Little Black Book of Scams & Frauds

PART I

eSkills
eSkills Malta Foundation

ĠEMMA
know, plan, act.

CONTENTS

eSkills
eSkills Malta Foundation

ĠEMMA entered into a strategic partnership with the eSkills Malta Foundation in July 2020. ĠEMMA and the Foundation will work together to issue new editions of ĠEMMA and eSkills Foundation Little Black Book on scams and fraud. The new editions will identify new scams and fraud and the emerging technologies that make them possible together with the eSkills required for persons to protect themselves.

First Edition, July 2020

INTRODUCTION

This e-book is ĠEMMA's Little Black Book of Scams and Frauds. The Little Black Book of Scams was first launched by the Australian Competition and Consumer Commission in 2012. The concept caught on. The Metropolitan Police Service in the United Kingdom and the Commission for Financial Capability in New Zealand have replicated the concept. As at 2019, The Little Black Book issued by the Metropolitan Police Service was in its fourth edition.

ĠEMMA too is replicating the Little Black Book concept. Rather than creating one comprehensive book which may be too much to read at one go, it will present a series. This is Part 1 of the series. ĠEMMA gives due recognition to the Australian Competition and Consumer Commission as well as the Little Black Books drawn up by the Metropolitan Police Service (UK) and the Commission for Financial Capability (New Zealand) which form both inspiration and basis for the ĠEMMA edition.

Why a Little Black Book of Scams and Frauds? Whilst the ĠEMMA Little Black Book series will present 'traditional-based' scams, such as cold telephone calling or door-to-door sales, with the event of the Internet, the smart phone, together with an increasingly

digital economy and society, scams and fraud are more and more becoming technology-inspired. Some frauds and scams are traditional but are carried out by and through technology – romance and dating schemes, for example. Others are technology-inspired and dependent – such as those dealing with vulnerable public Wi-Fi hotspots resulting in the hacking and stealing of information and data.

With many of these scams and frauds some knowledge on how you can protect yourself will go a long way toward keeping you safe from becoming a victim. Knowledge and tips on how to protect yourself against scams and fraud in Malta are fragmented. We too realised that we were creating content on scams and fraud in a non-structured manner.

Should you be aware of a scam or become the victim of one, and you want to report it, you are likely to feel lost – unless you know where to look. It took ĠEMMA time to source out who and where a person should report a scam. In putting together this first part of the ĠEMMA Little Black Book of Scams and Frauds we have sought to collaborate with authorities we believe have a role to play in scam and fraud reporting and action – so that we present to you the most comprehensive picture possible.

This e-book seeks to increase your knowledge and awareness of potential scams and frauds, and, in doing so, to empower you to take the necessary action not to be scammed and suffer financial loss. ĠEMMA 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 back, but in reporting it you may protect others from falling for the same scam**. ĠEMMA encourages you to share this e-book with your family, friends and colleagues.

THE ĠEMMA TEAM

ĠEMMA
know, plan, act.

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 the offer 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.

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 **Never send money to someone you do not know and trust.**
It is rare to recover money from a scammer.

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**

Pg 29, The Little Black Book of Scams, A pocket sized guide to spotting, avoiding and reporting consumer fraud, Australian Competition and Consumer Commission, 3rd Edition, Canberra, Australian Capital Territory, Commonwealth of Australia 2012.

Wi-Fi Hotspots

It is important that you keep in mind that not all Wi-Fi hotspots are secure. Wi-Fi hotspots are easy to hack. A criminal or an experienced IT user can easily capture your data from an insecure Wi-Fi network.

We advise you to take note of the following tips so that you protect yourself:

- Do not use public Wi-Fi for online banking, accessing e-mails or anything involving sensitive personal information.
- When doing this in public, use your 3G, 4G or 5G connection. Data passed over these connections is always encrypted.
- Make sure you are connecting to a trusted Wi-Fi hotspot, operated by the venue you are at. Ask staff if you are in any doubt.
- Use a Virtual Private Network (VPN) when connecting to public Wi-Fi. All your data will be encrypted and so, if it is intercepted, it will not be readable. VPNs can be downloaded onto devices as an app.
- Be aware of who is around you when you are using a public Wi-Fi.

Pg 7, The Little Book of Big Scams, Metropolitan Police Service, Mayor's Office for Policing and Crime and the Crown, 2019, Fourth Edition, United Kingdom.

HOLIDAY FRAUD

Most people today book their holiday online end-to-end – hotel, flight tickets, car, excursions, shows and concerts, museums, etc. You too are probably an e-tourist. As e-tourism has become big business, the scamming of online tourist-related bookings has become a significant area.

Unfortunately, you will probably realise that you have been scammed only at the point you get to board the plane, arrive at your accommodation, or present your pass for the show you are supposed to be attending.

Take note of the following tips so that you protect yourself:

- Scammers often ask for payment by direct bank transfer away from the website. To encourage you they may offer discounts for bank transfer payments.
- Scammers often use photos of accommodation taken from other sites on the web. Check the photos with a reverse image search engine that you will find on the Internet. Such engines check images to see whether they are used elsewhere on the Internet, e.g. **www.tineye.com** or **www.reverse.photos**.
- The scammers' advert may state that they belong to a trade body or a consumer protection scheme of the country you are thinking of visiting. Contact the body or scheme to check the credentials – you are likely to find their contact details on the Internet.
- If your are booking an accommodation try and call the owner of the property you shall be visiting.

Pg 9, The Little Book of Big Scams, Metropolitan Police Service, Mayor's Office for Policing and Crime and the Crown, 2019, Fourth Edition, United Kingdom.

MOBILE PHONE SCAMS

With smart phones being so affordable today we use mobile phones not only to communicate amongst ourselves but also to bank, shop, invest, and play skill games, amongst others. Although smart phones are mini-computers they do not have the processing power of a computer. Thus the security mechanisms on a smart phone are not as robust as those you get on your PC.

Take note of the following tips so that you protect yourself:

- If you use your app to carry out Internet banking, use only your bank's official app. If in doubt, check.
- Download apps only from official stores such as Apple iTunes and Android Marketplace.
- When the phone informs you that you have a new release of your phone's operating system, install this release. Amongst other matters, such releases address security vulnerabilities that would have been identified between one release and the other.
- Lock your mobile by a secure PIN number or password which you should not share with anybody else.
- There are anti-virus software tools for a mobile – use them insofar as these are from a reputable brand.
- Never click links contained on a text or email unless you are sure of the identity of the sender.
- You may receive an SMS saying that you have won a great prize – scammers make money by charging high rates for SMSs received from you. Do not reply. If the SMS asks you to call a number to claim your prize do not phone that number.
- 'Smishing' occurs when a scammer asks for your personal information. Do not reply back. No legitimate business will ask you to provide personal information over the phone.

Pg 23, The Little Book of Big Scams, Metropolitan Police Service, Mayor's Office for Policing and Crime and the Crown, 2019, Fourth Edition, United Kingdom.

INVESTMENT SCAMS

There are three types of investment scams:

(a) the investment offer is completely fake and does not exist;

(b) an investment offer does exist, but the money you give the scammer is not going towards that investment; and

(c) the scammers say they represent a well-known investment company, but they are lying.

Take note of the following tips so that you protect yourself:

- Find out the legal name of the business you are dealing with.
- Check that the business is regulated by the Malta Financial Services Authority.
- If the business is not based in Malta, find out who regulates it.
- Check the regulator's warning lists.
- If you have lost money through a scam, you are highly likely to be targeted again.
- Take your time when making investment choices. Be careful of "act now" or "before it's too late" statements.
- Say "no" to anybody who tries to pressure you or rush you into an investment.
- Be wary of salespeople who prey upon your fears or promise returns that sound too good to be true.
- Always ask for a written explanation of any investment opportunity, and then shop around and get a second opinion.
- Be wary of any financial adviser who tells you to leave everything in his or her care.
- Never invest in a product you do not understand.
- If the investment sounds too good, then it probably is too good to be true.

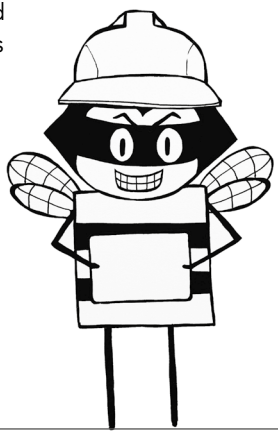
https://www.moneysmart.gov.au/scams/investment-scams

Identity theft

Identity theft is the deliberate use of your identity in order to take over or open new accounts, buy goods online, carry out online gaming or rent or buy properties or do other criminal things in your name.

Take note of the following tips so that you protect yourself:

- Never provide your personal information over the phone, via text message, email or the internet.
- Avoid public computers or Wi-Fi hotspots, such as in coffee shops, to access or provide personal information; they put you at risk.
- Create strong and unique passwords for each of your online accounts. Password-protect your devices and home Wi-Fi network.



- Use 2-Factor Authentication.
- Update your computer operating system.
- Use a secure and reputable payment service when buying online – look for a URL starting with "https" and a closed padlock symbol.
- Avoid giving out personal information on social media. It can be used along with your pictures to commit fraud.
- Always shield your PIN when using your card. If you hand it over to a cashier, never lose sight of it.
- Shred and destroy documents with personal information.
- Protect your mobile phones.
- Do not open any message that comes from an unfamiliar source. If you open a suspicious message, delete it. Do not click on links or call telephone numbers provided in the message. Be wary about opening attachments.

Pg 4, The Little Black Book of Scams, Commission for Financial Capability, Auckland, New Zealand

ROMANCE & DATING FRAUD

The Internet has given rise to a new way of meeting up with a partner – through the use of romance and dating sites as well as through social media such as Facebook. Amongst the genuine sites and people you come across in the digital world there are those who will cynically create a false persona or profile to get you romanced, play on your emotions, and ultimately steal your money.

Take note of the following tips so that you protect yourself:

- If you are using a romance and dating website to meet up with a partner, carry out research on that site. On the Internet you will find sites that will tell you which sites are legitimate and which carry out intensive checks before accepting a person to post their profile on the website.
- Be cautious about who you communicate with online. Before you get into any serious discussions, check out whether the person is for real. On the Internet you will find sites which blacklist persons who have been carrying out romance scams.
- Do not be convinced by the profile pictures – they may be stock photos or taken from other sites. You can check photos using a reverse image search on the Internet, e.g. **www.tineye.com** or **www.reverse.photos**.

Pg 13, The Little Book of Big Scams, Metropolitan Police Service, Mayor's Office for Policing and Crime and the Crown, 2019, Fourth Edition, United Kingdom.

- Some of the scams are very sophisticated: the messages are written to trigger your emotions, you are introduced to family members, etc. If the person asks you for money, even after you have spent months building the relationship, e.g. claiming that s/he has been robbed or needs to sort out some health issue, the chances are that this relationship is a scam. Do not respond to requests or hints for money and stop all contact immediately.
- If you find that you are getting serious with a person, the best thing to do is to meet that person in person – and that the person you are meeting pays for his/her travel costs.
- Never send money or give financial details on a dating site: this is a person you do not know, and in truth can be anyone.
- Avoid giving your personal details that could be used to impersonate you.
- Keep all communication on the dating website you are using.

DEBIT & CREDIT CARD FRAUD

A **DEBIT CARD** is a card issued by your bank which allows you to carry out a payment electronic transaction from your current or saving account – that is, you are using your own money, but rather than paying in cash you are paying by card. You can use your debit card both locally and overseas – and it is accepted by most establishments.

A **CREDIT CARD** is a card that can be provided either by your bank or by any other bank that accepts your application and enables you to carry out an electronic payment transaction for a 'loan' provided to you by the bank that issued it. Debit and credit card fraud, therefore, is when someone makes use of your debit or credit card to make purchases without your authorisation.

Take note of the following tips so that you protect yourself:

- Report lost or stolen cards immediately to the bank that issued you the card.
- In order that you can respond quickly in case your cards are lost or stolen, keep the following details: credit card name, card number, expiry date, 24-hour customer service number.
- Sign your card on the signature panel as soon as you receive it.
- Protect your cards as if they were cash – never let them out of your possession or control.

- Do not include your card number in an email.
- Do not give out your card number over the phone.
- Do not leave your credit cards in your car's glove compartment.
- Do not lend your cards to anyone. You are responsible for their use.
- Choose a personal identification number (PIN) that is easy for you to remember but difficult for others to guess.
- Never tell anyone your PIN. No one from a financial institution, the police, or a shop should ask for your PIN. You are the only person who needs to know it.
- Do not volunteer any personal information when you use your cards.
- Never write down your PIN – memorise it.
- When typing in your PIN, cover the keypad so others cannot see it.
- Always make sure that sales vouchers are for the correct purchase amount before you sign them.
- Always keep copies of your sales vouchers, credit card and ATM receipts.
- Always check your billing statement to make sure the purchase amounts are correct and that there are no suspicious charges.
- Ask whether your bank has a service that automatically texts you when the card is used. If it has, activate it.
- Always put disputes regarding your billing statements in writing immediately upon becoming aware of the disputed item.
- Read your credit card agreement and billing statements carefully for information regarding dispute notification requirements. You may also contact your credit card issuer to ask about their dispute notification requirements.
- If you receive a replacement card, destroy your old card. Destroy cards for cancelled accounts.
- Shop with retailers you know and trust. Make sure internet purchases are secured with encryption to protect your account information. Look for "secure transaction" symbols.

Internet banking fraud

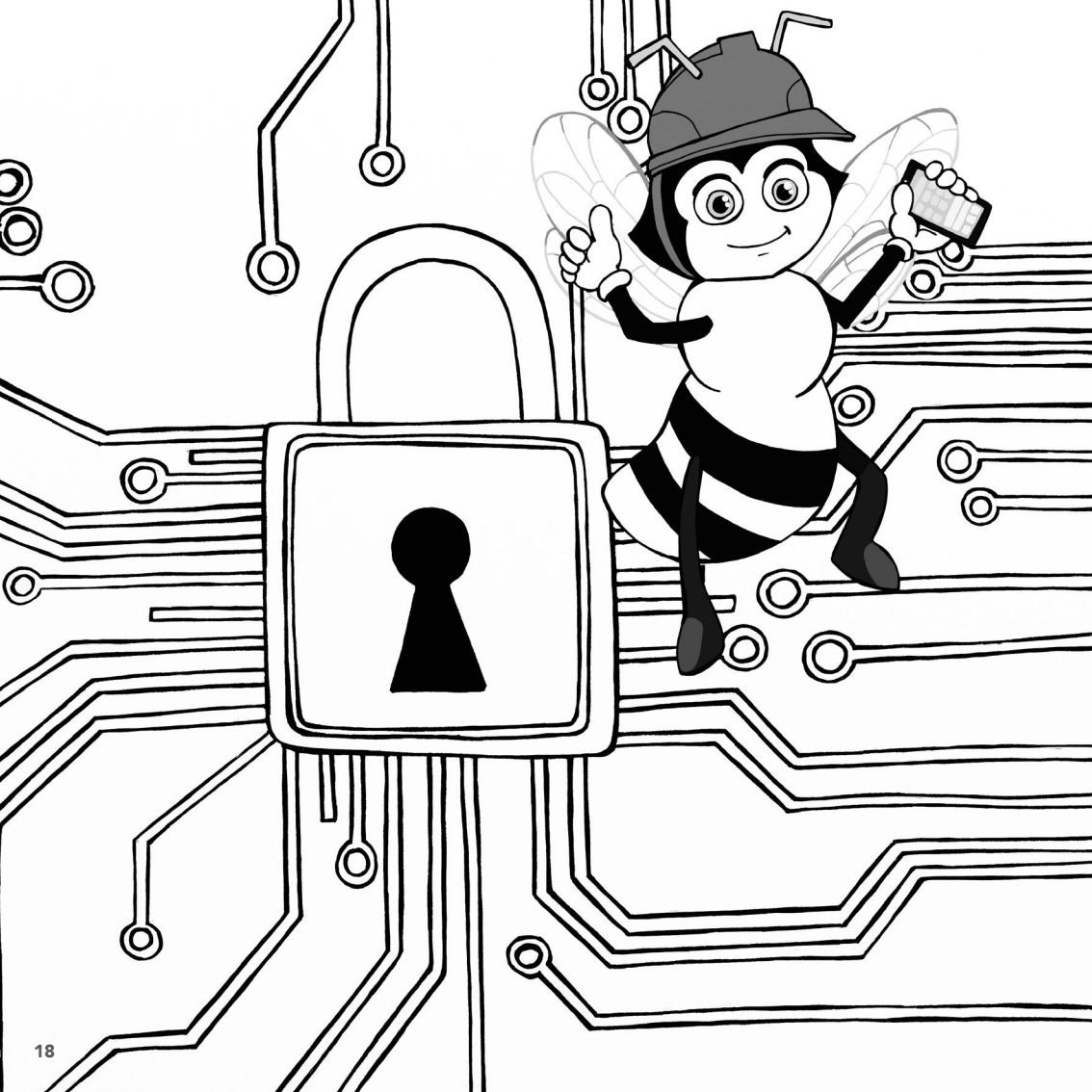
Internet banking fraud is a fraud using the Internet or mobile phone technologies to illegally remove money from your bank account and / or transfer money to an account that does not belong to you.

Take note of the following tips so that you protect yourself:

- Ensure that your bank provides you with a two-tier authentication mechanism – a 'token' gadget which creates a unique code.
- Make sure that your password is eight or more characters and combines letters, numerals and symbols.
- Access your accounts from a secure location, using computers and networks you know are safe and secure. Avoid using public networks.
- Always look for the padlock icon in the corner of the browser, signalling that the website is encrypted.
- Always log out and clear your computer's cache at the end of each session.
- Set up account notifications to immediately alert you if there is any suspicious activity on the account, such as large withdrawals or a low remaining balance.
- Never respond to urgent email claiming to be from a bank or any company that requests your account information or personal details.

- Limit the amount of personal information you provide on social networking sites. The more information you post, the easier it may be for a criminal to use that information to steal your identity, access your data, or commit other crimes.

- Be cautious about messages you receive on social networking sites that contain links. Even links that look like they come from friends can sometimes be harmful or fraudulent – and in fact may be attempts to gain control of your computer or steal your personal information. If you are suspicious, do not click the link.
- Keep your computer operating system and browser up-to-date with the latest software and security downloads.
- Do not open attachments or install free software from unknown sources; this may expose your computer and the information on it to unauthorised sources.
- Install a comprehensive firewall / antivirus / anti-spyware software package on your computer. These software suites help detect and remove viruses and spyware that can steal vital information.



HOW TO

PROTECT YOURSELF FROM SCAMS & FRAUD

We suggest that every 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
https://www.mfsa.mt/consumers/scams-warnings/typical-scams/

MFSA Warnings

On this page the MFSA warns the general public with regard to unlicensed entities that claim to operate from Malta. You are to 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

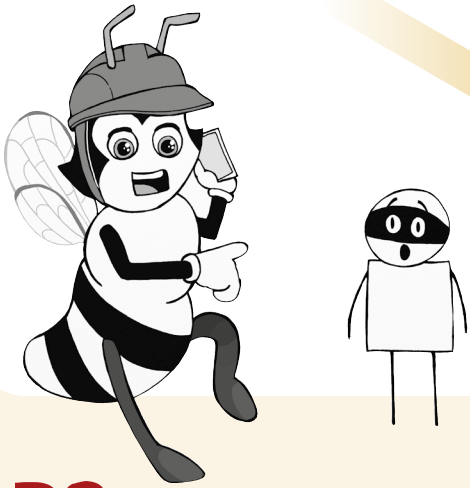
Consumer Notices

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 attention of investors the names of 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 the 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 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:
https://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 you were the target 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, contact your bank immediately. Do the same if you lose your debit or credit card.

The revised Payment Services Directive (PSD_2) 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 are only liable to pay a maximum of EUR 50. It is, however, important to note that you will not be entitled to any refund for losses relating to any unauthorised payment transaction if you have incurred 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 Directorate 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: St 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 VIDEOS ON SCAMS & FRAUD

(in Maltese)

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.

DEFINITIONS

WI-Fi hotspots
A WiFi hotspot is simply an area with an accessible wireless network. The term is most often used to refer to wireless networks in public areas like airports and coffee shops. Some are free and some require fees for use, but in either case they can be handy when you are on the go.

Virtual Private Network (VPN)
A VPN creates a secure connection between you and the internet and helps you to secure and remain anonymous on line.

2-Factor Authentication
This adds a second layer of protection. The first is a password. To be able to log you need to input another password. Normally this is a number sent to you on your mobile or another email address. You need to input this number to log in.

Reverse image search
Reverse image search is the uploading of a specific image instead of a keyword when you want to search for something on the Internet.

Computer's cache
Cache, which is pronounced "cash", stores recently used information so that it can be quickly accessed at a later time.

www.gemma.gov.mt
www.eskills.org.mt