Little Black Book of Scams & Frauds

PART 2

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 is the second e-book in the series of ĠEMMA's Little Black Book of Scams and Frauds. This second e-book retains the same format as the first e-book, in that it presents eight scams and frauds, and information that you should know with regard to how to protect yourself, what to do if scammed, where you can obtain further information, and ĠEMMA information and resources on scams and frauds.

ĠEMMA
know, plan, act.

Whilst it builds on the first e-book it is designed to read as a stand-alone. If this e-book is your first time that you are accessing ĠEMMA's Little Black Books of Scams and Frauds you can download the other e-books in this series from the following URL: https://gemma.gov.mt/gemma-e-book-the-little-black-book-of-scams-frauds/.

The first e-book explored the following frauds and scams and presents tips on how you are to protect yourself against each of these scams and frauds:

- Wi-Fi hotspots
- Holiday fraud
- Mobile phone scams
- Investment scams
- Identity theft
- Romance and dating fraud
- Debit and credit card fraud
- Internet banking fraud

This e-book discusses the following frauds and scams, and offers you tips to protect yourself:

- ATM use fraud
- Elderly relatives financial fraud
- Cold Calling scams
- Business e-Mail compromise fraud
- Phishing, Vishing, Smishing and Pharming scams
- Subscription traps
- Social Engineering

ĠEMMA's series of Little Black Books of Scams and Frauds is based on 'The Little Black Book of Scams' concept that 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
know, plan, act.

The objective of ĠEMMA's series of Little Black Books of Scams and Frauds is to make you familiar with the many scams and frauds that are perpetuated and equip you with some knowledge on how you can protect yourself. Indeed, knowing what to look for and some basic tips to follow go a long way towards keeping you safe from becoming a victim.

This e-book, together with the other e-books in ĠEMMA's series of Little Black Books of Scams and Frauds, are designed to increase your knowledge and awareness of potential scams and frauds, and, in doing so, to empower you to take the necessary action so that you are not 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

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. Avoid installation of illegal software copies.

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.**
The introduction of new financial services (e.g. sending money through mobile phones) makes it easier to send money. Make sure identity of receivers is verified. 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**

ATM USE FRAUD

Just like any computer device, ATMs have vulnerabilities. Thus they are open to being hacked. The majority of ATM frauds involve a level of physically manipulating parts of the machine or introducing devices.

Scams can include:

- **Skimming**: this normally involves the installation of a card reader device (skimmer) and a keypad overlay or pin hole camera which are placed over the card slot and key pad respectively. The purpose of the second reader is to copy data from the card's magnetic stripe and PIN – which will then be used to forge a card.
- **Shimming**: A shimming device is inserted in the ATM's card slot – between the card and the ATM chip reader. The device records data from the card chip whilst this is being read by the ATM machine. The stolen data is then converted to a magnetic stripe which is then used to create a fake version.
- **Card trapping**: The objective here is to physically capture the card whilst in the ATM machine. This is achieved by introducing a device that prevents the card from being ejected once your transaction is completed. Your PIN number is stolen either by shoulder surfing or through the use of a small hidden camera similar to that used in skimming.
- **Cash trapping**: This is like card trapping, but in this case the target is your cash. This normally achieved by the placement of a fake cash dispenser in front of the real one.
- **Snooping:** This is the snooping of keyboard clicks and credit card info by shoulder viewing or using strong binoculars in nearby overhead windows. The information snooped can be used by illegal replication of cards or online purchases.

How do you know whether an ATM machine has been tampered? Here are some tips:

- Tug on the card reader and cash dispenser to make sure that there are no extra devices attached.
- Look for false fronts – such as overcard and money slots, keypad or, worse, the entire ATM machine.
- Look for tiny holes where cameras could be watching.
- Look for mismatched key colours.
- Look at whether the green flashing light below or above the card slot is blocked by a false device.
- Check whether the bank's signage is correctly spelt.
- If the ATM has not given you the cash, stay beside the machine and call your bank's call centre and immediately terminate your card.
- If the ATM has not given you the cash and you cannot, for some reason, get through to your bank's call centre, record the exact date, time and ATM location and take a number of photos.
- If you are using a stand-alone ATM at a store or shopping centre alert an employee at once.

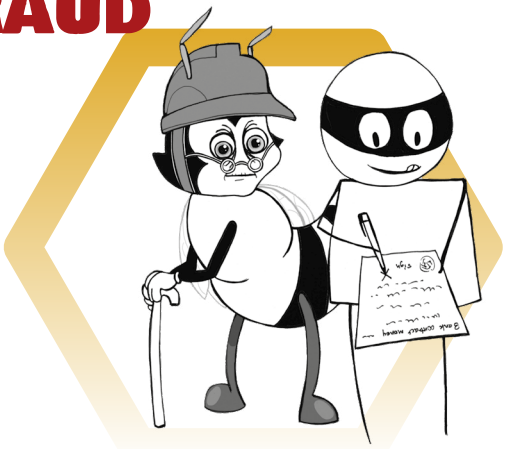
In using an ATM minimise the likelihood of being scammed by following these tips:

- Think about your personal safety when using an ATM.
- When you are by yourself, avoid using an ATM in out-of-the-way or deserted areas.
- Be aware of your surroundings when withdrawing funds.
- If a suspicious person offers to help you use the ATM, refuse and leave.
- When typing in your PIN, cover the keypad so others cannot see.
- After completing your transaction, remember to remove your card, cash and any printed documents such as receipts or statements.
- Put your money and ATM card away before you leave the ATM. Always avoid showing your cash.
- Always verify that the amount you withdrew or deposited matches the amount printed on your receipt.

- Take your receipts with you so potential criminals will not know how much you withdrew and use this to guess how much money is in your account.
- When using a drive-up ATM, keep your car doors locked and your engine running.
- Do not allow yourself to be rushed by an impatient person who is waiting for his or her turn at the ATM.

Elderly relatives financial fraud

Elderly fraud is when someone illegally or improperly uses an elderly person's finances or assets – characterised by the targetting of a person's vulnerability because of his or her age.



The following are characterised as elderly fraud:

- Taking your money or property.
- Fraudulently signing on your behalf or forging your signature.
- Deceptively coercing or using undue influence to get you to sign a deed, will, or power of attorney.
- Taking or using your possessions without your permission.
- Promising you long-term (even lifelong) care in return for your money or property and then not fulfilling the promise or short changing you in the process.
- Stealing physical possessions from your home.
- Deceiving you to gain your confidence such as 'new best friends' and 'sweethearts'.
- Gaining access to you as caregivers, counsellors, or other professional service providers.
- Seeking you out as a vulnerable widow or widower by reading obituaries, driving through your neighbourhood to see whether you live alone or are isolated, and establish a relationship with you through your network, e.g. at church or local activities.

As a relative of an elderly vulnerable person there are certain factors that you can look out for to make sure that your father, mother, grandparent, etc. is not the target of financial abuse.

Of note, look out for:

- Unusual or large withdrawals or transfers from bank accounts, or large credit card charges that your relative cannot explain.
- Cheques that are missing or include suspicious signatures.
- Strangers that suddenly form a close relationship with your elderly relative, gaining easy access to his or her home, money and other property.
- Newly executed documents, such as a will or power of attorney that your elderly relative does not understand.
- Changes in account beneficiaries or authorised signers.
- A large number of unpaid bills.
- Missing property.
- Signing or cashing of pension and social security benefits cheques without permission.
- Untreated physical or mental problems, including a dramatic change in mood or disposition, or other evidence of substandard care.
- Hold a financial meeting with your elderly relative on an ongoing basis.
- Watch out for signs of dementia and loss of cognitive abilities.
- Establish a system for your elderly relative for payment of recurrent expenses such as Internet or utility bills to be paid electronically automatically.
- Cancel for your elderly relative unused or extra credit and debit cards.
- Monitor on behalf of your elderly relative his or her bank and credit statements regularly.

COLD CALLING SCAMS

Cold calling scams consist of uninvited door-to-door visits or telephone calls to sell you goods and services.

This is a well organised method that places you on the spot when you least expect it and your guard is down, and pressures you in purchasing a good or service – using the techniques of persuasive selling and preventing you from having the time to think about the sale, normally by offering you significantly lower prices than if you had to make a purchase in your own good time.

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

- Place a sticker saying that cold callers are not welcome and will be reported.
- Terminate a door-to-door or telephone cold call immediately.
- Give no information – and 'no' means absolutely nothing.
- If telephone cold callers state that they are from, for example, your bank or a utility, insisting that they have important information or that there is an issue they wish to discuss, terminate the call and call the firm directly yourself.
- If you decide to talk to them, take your time. Do not allow yourself to be pressured. And if they are using aggressive sales techniques offering you fantastic discounts, remind yourself that when an offer looks too good to be true, it normally is not true.
- Ask for the caller's photo ID, get the name of the person and of the company they represent.
- Research before you invest. Do not sign anything, and always read the fine print.
- Never judge a person's trustworthiness by the sound of their voice.
- Set up call barring for unwanted calls.
- Do not automatically respond to numbers you do not know. Ask the caller to introduce him / herself.
- Do not sign anything – even if they are offering a quote.
- Report cold calling offenders.

Business e-Mail Compromise Fraud

A business email compromise (BEC) fraud is an online scam where the scammer impersonates a business representative and tricks you into transferring money or sensitive information.

The scammer impersonates a trusted person using an email that is almost identical to the trusted person's name, or a domain that is identical to the name of the trusted person's company. The scammer sends a legitimate message to you requesting money or sensitive information.

There are four basic forms of BEC fraud:

- **Executive fraud**:
  The scammer masquerades an executive's email address and then sends a message to staff in your business directing them to transfer funds to the scammer's account.
- **Legal impersonation**:
  The scammer masquerades as a lawyer or legal firm representative requesting payment for an urgent and sensitive matter.
- **Invoice fraud**:
  The scammer masquerades as a trusted supplier and sends a fake invoice to your business. In these scams, the scammer often has control of the supplier's email account and can access legitimate invoices. The scammer changes these invoices to include new bank account details and then sends the invoices to customers from the supplier's email account.
- **Data theft**:
  Instead of requesting funds, a scammer may masquerade as a trusted person to request sensitive information. This information can then be used also as part of a larger and more damaging scam.

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

- The email was unexpected. For example, the invoice came from a supplier you have not dealt with in a while, or the payment amount differs from previous amounts.
- The email asks for an urgent payment or threatens serious consequences if payment is not made.
- The email was sent from someone in a position of authority, particularly someone who would not normally send payment requests.
- The email address does not look quite right. For example, the domain name does not exactly match the supplier's company name. Double-check by looking at previous correspondence.
- The supplier has provided new bank account details.
- Teach your team to recognise and deal with **phishing** attacks as well as to report emails that request any sort of financial transaction. Promote refresher training frequently.
- If possible apply impersonation detection protection. This instantly scans all aspects of an email: header, sender, attachments and key words, paying special attention to new domains and external addresses, and establishes controls to thwart look-alike domains.
- Always verify. It always pays to confirm details with the parties involved, especially when it comes to messages that involve fund transfers.
- Instead of clicking on Reply, use the Forward feature and type in or select from your contacts list the e-mail address of the person you are replying to. This is to ensure that you are not replying to a spoofed address.
- Use two-factor authentication to verify any change made to account information or wire instructions.
- Check the full email address on any message and be alert to hyperlinks that may contain misspellings of the actual domain name.

Phishing, Vishing, Smishing and Pharming Scams

These scams are described below, including tips which you should take note of so that you protect yourself.

1 PHISHING

You are targeted via email whereby you are encouraged to click through to fraudulent sites, give personal information about yourself or even send money. The scams vary widely but a majority of them are fairly easy to spot.

What to look out for:

- Do you know the sender of the email? If not, do not open and do not click on any internal links. If you do, still be cautious.
- Are there any unrequested / unexpected attachments? If so, do not open before contacting the sender via another means to verify contents.
- Are there any grammatical errors or spelling mistakes? If so, be wary.
- Does the email ask for personal information? If so, ignore it.
- If you are associated with the business in question, are they addressing you by name?
- Check any and all links by hovering the cursor over it to see the URL. Will it take you to the expected website or a different one?

2 VISHING

You are contacted over the phone to extract personal information or to trick you into giving access to your computer or accounts. A common scam: you receive a call from Microsoft informing you that your computer is compromised and that you must download software to solve the problem. The software is sent via email, and if the file is opened malware is downloaded onto your computer.

What to look out for:

- Never give personal information over the phone to an unverified source. Companies like Microsoft will not contact you personally to warn you about malware but release frequent updates / patches to protect your machine from viruses.
- If you receive an unexpected request via email, text message or phone call to take some kind of action, the best course is to check the company's details via their website and take any actions using those details.
- If you are in any doubt about correspondence received, send it on to the customer service or security of the company in question to verify it.

3 SMISHING

This is short for SMS phishing and it works much the same as phishing. You are tricked into downloading a Trojan horse or virus onto your phone from an SMS text as opposed to from an email onto their phone.

What to look out for:

- Avoid clicking on links within text messages. It is even possible for scammers to piggy-back onto existing message threads from trusted sources, like your bank. Double check all sources before sharing personal data or moving money if prompted to do so by text message.
- Do not respond to messages that request private or financial information from you.
- Be wary of urgent messages that require immediate action. If it is your bank, call the number on the back of your card.
- Never call a phone number from an unidentified text.

4 PHARMING

This scam uses domain spoofing (in which the domain appears authentic) to redirect you to copies of popular websites where personal data, like your name, passwords and financial information can be 'farmed' and collected for fraudulent use.

What to look out for:

- Check the URL of any site that asks for any personal information. Ensure that the session begins at the known address of the site without any additional characters.
- Install a trusted anti-virus on your computer.
- Do not disable or weaken your computer's firewall. Also allow regular updates to further protect your machine.
- Use a reliable and legitimate Internet Service Provider because significant security is needed at the ISP level as a first line of defence against pharming.

SUBSCRIPTION TRAPS

A subscription trap takes place when you sign up on-line for free or low-cost trials of products or services – only to find yourself unwittingly locked into cost repeat payments.

The subscription trap scam exploits a 'continuous payment authority' normally by requesting your payment card details as proof of identity and age, then retaining those details to draw monthly payments from your account. Details of this on-going commitment are generally buried in the terms and conditions and are missed by many people eager, instead, to take advantage of the 'fantastic offer' being advertised.

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

- Read the small print (terms and conditions) carefully before entering into any agreement or making a purchase, however long this may take.
- Make sure the terms and conditions box has not been pre-ticked.
- Be clear how you back out. If you make a purchase of this kind that gives you a limited timescale to cancel the agreement, make sure you do so before the due date if you want to cancel it.
- Never provide bank or debit / credit card details to companies without doing some prior research beforehand.
- Check your bank / payment card statements regularly for unexpected payments.
- Contact your bank to cancel future payments.
- Ascertain with your bank whether a new card is needed.
- Trust your instincts. If it is too good to be true, do not sign up.
- If you go ahead with a free trial, keep all documents, receipts, emails and text messages.

HOW TO

PROTECT YOURSELF FROM SCAMS & FRAUD

We suggest that ever so often you visit the web page titled 'Scams Detection & 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 about 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 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:
https://www.mfsa.mt/consumers/scams-warnings/consumer-notices/

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 €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

Shoulder surfing
This occurs when someone watches over your shoulder or listens to your conversation or password, ATM PIN, or credit card number, as you key it into a computer, tablet or mobile.

Compromise fraud
Somebody obtains access to a business email account and imitates your identity in order to steal from your company and its employees, customers or partners.

Pharming scams
Pharming is a form of e-mail virus that directs you to a fake website which mimics a real site in order to steal (pharm) your personal data, such as passwords or financial detail.

Domain spoofing
E-mails containing virus are sent you from what seems to be a real company. Once you open the mail a virus is inserted in your computer. Once inside, the thief can take your personal and financial information as well as that of the company and other employees.

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.

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