health deteriorated. She not only became bed-bound but she also started showing signs of dementia. At this stage, her brother thought that €50 per week agreed upon some years back hardly covered the expences so he asked his daughter, the one who held power of attorney, to start withdrawing more money from her aunt's bank account.

Her niece had just got engaged and was looking for a property to live in. She finally found the property of her dreams but did not have enough money for the deposit. She thought of obtaining some badly needed help from her aunt's bank account.

In the past she used to go to the branch every month to withdraw the money required by her aunt over the counter. She thought that the teller at the branch might become suspicious if she withdrew large amounts of money using the power of attorney, so she created an internet banking profile to be able to manage her aunt's account remotely. She then used online banking to transfer €50,000 from her aunt's account to her personal current account held at the same bank. She made daily withdrawals from her current account. After two months of daily withdrawals she at last had enough cash for the deposit.

ROMANCE SCAM

75-year-old Pawla had a daughter who was assigned a two-year job in Brussels. Her daughter, married with two small kids, wanted to keep in touch with her mother, so she bought her a tablet, created her a social media profile, and taught her some basic skills in the use of the internet and social media.

After some months, Pawla started chatting with a guy named Bobby Smith. Bobby was a U.S. military officer serving in Afghanistan. They chatted every day, and Bobby told Pawla that he had lost his wife to cancer five years earlier and that he lived on his own. He also told her that he was going to retire in a few months' time and was looking forward to take a flight to Malta to meet up – she was the only one person in the world who could make him happy.

He asked Pawla to send him $4,000 for the flight tickets and told her that he would be repaying her once his card problems were settled. He also told her that he needed to purchase the tickets as soon as possible because flight tickets cost more when the date of the flight gets closer.

Pawla wired him $4,000. Some days later Bobby sent her copies of the air tickets from Kabul to Malta.

Subsequently Bobby told Pawla that he found an apartment and wanted to make a deposit to secure its purchase. He asked her to lend him $20,000 to be repaid to her after he received his retirement package which, he claimed, amounted to close to a million dollars.

Again, Pawla wired Bobby the money.

Red Flags:

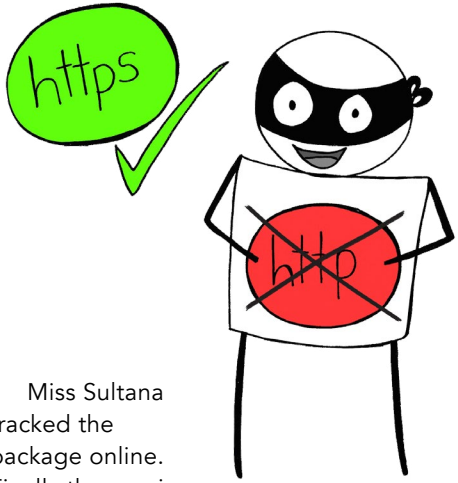
- Playing with sentiments – his wife dying of cancer, feeling lonely, stating after just a few weeks that she was the only person who could make him happy, etc.
- Asking for money a few weeks only after starting to chat
- Urgency – the need to buy air tickets as soon as possible to avoid hikes in the price;
- Finding an apartment in Malta ... when still in Kabul;
- Retiring soon and will have a large amount of money available to repay her.

Notes:

- Fake profiles can be easily created on the internet and images easily sourced.
- Check whether the images sent match the description of the person on the internet profile or the description given over the chat.
- It is easy to create fake documents, including airline tickets, contracts, etc.
- Look for poor English – spelling mistakes and poor sentence construction.
- Look for any mistakes on the social media profile, such as an address not found on maps, wrong postcode, etc.

ONLINE "BARGAINS"

Miss Sultana is into fashion. She likes to buy her clothes and accessories from well-known fashion brands. Wanting to purchase a pair of running shoes (normal cost about €175) she stumbled on a very good deal – just €100.



The site looked genuine, and had many other bargains on offer. Miss Sultana was excited and added a number of items to the shopping cart, including, of course, the running shoes.

She finally checked out and paid with her credit card. In all she paid €442 for the items purchased. She was informed that she would be receiving her goods in one package. She was also given a tracking number. She felt so satisfied with this bargain that she forwarded the link to her friends who also looked very interested.

Miss Sultana tracked the package online. Finally the courier called at her address with the expected package. Although the package was much smaller than expected, she signed for the delivery. On opening the package, she found a very cheap shirt that cost not more than €10.

Red flags

- Website showing goods at out-of-the-norm discounts.

Notes:

- Fraudsters can register and create new websites very easily, using images that have the look and feel of genuine sites.
- Check when the domain name has been registered. Most of the time, fake websites will be closed off and new websites and names will need to be created. Beware of websites offering deals that have been created very recently.
- Do an internet search, even of the website name. Include "scam" or "fraud". There is a good chance that such websites would have already been reported on a number of "scam-warning" websites.
- Be wary of accepting packages if you notice that the package size or shape is not what you expected. This might be used by fraudsters to prove to the cards schemes that they had actually delivered the goods to the address provided and that the package was actually accepted.
- In many other instances, no package would arrive.

Technology company scam

Late one evening, Mr Pisani received a telephone call that claimed to be from a well known technology company. The operator advised him that his software licence had expired and that to continue using his computer he had to pay for a licence renewal of €5. Afraid to lose access to his computer, Mr Pisani accepted the offer and provided his card details, including the security number at the back of the card (CVV) to the "technology company" over the phone.

Some seconds later the "operator" asked Mr Pisani to provide the security code received on his mobile via SMS, and Mr Pisani duly obliged. After this, the operator advised Mr Pisani that the transaction had failed validation and that he should have received a second code on his mobile. Mr Pisani read out the second code received via SMS.

On checking his card statement, Mr Pisani realised that there were two transactions that he could not recognise on the same day as the call. One transaction was of €500, the other of €1,000.

Red flags

- Unsolicited call from a big technology company – these do not normally call private persons to advise of licence expiry.
- Asking for the CVV number over the phone.
- Asking for the SMS one-time password over the phone.
- The low asking price for the licence – when in doubt, consult technical persons.

Notes:

- Normally, licence expiry is displayed on your computer when you launch or use the software/application.
- Licence fees are usually much higher than €5. The low price is used by scammers to encourage the victims to pay.
- Businesses do not ask for the CVV and the SMS one-time password when one effects a transaction over the phone.
- In such cases, do **not** take action immediately. Ask for a contact number to phone back. This will allow enough time for verification with someone who is knowledgeable. If you notice a sense of urgency, then **that** will be another red flag!

U.K. CAR IMPORT SCAM

Mr Borg wanted to buy a second-hand car, so he started looking for bargains on the internet. He did not take too long before he found a website that listed a number of cars for sale, claiming that shipments could be made to any country. Mr Borg searched the list and found a good-priced luxury car with very low mileage and on the road for just two years. There were numerous pictures of the car's exterior and interior. The website looked very professional.

Mr Borg did some research on the trading company. The company had an address registered in Manchester, with more than 50 cars advertised on the virtual showroom. Mr Borg also did a check on the car number plates to verify whether the car was stolen, using one of the free online checking websites. Everything appeared in order. Internet searches also provided a list of adverts issued by the company.

Mr Borg was satisfied that the company was genuine, so he contacted the seller via the email published on their website. He soon got a response with more details about the car and the options available to have the car shipped to Malta. The agreed price was £10,000 with an additional £2,000 for shipping and other administrative costs. Mr Borg was then asked to pay £2,000 upfront for the shipping arrangement, with the rest of the money to be paid once the car is boarded.

Mr Borg did a final check and phoned the number shown on the website. The response was immediate, and a professional telephone service guided Mr Borg through a number of service options available via the telephone. He chose the car sales

service option and was redirected to a certain Mr Stevens. Mr Stevens confirmed the order and the agreed amounts and provided Mr Borg with a U.K. bank account number.

After the call, Mr Borg transferred £2,000 to the account number provided and sent a confirmation email which was immediately acknowledged. After a few days, Mr Borg received an email from the company claiming that the paper work had been completed and that the car was onboard and on its way to Malta via Italy. Copies of the relevant shipping documents were attached to the email. Mr Borg was then asked to effect the full payment before the car reached Italy. Again, Mr Borg obliged, transferring the rest of the money using the bank's internet banking service to the same account used for the deposit.

More than 15 days passed and the car never arrived.

Red flags

- Price for the car was very low.
- Full payment was requested upfront.

Notes:

- It is important to check the address using one of the available online tools. These give you a street view of the place. In such cases, you would expect to see a car showroom or warehouse.
- The website address did not include the company name. This could indicate that the website was fake.
- It is important to physically check the car before paying any money.
- Note that it is very easy to create fake electronic documents, so do not rely on such documents if you want to ascertain whether the sale is genuine.

Unsolicited email to change contact details

Ms Vassallo had just finished her hairdressing course and had just opened her own hair salon. She had also managed to get in contact with an international company selling hair products. She corresponded via email with the sales representative. After a chain of emails, Ms Vassallo agreed to import hair products worth €5,000. She intended to distribute the brand's products in Malta.

As part of the email correspondence, the sales representative advised her about the payment method and provided her with the company's IBAN number, name and address details.

Soon after, Ms Vassallo received an email purportedly originating from the same sales representative. It stated that the company had recently changed its bankers and that they had erroneously provided her with the old IBAN number. A new IBAN number with a different bank was then provided. Ms Vassallo was reminded that following receipt of the payment the order would be processed for delivery. Ms Vassallo sent the money to the new IBAN and confirmed the purchase by replying to the most recent email.

After 15 days, the delivery had not yet been received, so Ms Vassallo emailed the sales representative. Contrary to previous occasions, her email went unanswered for a couple of days so she decided to phone. The sales representative sounded very

surprised, claiming that he had not sent a second email with a different IBAN number; the original IBAN number was the correct one.

On looking carefully at the email addresses, Ms Vassallo noticed that in the last email received (the one that notified the change of IBAN) there was a minor change in the email address: the "o" in the email address was actually a numeric "0".

It resulted that someone was intercepting the email communication between Ms Vassallo and the company. A new email domain had been created which was very similar to the original one, that is, salesrep@hairproducts.com vs salesrep@hairpr0ducts.com. When the deal was confirmed, an email with the fraudulent email address had been sent to the victim. The money was then transferred to an account that was managed by the fraudster.

Red flags

- Request for a change in bank and account details.

Notes

- There are various ways in which emails can be compromised or email communication spoofed or abused. It is always important to check the email address in detail, especially where one takes action that could lead to loss of money.
- Even if an email looks genuine, it is recommended that another channel is used to confirm the payment details, e.g. by using the company official telephone. This is even more important when a change of account is involved.

VIRUS INFECTION ON COMPUTER

INTERNET BANKING PROMPTS

Mr Gauci used his laptop computer to do his banking, using the internet banking facilities offered by his bank. He did not install adequate protection, such as an anti-virus.

One day, whilst logged into his account, Mr Gauci received a warning prompt on his screen advising that his security token was out of sync. The prompt provided him with instructions on how to resync his token. He followed the instructions provided and was prompted to repeat the procedure more than once. A few days later, he identified a withdrawal of €5,000 from his current account on the date he had last logged in and had received the prompts to resync.

When Gauci phoned the bank, he was advised that the bank never issues such prompts.

Mr Gauci's laptop had been compromised by a virus which ran in the background waiting for a login to the internet banking site. Once the login was successful, the virus took over the session and started prompting for the token resyncing. In such cases, the information provided is then sent to the fraudsters who will use the token codes provided to transfer money out of the account.

Red flags:

- It is not normal to receive such prompts, especially when one is not effecting a transaction.

Notes:

- There are a number of viruses and malware that can target internet banking users. It is important for customers to read the security pages of the relevant bank or online security websites that have a list of controls that can be put in place to mitigate such a risk, e.g. installing an anti-virus software, keeping it updated, installing software and operating system patches when released.
- It is also important that if you receive an unexpected message, or there is something abnormal during an internet banking session or whilst logging in, you terminate the session immediately and call the bank to verify.

OFFSHORE INVESTMENT SCAM

Mr Camilleri inherited some money. Not happy with the interest rates offered by the banks, he did some online searches for other investment opportunities. He found an advert marketing "new investment opportunities". He left his details (telephone and email address) to be contacted by an investment officer.

Next day he received a call in reply and was offered an investment product with:

- full capital security
- high return (18% +)
- no tax (as the investment was in a jurisdiction that allowed tax-free investments)
- free access to their website to monitor the investment on a daily basis
- a promise of a bonus of €500 if he finds another investor.

Mr Camilleri was also advised that he needed to act fast as the offer for this product was going to lapse within two days. Mr Camilleri agreed to invest €20,000 and sent the money to the account provided by the "financial officer".

He monitored his investment for a number of days and was very happy to see the relevant graphs going in the right direction. He then decided to talk to his cousin. He too had inherited some money. He managed to convince him, and his cousin invested €10,000.

A few days later, Mr Camilleri received an inward transfer of €500 in his bank account as a bonus for his cousin's introduction and investment. He also received an email with a thank you note and another investment opportunity offer.

Feeling more comfortable after receiving the bonus, Mr Camilleri invested the remainder of the inheritance – a further €30,000.

Red flags:

- High returns – too good to be true, especially when you have a low-risk product with full capital protection.
- Bonus – normally used by scammers to convince you that the company truly exists and that they deliver on their promises.
- Tax benefits
- Offshore investments
- Urgency to invest

Notes:

- Ask questions in relation to the company, the licence number, and where it is registered, the address, etc. Ask for the investment prospectus. Even if these questions are answered satisfactorily, it still does not mean that the investment is genuine.
- Do your own research and verify the information provided:
- check that the address exists, and use a maps tool to see whether it makes sense;
- check that the company selling the product is registered with a securities regulator;
- check that the prospectus is also filed with a securities regulator;
- do online searches with the address, the investment name, the company name, etc.
- Once fraud is discovered, be wary of follow-up scams where scammers will contact you, offering help to recover your funds or to help you open a court case in the country where the funds were transferred, etc.

HOW TO
PROTECT YOURSELF FROM SCAMS & FRAUD

We suggest that ever so often you visit the web page titled "Scams Detection and Warnings" of the Malta Financial Services Authority.

To visit this page, click on this URL:
www.mfsa.mt/consumers/scams-warnings/

On this page, you will find the following sections:

Scam Detection Guidelines
A list "Scam Detection Guidelines" issued by the Malta Financial Services Authority.
www.mfsa.mt/consumers/scams-warnings/typical-scams/

MFSA Warnings
On this page the MFSA warns the public with regard to unlicenced entities that claim to operate from Malta. Avoid investing in any of these companies. To visit this page, click on this URL:
www.mfsa.mt/news/warnings/MFSA-Warnings/

Foreign Warnings

On this page you will find a list of warnings issued by European counterparts of the MFSA. Before you decide to invest with a firm over the Internet make sure that you visit this page. To visit this page, click on this URL:
www.iosco.org/investor_protection/?subsection=investor_alerts_portal

Consumer Notices

On this page you will find a list of consumer notices issued by the MFSA. These notices, which are in Maltese and English, bring to the intention of investors firms that purport to operate from Malta or to be registered with the MFSA. You are not to enter into any financial services transactions with any firm in respect of which MFSA has issued a consumer notice unless you have ascertained that the entity with whom the transaction is being made is authorised to provide such services by the MFSA or by another reputable financial services regulator. To visit this page, click on this URL:
www.mfsa.mt/news-item/mfsa-notice-ahb-consulting/

Entities licensed by the MFSA

You are advised to always check whether a financial services firm is licensed by the MFSA. You can access this list by clicking on the following URL:
www.mfsa.mt/financial-services-register/

ĠEMMA
know, plan, act.

WHAT TO DO IF YOU GET SCAMMED

If you believe that you have uncovered a scam or was the target or victim of one, ĠEMMA advises you to report this. Do not let the scammer get away with it. Remember that there are vulnerable people who may not have the knowledge you have and may be at a high risk of being scammed unless the scam is stopped.

The following are entities to whom you may wish to make the report:

Cyber Crime Unit at the Malta Police Force

You will find the website of the Cyber Crime Unit on this URL:
pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx.

You can contact the Unit as follows:

Online:	computer.crime@gov.mt
Telephone:	356 2294 2231/2
In person:	Call or visit any Police District station and lodge a report. The District Police Officer will request the assistance of a member from the Cyber Crime Unit as required.

European Consumer Centre Malta

You will find the website of the European Consumer Centre on this URL:
eccnetmalta.gov.mt/

You can contact the Centre as follows:

Online:	ecc.malta@mccaa.org.mt
Telephone:	356 2122 1901
In person:	'Consumer House', No 47A, South Street, Valletta

For opening hours kindly click this URL:
eccnetmalta.gov.mt/contact-us/contact-us-2/

Your Bank

If you are the victim of a debit or credit card fraud, immediately contact your bank. Do the same if you lose your debit or credit card.

The revised Payment Services Directive (PSD2) establishes that if you, as a client of a bank, have lost or had your debit or credit card stolen and it transpires that a fraudulent transaction has occurred after you notified your bank of the loss of your card, you will be only liable to pay a maximum of €50.

But it is important to note that you will not be entitled to any refund for losses relating to any unauthorised payment transaction if you incur such losses by acting fraudulently or by failing to fulfil your obligations with intent or gross negligence.

Complaints and Conciliation Directorate at the Malta Competition and Consumer Affairs Authority

You will find the website of the Complaints and Conciliation Directorate on this URL: **www.mccaa.org.mt/Section/Content?contentId=1193**

You can contact the centre as follows:

Online:	**info@mccaa.org.mt**
Online form:	**mccaa.org.mt/home/complaint**
Freephone:	**356 8007 4400**
In person:	**Malta: Mizzi House, National Road, Blata l-Bajda** **Gozo: Elizabeth Street, Xewkija, Gozo**

MORE INFORMATION ON SCAMS & FRAUD

If you wish to know more on scams and fraud, visit the following websites:

Cyber Security Malta: cybersecurity.gov.mt/

European Consumer Centre Malta:
eccnetmalta.gov.mt/consumer-information/e-commerce/how-to-shop-online-safely/

Malta Financial Services Authority:
www.mfsa.mt/consumers/scams-warnings/typical-scams/

Depositor and investor compensation schemes:
www.compensationschemes.org.mt/

ĠEMMA RESOURCES ON SCAMS AND FRAUD

ĠEMMA invites you to look at its videos (in Maltese) on scams and fraud:

Agħżel minn fejn tixtri bil-karta ta' kreditu
www.youtube.com/watch?v=9K8ZhFfaIJY

Mhux kulma jleqq hu deheb
www.youtube.com/watch?v=mSGdWioPnyI

Uża l-ATM b'mod sigur
www.youtube.com/watch?v=zzxzT5iszts

Ħares il-karta ta' kreditu tiegħek
www.youtube.com/watch?v=qJhFg8HblKM

ĠEMMA
know, plan, act.