

# LITTLE BLACK BOOK OF SCAMS & FRAUDS

## PART 3



**GEMMA**  
know, plan, act.

# CONTENTS

Introduction .....	3
How A Scam Works .....	5
The 10 Commandments to protect yourself against scams and fraud.....	8
Nigerian Scams.....	11
Contactless Card Fraud .....	13
Computer Service Fraud .....	15
Work-From-Home Job Scams .....	17
Lottery and Prize Scams .....	19
Extortion Scam .....	22
Facebook Scam .....	25
How to protect yourself from scams and fraud .....	28
What to do if you get scammed.....	30
More information on scams and fraud .....	33
GEMMA Resources on scams and fraud .....	33

# INTRODUCTION

**GEMMA has teamed up with the e-Skills Malta Foundation, and together we are pleased to bring to you its third e-book in its series of Little Black Books of Scams and Fraud. In this new Little Black Book we introduced an addition to the first two e-books issued in this series.**



GEMMA has included a new section titled 'How a Scam Works'. This new section presents the following:

- The Scammer's approach
- Communicating and grooming you
- Sending the money

The section relating to the 10 Commandments now also includes a number of important facts. We also include, where possible, examples of frauds and scams. Otherwise, the e-book

remains unchanged. In this third e-book we present and discuss the scams shown below, identify what you should look out for, and the action you should take:

- Nigerian scam
- Contactless cards fraud
- Computer Service fraud
- Work from home fraud
- Letter of credit scam
- Extortion scam
- Facebook scam
- Non Delivery of Merchandise

Although scams and fraud are effected both in traditional manner – a service paid by a stolen cheque, for example – and over the Internet, the fact is that the majority of fraud now not only occurs over the Internet but is increasingly more sophisticated.

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

- Stop and think when you are confronted by 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.

Although they are rarely headline news on the media, scams and fraud are very real – leaving people financially as well as psychologically poor.

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 you can protect yourself, present you with resources you may look up, and where you should report should you need to do so.

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

**THE GEMMA AND E-SKILLS MALTA  
FOUNDATION TEAM**



# HOW A SCAM WORKS

**Most scams follow the same pattern – understand this pattern and it 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. S/he targets your emotions and behaviour – 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, a lovely lady.

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.

---

#### **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 – sending the money or providing 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 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

GEMMA 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 – 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 is a tell-tale sign that it is part of a scam. And if you do hand money, it's rare to recover it.

**9****Protect your identity.**

Your personal details are private and invaluable. Keep them that way and away from the scammer.

**10****If you have spotted a scam, spread the word.**

Tell your family and friends, and report it to [computer.crime@gov.mt](mailto: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 always not true that all websites are legitimate. It is easy and cheap to set up a website. And an enterprise's website can easily be copied and trick you into being 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.



# NIGERIAN SCAMS

**One of the oldest and most popular Internet scams is used mostly by a member of a Nigerian family with wealth to trick different people. It is also known as “Nigerian 419”, and named after the section of Nigeria’s Criminal Code which banned the practice. This type of fraud is also known as an “advance fee” fraud.**

A typical Nigerian scam involves an emotional email, letter, text message or social networking message coming from a scammer (who can be an official government member, a businessman or a member of a very wealthy family member – and not necessarily, but possibly, from other countries, usually where there is a form of conflict – such as a Syrian banker or a U.S. soldier in the Middle East) who asks you to assist in retrieving a large sum of money from a bank, paying initially small fees for documents and legal matters. In exchange for your help, they promise you a very large sum of money. They will be persistent and ask you to pay more and more money for additional services, such as for transactions or

transfer costs. You will even receive papers that are supposed to make you believe that it is all for real. In the end, you are left broke and without any of the promised money. The FBI reports annual losses of millions of dollars to these schemes. Some victims have been lured to Nigeria, where they were imprisoned.

You have to watch out for the following warning signs:

- You get an unsolicited email from someone claiming to be a foreign dignitary or senior executive.
- The email promises you a share of a multimillion £, \$ or € fortune in exchange for helping get the money out of the sender’s home country.





*This is an example of a Nigerian scam letter:*

Dear Beloved Friend,

I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.

I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US\$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.

I am here seeking for an avenue to transfer the fund to you in only you're reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent's and I want you to help me transfer the fund into your bank account for investment purpose.

Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent's. Reply to my alternative email: [missnaomisurugaba2@hotmail.com](mailto:missnaomisurugaba2@hotmail.com), Your immediate response would be appreciated.

Remain blessed,

Miss Naomi Surugaba.

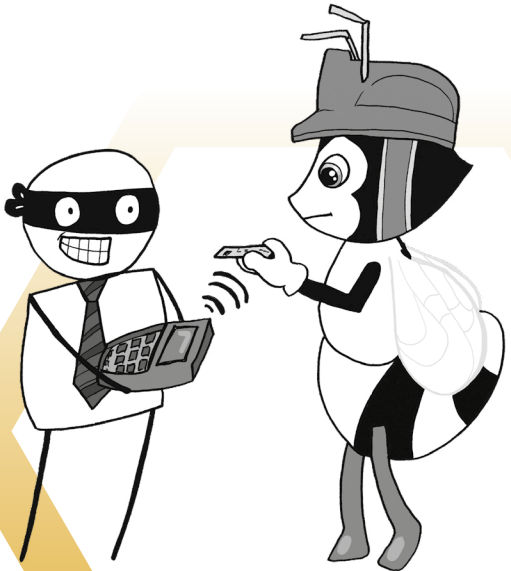
### **How to protect yourself:**

- Be sceptical of any promise of a huge payoff for your cooperation in such a fund-transfer scheme.
- Do not believe the promise of large sums of money for your cooperation.
- Do not reply, even out of curiosity, to emails (or to any form of communication).
- Do not provide personal or financial information to the person making such an appeal.
- Do not agree to send money by wire transfer, international fund transfer, or cryptocurrency to the sender of the email.
- Think: why should a stranger give me such a large amount of money? Remember: what is too good to be true is probably not true.

# CONTACTLESS CARD FRAUD

**Contactless card payments are hugely popular in Europe and the UK. Contactless card payments involve transactions that take place without you having to give your card to the seller to process the transaction.**

Several countries in the EU and elsewhere are raising the spending limits permitted by the cards. Contactless cards are now offered by local banks, and persons and businesses are accepting and making use of contactless card. Contactless cards are relatively safe compared to regular payment cards. Contactless card fraud occurs at less than half the rate of overall card fraud. Contactless fraud reached £20.6m during 2019 in the UK alone – 3.3% of overall card transactions. So far, most contactless payment fraud has been carried out through unsophisticated means, namely, by stealing the credentials or devices directly and using them to make purchases.



This does not mean that contactless payment is inherently more secure. As the € limit increases, fraudsters will be trying harder than before to test their defences and seek out vulnerabilities. Contactless cards are based on new technology. And as the use of contactless cards increases, the efforts of fraudsters to find ways of how to bypass the security features are likely to increase. Indeed, researchers in 2019 were able to show how to bypass the UK's then £30 (€32.7) limit for contactless payments made using physical cards, among other hacks. In follow-up research in later 2020 it was shown how it was possible to bypass multi-factor authentication controls designed to guard against tap-and-go fraud with contactless credit and debit cards.

It is thus important that you are vigilant in the use of your card. You may wish to protect yourself by taking the following steps:

- Do not keep your cards in easily accessible pockets or bags which will draw pickpockets' attention.
- Do not let anyone take your card out of sight while taking a payment – even for just a few seconds. They could be using a skimming device to copy data from your card's magnetic strip.
- Do not give your friends your card to make payments – always make sure you are there for all transactions.
- Ask for a receipt to make sure you were charged the correct amount.
- Keep a close eye on bank statements and your credit report to look for any unusual activity.
- Report any lost or stolen cards as quickly as possible and get the card immediately blocked.

# COMPUTER SERVICE FRAUD

**Scammers use many different tactics to trick you. Spotting these tactics will help you avoid falling for the scam. These include:**

## 01. Phone Calls

A Computer Service or Tech Support scammer may call and pretend to be a computer technician from a well known technology company, such as Microsoft or Apple. The alleged tech support representative falsely claims that your computer is infected with a virus. Scammers prey on your fear that you will be hacked. The scammer will walk you through the process of installing applications that allow remote access to your computer. The goal is to get you to pay, in the form of a one-time fee or subscription, to fix the problem and, while connected, the scammer may install malware (malicious software), such as a virus, or spyware that can steal

information from your computer, such as bank account information and online passwords.

**Action:** This may include:

- If someone claiming to be a representative calls you, hang up. Microsoft, Apple and all other brands do not initiate contact via phone or email messages to fix your computer issues. None of these firms include phone numbers on their error and warning messages. Put down the phone!
- Never allow anyone to remotely access your computer unless this is from your office IT support.



## 02. Pop-up Warnings on Your PC

Scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites. The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

**Action:** This may include:

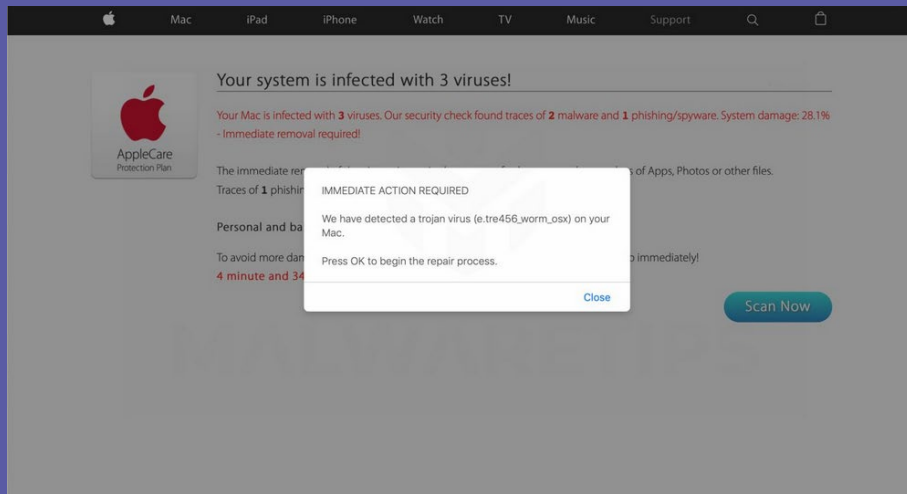
- Installing software like Adblock that blocks pop-ups at the first instance.
- Getting rid of a fake virus alert message by shutting down your browser. On Microsoft you can do this on a Windows PC by pressing Control-Alt-Delete and bringing up the Task Manager. On a Mac, press the Option, Command and Esc (Escape) keys, or use the Force Quit command from the Apple menu.

- You may come across pop-ups that will not go away, pages that infinitely reload, and ads that crash your browser altogether. Force-quitting the browser app is usually enough to get around this type of scam.
- Always have an antivirus program installed on your computer and use the antivirus software to regularly scan your computer for malware. Run a scan immediately after getting a scam pop-up.
- Do not click on any pop-up that tells you to install software to remedy an issue as this is trying to infect your system or steal money from you. This is a common tactic a scammer uses to install fleeceware on unsuspecting victims.
- Do not call the number in a pop-up alert. Real warnings from your operating system or antivirus program will not ask you to call anyone for support.
- Make sure you download security software from official vendors only.





*This is an example of what a pop-up scam may look like:*



# WORK-FROM-HOME JOB SCAMS

**Identifying work-from-home scams can be tricky, especially because they often appear alongside legitimate opportunities on popular job-search websites.**

Typical plays invite you to get to work stuffing envelopes, processing billing forms for medical offices, filling out online surveys, doing typing or data entry, or assembling crafts. The common thread is that you will be asked to pay something upfront for supplies, certifications, coaching or client leads. In return you may get a load of useless information, or nothing at all, or a demand that you place more ads to recruit more people into the scheme.

There are genuine work-from-home jobs out there. The trick is knowing how

to spot the real opportunities in a sea of empty – and costly – promises.

## **Look for the following warning signs:**

- A job ad claims that no skills or experience are required.
- It offers high pay for little or no work.
- A company promises that a business opportunity is sure-fire and will pay off quickly and easily.
- You are required to pay upfront for training, certifications, directories, or materials.



- The employer wants to urgently hire you.
- You do not speak with or see a real person – everything is done through e-mail or on-line chat.
- A generic email account is used like Gmail, Yahoo, etc.

### Action you may take:

- Ask detailed questions. How will you be paid? By salary or by commission? Who will pay you, and when will the cheques start? What is the total cost of the programme, and what will they get for your money?
- Do not stick around if there is any suggestion that your earnings are based primarily on recruiting other people to join the operation – if so, it is probably a pyramid scheme.
- Do not assume a work-at-home offer is honest just because you saw it in a trusted newspaper or on a legitimate job website. It could still be a scam.
- Do not believe website testimonials. Fake work-at-home sites are full of personal stories of people (often struggling single moms) making thousands of dollars a month because they took advantage of this amazing opportunity.

- Do not sign a contract or make a payment without doing your homework about the company making the offer.
- Before you say yes to any online jobs from home, whether it is remote or in a traditional office setting, researching the company is a must.



*This is an example of a work-at-home job scam:*

No Experience, High Income, No Company Name, Huge Range of Jobs

# Now Hiring Apply Today

**\$400 - \$1200 per Day**



## CURRENTLY HIRING FOR

Customer Support - Sales - Consulting - Management - Coaching -  
Data Entry - Writing - Insurance - Real Estate - Broadcasting -  
Blogging - Survey - Pastoral - Counseling - Life Coaching - Product  
Specialist - Sales Trainers - Financial Advisors - Loan Originators -  
Business Development - Team Management -

- Work From Home
- Flexible Schedule
- Sales & Non Sales opportunities
- Hourly & Salary opportunities
- Management & Training Positions Available
- No Experience Needed to Start
- Training Provided



# LOTTERY AND PRIZE SCAMS

**Unexpected prize and lottery scams work by asking you to pay some sort of fee to claim your prize or winnings from a competition or lottery you never entered.**

You will receive notification that you have won a lot of money or a fantastic prize in a competition or lottery that you did not enter. The contact may come by mail, telephone, email, text message or social media. To claim your prize, you will be asked to pay a fee. Scammers will often say these fees are for insurance costs, government taxes, bank fees or courier charges. The scammers make money by continually collecting these fees from you and stalling the payment of your winnings. The email, letter, or text message you receive will ask you to respond quickly or risk missing out. It may also urge you to keep your winnings private or confidential, to 'maintain security' or stop other people from getting your prize by mistake.



Scammers do this to prevent you from seeking further information or advice from independent sources.

Lottery scams may use the names of legitimate overseas lotteries, so that if you do some research, the scam will look real. You may also be asked to provide personal details to prove that you are the winner and to give your bank account details so the prize can be sent to you. Scammers use these details to try to misuse your identity and steal any money in your bank account. Sometimes, the scammers do send a cheque for part of your winnings, such as a few thousand dollars or euros of winnings, to trick you into thinking

the offer is legitimate. This cheque will eventually bounce, and you will receive no real payments. The scammer will take your payment and will fail to deliver the prize or will send you something that falls short of the promised prize.

### **What you should know:**

- If you have not entered a lottery, raffle, competition, etc., then you cannot win it!
- To win any lottery game, you must have bought a ticket for the correct draw date and you must match the winning numbers exactly on your ticket.
- No legitimate lottery randomly selects email addresses or mobile phone numbers to win prizes.
- Legitimate lotteries will not approach you asking you to claim a prize. You may receive an email advising you of a win and instructing you to check your online account, but it is for you to approach the lottery company to claim any prize that you are due.
- Legitimate lotteries do not ask for upfront payment or fees to process your win.

### **How to identify the scam:**

- The message will claim to be from a legitimate company, but the email address will be a free webmail address like Hotmail.com or Gmail.com.
- It may not refer to you by name, but as “Dear Winner” or something similar but vague.
- They will give you a strict time limit to claim the prize and a confidentiality clause to pressure you into parting with your money or bank details. Also designed to act on your psychology.

### **Action you may take:**

- Ignore it.
- If you receive a call, check the number – if it is +4470, it is a Personal Redirect Number, used from anywhere in the world, or area codes such as 876 (Jamaica) or 809 (Dominican Republic). No legitimate lottery uses this sort of phone number. Do not answer the phone.
- Do not deposit supposed winnings that come in the form of a partial-payment cheque – this will bounce.



This is an example of a lottery scam:

#### Email Fraud Example



212 West 3rd Street, Suite 210 Pueblo, CO 81003  
Website: [www. www.coloradolottery.com](http://www.coloradolottery.com)

Attention: Email Account Holder

Are you the correct owner of this email? If yes, then, be glad this day as the result of the Colorado Online Lotto and email address free-ticket draws of the 2016 Promotion Award has been released and we are glad to announce to you that your email address came out in the first category and entitles you to claim the sum of **US\$800,000.00**.

It is a promotional Program to encourage the use of Linked in and Microsoft and Internet Programs. Your email address was entered for the online draw on this free ticket number: **B55607545 6152** with reference number **SAJA2C110P5** and Serial number **SA5365/3** , Batch number **XA87-2PY**, drew the lucky numbers: 04-09-20-22-29-38 - **Bonus 06**  
This subsequently won you the lottery in the 1st category i.e. matches 6 lucky numbers Plus Bonus number.

You have therefore been allocated to claim a total sum of **US\$800,000.00 (Eight Hundred Thousand, United States Dollars)** in cash is credited to file **SAPC/9080144308/05**. This is from a total cash prize of **US\$8,000,000.00** Shared amongst the 10 with (2) lucky winner in "1st" category.

This promotion was drawn based on email address as the key identification for setting up online accounts. All valid email addresses in the World Wide Web Draw used/participants for the online email promotion version were selected randomly via computer balloting from a global website collaboration with internet companies like eBay, pay pal, Perfect Money, and Google whom also built their systems and based their membership registration identity on email addresses supporting this computer draw system done by extracted email addresses from over 100,000 users, associations, and corporate bodies and affiliated members to the National Lottery website and their advertisers listed online. This online promotion takes place via virtual ticket balloting and it is done Bi-annually.

Please note that your lucky winning ticket file and number falls within our **Africa** booklet representative office in **South Africa** as indicated in your ballot played coupon. In view of this, your **US\$800,000.00** would be released to you by our payment department.

Kindly provide the following information urgently:-

1. Full Name: 2. Email Address: 3. Physical Address 4. Age/Occupation: 5. Reference Number/Ticket Number: 6. Telephone Number: 7. Country: 8. Batch number

Contact our Fiduciary agents immediately to commence release of your lottery prize by providing details below.

Contact Person: Mrs Juanita Lee  
Tel: +27 839 430 477  
E-mail: [admin@lotterypost.ec](mailto:admin@lotterypost.ec)

Sincerely,

  
Mrs. Mary Clark



APPROVED



Controller General Copyright (c) 1994-2015 the US Lottery International Promotion Inc. All rights reserved.  
Terms of Service -Guideline 77635 476378 255667466.

# EXTORTION SCAM

**People are more likely to respond to threatening scam messages than to those that promise rewards. That might explain the growth of email extortion scams that threaten to publicize compromising information about you — true or not — if you do not make a quick payment.**



Extortion scammers have a valuable scare tactic at their disposal: they show in their messages that they know a password you've used for online accounts. To make it even more intimidating, some scammers tinker with their email messages, filling in the "From" section with your actual email address to create the illusion that they have control of your account. They claim they have implanted malware on your computer that lets them capture your keystrokes, watch through your webcam or walk through your drive and amass evidence that you, say, frequent adult websites, and they say they will share that information with

all your email and social media contacts — perhaps with a video of you enjoying your viewing — unless you pay them, typically several hundred euros or other currency in the form of Bitcoin.

Should you worry? There is little chance that a scammer has really invaded your computer. Extortion scammers send out threats indiscriminately, using big batches of email addresses and associated passwords that they likely obtained on the black market following big corporate data breaches. They hope to stumble across a few people who do not change their passwords regularly or do have some secret they do not want known.



## *This is an example of an extortion scam:*

do know, \*\*\*\*, is your password.

I require your full attention for the upcoming 24 hrs, or I may make sure you that you live out of shame for the rest of your lifetime.

Hey, you don't know me. Yet I know just about everything about you. Your entire facebook contact list, mobile phone contacts along with all the digital activity on your computer from past 145 days.

Which includes, your masturbation video clips, which brings me to the primary motive why I am writing this specific email to you.

Well the previous time you went to the adult porn online sites, my malware was triggered in your computer which ended up logging a eye-catching footage of your self pleasure play by activating your webcam.  
(you got a unquestionably weird preference btw lmao)

I have got the entire recording. If, perhaps you feel I am fooling around, just reply proof and I will be forwarding the particular recording randomly to 10 people you recognize.

It might be your friend, co workers, boss, mother and father (I'm not sure! My software will randomly choose the contact details).

Would you be capable to look into anyone's eyes again after it? I doubt it...

However, it doesn't have to be that way.

I want to make you a 1 time, non negotiable offer.

Buy \$ 2000 in bitcoin and send them to the listed below address:

1AEZYiEBLps39i1k3qS3N\*kLyW63fdj3DGV  
[CASE-sensitive, copy & paste it, and remove \* from it]

(If you do not know how, google how to buy bitcoin. Do not waste my precious time)

If you send out this 'donation' (we will call it that?). After that, I will go away for good and never contact you again. I will eliminate everything I have in relation to you. You may very well proceed living your current regular day to day lifestyle with zero fear.

You have got 24 hours to do so. Your time will begin as soon you go through this mail. I have an one of a kind program code that will notify me once you see this e-mail therefore don't attempt to play smart.



### **This is what you should look for:**

- The email includes a password you use online or one you used in the past.
- The message seems generic and does not cite any specific websites the sender claims you visited.
- The threat may be poorly worded and includes grammatical errors.
- You are given a short deadline to respond, typically a day or two – a classic high-pressure scam tactic.

### **Action you should take:**

- Do not reply to the mail.
- Do not pay. If you do, probably the scammer will be coming back for more.

- Immediately change your password. If you are sufficiently technically savvy to strengthen your password security, do so or ask somebody you know and trust who is able to do this to help you out.
- Make sure that your anti-virus software is functioning. If you do not have one, get advice from a computer shop or credible computer magazines or their online version and buy one.
- Cover the lens of your computer webcam when you are not using it – to block a scammer if he hacked you.
- Clean your internet history frequently so that you do not leave traces of sites you visited.

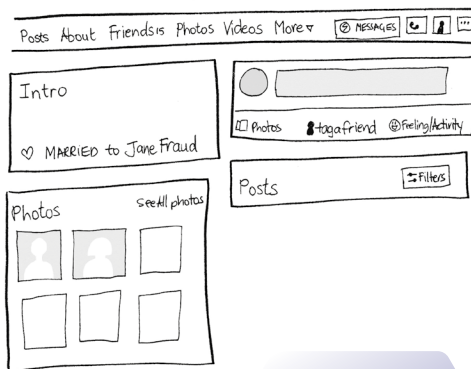
# FACEBOOK SCAM

**If you have a Facebook or other social media account, then you are also at risk of being scammed. Over the years, several scams have popped up on Facebook and other social networks.**

If you are not already familiar with them, some of the most common scams (which include others discussed in our Little Black Books, such as romance scams, lottery scams, work at home scams, etc.) are presented below so that you can protect yourself.

## Duplicating accounts:

One way in which scammers trick Facebook users is by imitating the email template from Facebook, which makes it look like you have an official message. Once you click through the email to Facebook and enter login information, the phishers can duplicate your account, hold it for ransom, or begin asking your friends for money or information.



### **Viral video:**

Viral videos are extremely popular on social media pages, especially if they are funny, shocking, or scandalous. However, since they are irresistible to many, they are also the perfect bait for scammers. When you click on one of these videos that are part of a scam, you may be asked to update your video player, and, when you do, it downloads and installs a virus onto your system. It also shares the same scam with your friends, who will believe the message they receive is safe since it looks like you shared it.

### **Links / Click Jacking:**

Fake news, free giveaways, etc. can be delivery methods for malware. Just like email scams, these leverage stories, news or offers that catch your attention. The point is to have you click on a link or share something that propagates malware. Examples include direct messages with links or attempts to get you to look at something; links resulting in another login request for Facebook/Email Provider – this is to harvest

your account; surveys – some surveys on Facebook are created to harvest information about users for identity theft/account hijacking/spear phishing (crafted attacks).

### **Burglary:**

Criminals also use Facebook to determine if a potential victim is at home or not. Publicly sharing information about vacations and other times when you are away from your home is exactly what burglars are looking for.

### **Free coupons:**

You have probably seen this many times. You are promised free coupons at large retailers worth more than usual, or coupons for a free vacation. All you need to do is use your Facebook login on a site, and you will get a free vacation – or your social media identity will belong to someone else without the vacation.

### **This is what you should look for:**

- People who you do not know in person asking you for money.

- People asking you to send them money or gift cards to receive a loan, prize or other winnings.
- People asking you to pay a fee in order to apply for a job.
- People representing large companies, organizations or public figures that are not verified.
- People asking you to move your conversation off Facebook to a less public or less secure setting, such as a separate email.
- People claiming to be a friend or relative in an emergency.

### Action you should take:

- Before you buy, on the basis of an ad or post, check out the company. Type its name in a search engine with words like "scam" or "complaint."
- Never send money to a love interest you have not met in person.
- If you get a message from a friend about a way to get some financial relief, call them. Did they forward it to you? If not, tell them their

account may have been hacked. If so, check it out before you act.

- Before paying into an "opportunity" to earn money, check out: [www.mfsa.mt/news/warnings/MFSA-Warnings/](http://www.mfsa.mt/news/warnings/MFSA-Warnings/).
- Do not make it easy for scammers to target you – check your social media privacy settings to limit what you share publicly.
- Consider what pictures you post on your Facebook account. You may be presenting information that makes it worth a scammer or a criminal to place you in his/her sights.
- Be wary of what you click on.



This is an example of an extortion scam:

Facebook - Google Chrome

https://www.facebook.com/sharer/sharer.php?u=

Share on Facebook

On your own Timeline


Say something about this...

### BUSINESS CLASS

PASSENGER NAME  
**FIRST/LAST**

87YHGX30FYHWT5.KJ20LF9TE4

FROM YOUR LOCATION	CLASS 1	FLIGHT EK0415	DATE OCT 2015	DEPARTS 1945
TO ANY LOCATION				
ZONE <b>A</b>	SEQ <b>004</b>	GATE <b>12</b>	BOARDING TIME <b>19.00</b>	SEAT <b>5B</b>



BOARDING STARTS 45 MINUTES BEFORE YOUR FLIGHT. GATES CLOSE 30 MINUTES BEFORE DEPARTURE. IF YOU REPORT LATE, WE WILL NOT BE ABLE TO ACCEPT YOU FOR TRAVEL.

PASSENGER NAME  
**FIRST/LAST**

FREE ANY TO ANY

FLIGHT EK0415	DATE OCT 2015	DEPARTS 1945
SEAT <b>004</b>	BOARDING <b>19.00</b>	SEAT <b>5B</b>

04/00  
EK 1923E7K30N73AS00P00

Giveaway - 388 Free First Class Tickets. (Limited Time Remaining)

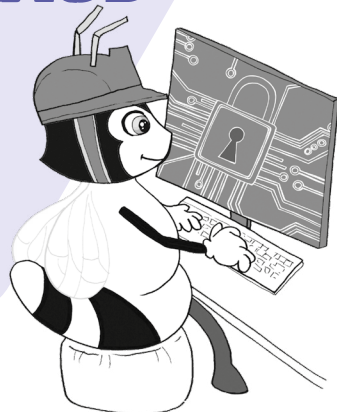
Claim your free First Class Tickets Around The World

DISCLAIMER: 100% REAL

# 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/](http://www.mfsa.mt/consumers/scams-warnings/)



**On this page, you will find the following sections:**

## **Scam Detection Guidelines**

A list 'Scams Detection Guidelines' is issued by the Malta Financial Services Authority.  
[www.mfsa.mt/consumers/scams-warnings/typical-scams/](http://www.mfsa.mt/consumers/scams-warnings/typical-scams/)

## **MFSA Warnings**

On this page, the MFSA warns the 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/](http://www.mfsa.mt/news/warnings/MFSA-Warnings/)

## Foreign Warnings

On this page you will find a list of warnings issued by European counterparts to 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](http://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 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/](http://www.mfsa.mt/news-item/mfsa-notice-ahb-consulting/)

## Entities licensed by the MFSA

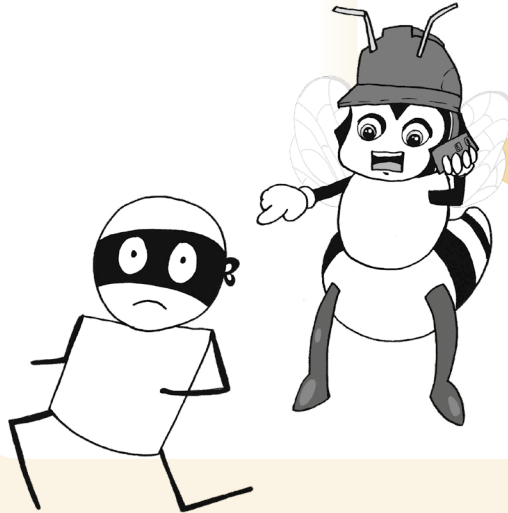
You are advised to always check whether a financial services firm is licensed by the MFSA. You can access this list by clicking on the following URL:

[www.mfsa.mt/financial-services-register/](http://www.mfsa.mt/financial-services-register/)





**GEMMA**  
know, plan, act.



## WHAT TO DO IF YOU GET SCAMMED

If you believe that you have uncovered a scam or you were the target or a victim of one, GEMMA 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](http://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](mailto: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/](http://eccnetmalta.gov.mt/)

You can contact the Centre as follows:

Online: [ecc.malta@mccaa.org.mt](mailto: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/](http://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 your 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 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](http://www.mccaa.org.mt/Section/Content?contentId=1193)

You can contact the centre as follows:

Online:	<a href="mailto:info@mccaa.org.mt">info@mccaa.org.mt</a>
Online form:	<a href="http://mccaa.org.mt/home/complaint">mccaa.org.mt/home/complaint</a>
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/](https://cybersecurity.gov.mt/)

**European Consumer Centre Malta:**

[eccnetmalta.gov.mt/consumer-information/e-commerce/how-to-shop-online-safely/](https://eccnetmalta.gov.mt/consumer-information/e-commerce/how-to-shop-online-safely/)

**Malta Financial Services Authority:**

[www.mfsa.mt/consumers/scams-warnings/typical-scams/](https://www.mfsa.mt/consumers/scams-warnings/typical-scams/)

**Depositor and investor compensation schemes:**

[www.compensationschemes.org.mt/](https://www.compensationschemes.org.mt/)

## GEMMA RESOURCES ON SCAMS AND FRAUD

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

**Aghżel minn fejn tixtri bil-karta ta' kreditu**

[www.youtube.com/watch?v=9K8ZhFfalJY](https://www.youtube.com/watch?v=9K8ZhFfalJY)

**Mhux kulma jleqq hu deheb**

[www.youtube.com/watch?v=mSGdWioPnyI](https://www.youtube.com/watch?v=mSGdWioPnyI)

**Uża l-ATM b'mod sigur**

[www.youtube.com/watch?v=zzxzT5iszts](https://www.youtube.com/watch?v=zzxzT5iszts)

**Fares il-karta ta' kreditu tiegħek**

[www.youtube.com/watch?v=qJhFg8HbIKM](https://www.youtube.com/watch?v=qJhFg8HbIKM)

