

LITTLE BLACK BOOK OF SCAMS & FRAUDS

PART 4



GEMMA
know, plan, act.

CONTENTS

Introduction	3
How A Scam Works	5
The 10 Commandments to protect yourself against scams and fraud.....	8
Free Streaming Site Scams.....	11
Small Business Fraud.....	14
Online Shopping Scam.....	17
Online Selling Scam	20
Anti-virus Scam.....	22
Money Mules.....	25
COVID-19 Vaccine Scam	28
How to protect yourself from scams and fraud	31
What to do if you get scammed.....	33
More information on scams and fraud	36
GEMMA Resources on scams and fraud	36



GEMMA and the eSkills Malta Foundation have a strategic partnership directed to engender knowledge on financial capability and fraud. The Little Black Book series is one of GEMMA and the Foundation joint initiatives on this matter.

INTRODUCTION

This is the fourth e-book in the series “The Little Black Books of Scams and Fraud” and the second since GEMMA has partnered with the e-Skills Malta Foundation.



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

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

In this e-book we have included the majority of the current frauds currently in play:

- Free Streaming Site Scam
- Small Business Fraud
- Online Shopping Scam
- Online Selling Scam
- Anti-virus Scam
- Money Mules
- COVID-19 Vaccine Scam.

Although scams and fraud are effected both in traditional manner – a service paid by a stolen cheque for example – as well as over the Internet, the fact is that the majority of fraud now not only occurs over the Internet but is also 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 to 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**



GEMMA
know, plan, act.

HOW A SCAM WORKS

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

(a) The Scammer's Approach

A scammer will approach you with a story designed to make you believe a lie. She or he targets your emotions and behaviour – offering you a chance to make money, to find a partner, to help somebody in need. Invariably, the scammer will dress him/herself

as a government official, a company – including branding names you are familiar with, an expert investor, a government official, a lottery officer, 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 you.

Online shopping, classifieds, and auction sites

These are used by scammers to trick you, with initial contact often made through reputable and trusted sites or fake websites that look like the real thing.

Over the Phone / Mobile

Phone calls

Calls are made by scammers to homes and businesses in a wide variety of scams: from threatening tax scams to offers of prizes or 'help' with computer viruses.

SMS

Scammers tend to send a whole range of scams including competition or prize scams.

Knocking at your Door

Door-to-Door

This usually involves the scammer promoting goods or services that are not delivered or are of a poor quality.

Charity / Church / Town Band Representative

The scammer seeks donations setting out a heart-rending story or for a social / religious project underway for which funds are being raised.

(b) Communicating and Grooming You

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

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

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



4**Ask yourself who you are really dealing with.**

Scammers pose as people or organisations that you know and trust.

5**Do not let scammers push your buttons.**

Scammers will play on your emotions to get what they want, including adopting a personal touch. Alternatively, they seek to rush you into making a quick decision before you look into it. Remember there are no guaranteed get-rich-quick schemes!

6**Keep your computer secure.**

Always update your firewall, anti-virus and anti-spyware software, and buy only from a verified source.

7**Only pay online using a secure payment service.**

Look for a URL starting with 'https' and a closed padlock symbol.

8**Do not hand over money and information to someone you do not know and trust.**

Any request for payment by an unusual method such as wire transfers, reloadable cards, or gift cards that are nearly impossible to reverse or track is a tell-tale sign that it is part of a scam. And if you do hand money ... it is rare to recover it.

9**Protect your identity.**

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

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

Tell your family and friends, and report it to: computer.crime@gov.mt

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

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



FREE STREAMING SITE SCAMS

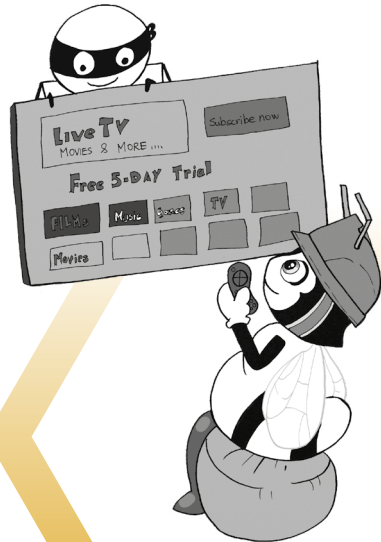
The rapid increase in subscribers of streaming services such as Netflix and Disney+ has rendered the streaming market an attractive target to scammers.

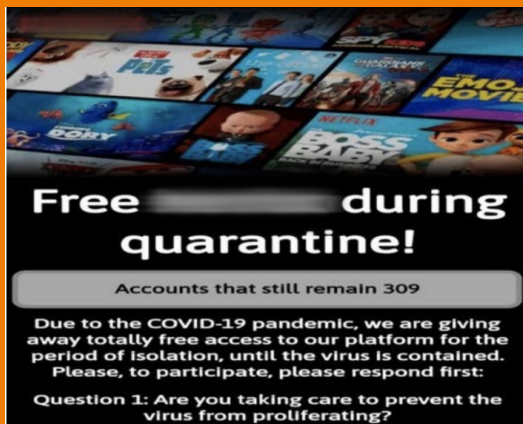
And so ... you are browsing through the Internet and you come across a streaming platform. It looks just like other major streaming platforms, even if the web address and logo look a little different from Netflix or Disney+. It says you can stream all the latest shows and films, and even offers a free five-day trial. What could go wrong? Right?

Wrong! You sign up, only to find no videos are loaded and you have a hefty bill in your email inbox! You have been scammed! Scam streaming platforms typically advertise a five-day free trial to watch movies and series. To register, you will be asked to provide an email address and telephone number, as well as your home address. Some scammers will ask for your credit details as well.

By using similar branding, visuals, pop-ups and messaging to legitimate

streaming sites, scammers can trick you. Whilst looking for a good deal you are lured to a fake streaming platform. During your visit to the site, you will not receive





This is an example of the home page of a streaming scam website

any indication that a payable subscription is needed. You subscribe, but once you subscribe, and you return to the main page, you will find that you cannot stream any movies ... yet you will promptly receive an email invoicing you for the cost of an annual subscription.

Other versions of this scam will request you to register (enabling them to harvest your data such as your name, address and other personal information, and to steal your credit card details for financial gain)

and then it will redirect you to a legitimate streaming site. By redirecting you to a legitimate site, you will have no idea that you have been scammed – until, of course, you receive their free subscription or account credit by email, or you are unable to login. Scammers can then sell your account credentials online or attempt to use them to log in to other accounts you may own, creating a ripple effect for future account takeover attacks.

Action that you may take includes:

- If you have been routed to a popular mainstream streaming service such as Netflix, Disney+, etc., before you take any action make sure that you are dealing with a legitimate site of the promoted provider. Research the site well.
- If the request for payment is done through a third party vendor site, rather than through the site itself, click out of the site.
- If you are approached through an email, for example the streaming provider asks you to update your payment or other information, check the email headers – the 'From', 'To' and 'Subject' lines. If the URLs are long and (probably) do not include the name of the service provider, this will be a scam.
- Illegal file-sharers and malicious scammers do not put a lot of effort into designing their sites. Compared to a legitimate business site, spoofed or fake websites contain easy-to-spot errors, such as grammatical and spelling mistakes. Graphics are missing, unprofessional, or totally out of context with the rest of the material. Fonts are inconsistent or unreadable.
- Another sign of an illegitimate website are the ads – not just an occasional embedded advertisement but intrusive and persistent pop-up ads, banners and even malware warnings will show up constantly. Since these sites do not make money using subscription services, they use online advertising to gain revenue.
- Beware of the never-ending link. Once you have found the content you want to watch, you then click the movie title or graphic. The site directs you to another page with another link. You click the movie title again. You are directed again, to yet another page filled with more links to the same movie title, but you never end up accessing the content. The purpose of this scheme is to try to trick users into sharing personal information or generate revenue by clicking ads.
- Legitimate streaming companies usually charge a small subscription fee for accessing their content. If a website claims to have all content free, beware. It could be a scam, or just a site illegally streaming pirated content, which is equally as bad.

SMALL BUSINESS FRAUD

Small businesses are more vulnerable to scams than larger enterprises. This is because small businesses are less likely to have the cyber security support or established accounting processes of larger companies.



There are various ways in which a small business can be scammed. The following are examples of some of the more common scams:

1. **Fake invoices:** Scammers createphony invoices that look like they
2. **IT Support:** For example, an alarming pop-up message pretending to be

are for products or services your business uses, maybe office or cleaning supplies or domain name registrations. Scammers hope the person who pays your bills will assume the invoices are for things the company ordered. Scammers know that when the invoice is for something critical, like keeping your website up and running, you could pay first and ask questions later. A variant of this is scammers posing as legitimate suppliers who advise changes to existing payment arrangements. The fraud may not be detected until it is too late – when the business is alerted by complaints from suppliers that payments were not received.

from a well-known company, telling you there is a problem with your computer security. Their goal is to get your money or access to your computer, or both. They may ask you to pay them to fix a problem you do not really have or to enrol your business in a non-existent or useless computer maintenance programme. They may even access sensitive data like passwords, customer records, or credit card information.

3. **Payment fraud:** The intention is to get you to transfer money to a bank account operated by the scammer. An example is the receipt of an email asking you to make a payment or to transfer funds for an ongoing or new business transaction. The payment request is marked as urgent, and pressure is applied to make the payment as soon as possible.
4. **Ransomware or Social Re-engineering:** Your employees are tricked into giving up confidential or sensitive information, such as passwords or bank information. It

often starts with a phishing email, social media contact, or a call that seems to come from a trusted source, such as a supervisor or other senior employee, but creates urgency or fear. Scammers tell employees to wire money or provide access to sensitive company information. Other emails may look like routine password update requests or other automated messages but are attempts to steal your information. Scammers can also use malware to lock organizations' files and hold them for ransom.

5. **Website Domain Name:** If you have your own website sites, you may receive an unsolicited letter warning you that your Internet domain name is due to expire and must be renewed, or offering you a new domain name like their current one. If you have registered a domain name, be sure to carefully check any domain name renewal notices or invoices that you receive. While the notice could be genuine, it could also be from another company trying to sign you up, or it could be from a scammer.

Action you may wish to take:

- Your best defence is an informed workforce. Explain to your staff how scams happen.
- Encourage people to talk with their co-workers if they spot a scam. Scammers often target multiple people in an organisation, so an alert from one employee about a scam can help prevent others from being deceived.
- Pay attention to how someone asks you to pay. Tell your staff to do the same. If you are asked to pay with a wire transfer, reloadable card, or gift card, you can bet it is a scam. Similarly, if the email directs you to change bank details on an account or a one-off payment, check whether you are dealing with a legitimate business.
- Make sure procedures for approving invoices or expenditures are clear. Review your procedures to make sure major spending cannot be triggered by an unexpected call, email, or invoice.
- If a caller claims that you ordered or authorised something, tell the person to desist in contacting you, or otherwise you will escalate the matter.
- Obtain a physical address, rather than simply a post office box, and a telephone number and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active. Be wary of those who utilize free e-mail services where a credit card was not required to open the account.
- Consider not purchasing from sellers who will not provide you with this type of information.

ONLINE SHOPPING SCAM

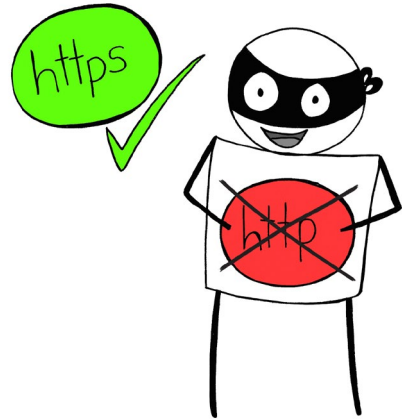
Fake websites are one of the largest types of online scams. But what do they do? Scammers set up fake retailer websites that look like genuine online retail stores. They may use sophisticated designs and layouts, possibly stolen logos, and a '.com' of a major country domain.

Many of these websites offer luxury items such as popular brands of clothing, jewellery and electronics at exceptionally low prices. Sometimes you will receive the items you paid for, but they will be fake, but most times you will receive nothing at all.

The biggest tip-off that a retail website is a scam is the method of payment. Scammers will often ask you to pay to a random PayPal address, wire it by Western Union, pay in gift card such as iTunes or by Bitcoin.

This is what you should look for:

- There should be a padlock symbol in the browser window where you



can see the site address / URL when you log in or register (beware these on unfamiliar sites as this can be faked). If you are not sure the webpage is genuine, do not use it. Be sure that the padlock is within the address bar at the top of the screen, not on the page itself.

- The web address should begin with 'https://' (the 's' stands for 'secure'). If it starts with 'http//'

then the site is not secure and must not be trusted with your personal information.

- Product is advertised at an unbelievably low price, or advertised as having amazing benefits, or features that sound too good to be true.
- They insist on immediate payment, or payment by electronic funds transfer, or a wire service.
- They may also insist that you pay up-front for vouchers before you can access a cheap deal or a give-away.
- The store may have limited information about delivery and other policies. A scam retailer is likely not to provide adequate information about privacy, terms and conditions of use, dispute resolution or contact details.
- Ads are a fact of life. No matter where you go, you are going to run into ads. But if you are on a website that is more ads than content, tread carefully. If you must click several links to get through intrusive pop-ups that redirect you to reach the

intended page, then you are on a website that is probably fake or at least scamming. There is a fine line between user experience and selling ads. When a website has no regard for that line, you need to be wary.

- You may be pressurised to transfer payment or a holding deposit before you have seen the item(s) in person.

Action to take:

- Check if the website or social media page has a refund or returns policy, and that their policies sound fair. The better online shopping and auction sites have detailed complaint or dispute handling processes in case something goes wrong.
- “Contact Us” section: How much information is there? Is an address supplied? Is there a phone number? Does that line connect to the company? The more information that is supplied, the more confident you should feel – provided it is actually good information. If all

The image shows a Facebook post from a page named "Gypsyde". The profile picture is a circular logo with a heart and the word "GYPSIDE". The navigation menu on the left includes Home, Posts, Photos, Community, Videos, About, and a "Create a Page" button. The main post features a photograph of a person wearing a grey hoodie with a red heart on the sleeve, blue jeans, and a brown bag. Below the photo is a "Shop Now" button. The post is from "Gypsyde" (Website) and has 24 comments and 11 shares. The visible comment from Cecilia Abecasis, Lin Baker and 78 others says: "I placed an order with you guys last Friday and have yet to get an email saying that my items have shipped." Below this, a reply from another user says: "They don't send an email letting you know that it was shipped, and you most likely won't receive what you ordered. They just take your money".

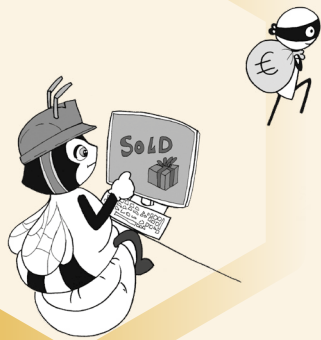
This is an example of an on-line shopping scam

they are giving you is an email address or, worse, there is no contact information whatsoever, abort. And remember to verify the information. Google the address, maybe even check out street view. See if any employee that is listed has a LinkedIn profile. Do a little homework.

- When making online payments, only pay for items using a secure payment service. Look for a URL starting with 'https' and a closed padlock symbol, or a payment provider such as PayPal.
- If payment is requested by virtual currencies such as Bitcoin, then abort.

- Avoid purchasing online with an e-shop that asks you to make the payment to a random PayPal address, or wire it by Western Union, or pay in iTunes gift cards.
- Think twice and check the site and the domain well before you respond to provide your financial details to proceed to centre parts of the on-line store.
- Check for a digital footprint. On the Internet nothing exists in a vacuum. Chances are other people have had experiences with this company and – good or bad – they have shared those experiences somewhere. With just a tiny bit of digging you can probably figure out if a website is fake, based on reviews alone. Google the name of the site along with "+ reviews". Also look for online reviews on sites such as Trustpilot, Feefo or Sitejabber which aggregate customer reviews before you take any action.
- Never accept a cheque or money order for payment that is more than what you agreed upon or to forward money on for anyone.

ONLINE SELLING SCAM



You are likely to do this increasingly these days. You have an item, furniture, a bike, some books, etc. that you have grown out of and you decide to sell. You go on online marketplaces – local or overseas – and advertise the sale. Be aware that in selling an item online you can be scammed. There are various ways this can be done.

One example: the buyer offers to purchase the item you are selling, but at the last minute makes up an excuse about why s/he needs to send you a cheque for more money than the cost of the item. You agree, deposit the cheque, send the excess funds, and ship the goods. The scammer will ask you to wire (or send via Western Union) the extra funds or mail a cheque, money order or prepaid debit/credit cards. A few days later your bank tells you the cheque bounced because it was fake. Your bank account is now overdrawn, and the item is gone. This scam works because you may be under the impression that a cheque is as good as cash. This is

false. With today's computer and printer capabilities, almost anyone can make a very realistic looking fake cheque.

This example underlines one important matter which is discussed in the section on "Money Mules" (see below). By sending you excess money, that is more than you asked for, and following that up with a request that you forward the excess money to a third party, the scammer is using you as a "mule". You are, in fact, laundering the money that the scammer stole to a third party, thus allowing the scammer to create layers to make it harder for him to be traced by police and other investigative authorities.

Alternatively, an interested buyer contacts you and says that s/he wants to buy the item right away and arranges to meet for the exchange. When he meets you, the buyer will tell you that s/he has already sent you the payment by PayPal and that you should check your mailbox as you should have received confirmation of payment from PayPal. You check your mailbox and you indeed have a mail from PayPal. The reality is, however, that the mail from PayPal, or, for that matter, any other popular secure payment gateway, is fake. Most people will only realize this when they check their account and find out that no money was deposited. By the time you discover this, the scammer will have long disappeared.

This is what you should look for:

- There is no legitimate reason for someone who is giving you money to ask you to wire money back.
- Being asked to ship the item outside of the address stated online in the e-selling online platform.
- A buyer from overseas – this goes against the normal, as data shows that most buyers tend to be local.
- A buyer from overseas who wishes to buy the item when this is easily available in his/her country of origin and likely to be cheaper considering the freight costs.

Action you should take:

- Do not accept cheques or money orders. When selling to someone you do not know, it is safer to accept cash or credit card payments.
- Do not accept overpayments. When selling online, do not accept payments for more than the sale price, no matter what convincing story the buyer tells you.
- Do not resend the money. Immediately inform your bank.
- Always confirm the buyer has paid before handing over the item. Do not take the buyer's word for it.
- Be wary of individuals claiming to be "overseas". In many different types of scams, con artists claim to be living abroad to avoid contact in person. Consider this a red flag.
- Meet potential buyers in person and in a safe place. Never invite buyers into your home. Suggest meeting in a public area. This might be enough to scare off a scammer.



ANTI-VIRUS SCAM

Has this ever happened to you? You are browsing online when a pop-up ad appears on your screen warning you that your computer is infected with dozens of viruses.

The ad says that you can remove them by buying antivirus software that will immediately eliminate them – and certain versions are designed to disable legitimate security software, making it challenging to remove the illegitimate software. If you have seen this, you have been hit with a scareware attack directed to get you to buy a fake anti-virus software.

What is a “fake antivirus”? It is a software that masquerades as a legitimate antivirus software that supposedly detects and eliminates viruses and other malware. Fake virus alerts are spread mostly on the Internet.

- The most common way people get scammed into installing fake antivirus software is through an alarming antivirus pop-up window appearing in their browser, claiming that their computer

has been infected by something bad and that they need to take immediate action and ‘click here’ – or words to that effect.

- A programme to remove the alleged malware is offered directly for sale or for download (and later purchased).

The tactic preys on people’s insecurity, especially those who are less tech-savvy. The scam is based on scaring you that your PC is riddled with viruses and malware. That is why the text of these pop-up ads usually contains dire warnings that your computer is infected with hundreds of viruses. To make their warnings seem even scarier, many of these scareware pop-ups will seemingly start scanning your computer for viruses, displaying a list of the dozens or hundreds of viruses they claim to be uncovering. However, scareware programmes are not really scanning your computer. The results they are showing

are fake. The scam is designed to target your behaviour – mainly by frightening you and make you lower your level of rational thinking – and to nudge you to buy the fake anti-virus.

This is what you should look for:

- Rogue anti-virus / spyware programmes often generate more “alerts” than the software made by reputable companies.
- You may be bombarded with pop-ups, even when you are not online.
- High-pressure sales copy will try to convince you to buy immediately.
- If you have been infected, your computer may dramatically slow down.
- Other signs of infection include new desktop icons, new wallpaper, or having your default homepage redirected to another site.
- Your antivirus software keeps detecting issues and displaying pop-up windows.
- The issues it finds can only be fixed by purchasing an upgraded subscription or additional software.
- Another likely sign that you are being scammed is when the name of the antivirus software being hawked onto you is one you do not recognise.

- Your computer is working at a low Internet speed and slow system performance as the software uses the Internet connectivity to install junk malware – with the result that the efficiency of the system also decreases gradually.
- You cannot shut down or uninstall your antivirus software.
- The easiest way to know if you have a rogue programme installed on your system is when you find that your homepage within the web browser is changed.

Action you should take:

- Keep your computer updated with the latest anti-virus and anti-spyware software, and be sure to use a good firewall.
- Never open an email attachment unless you are positive about the source.
- Do not click on any pop-up that advertises anti-virus or anti-spyware software.
- Remember that anti-virus scams mimic the design of well-known brands such as Grisoft AVG, Norton and McAfee. Do not buy it because of a pop-up ad on your browser. Go to the actual brand's



This is an example of an on-line shopping scam

site and buy it at your convenience – ideally looking first at what is out in the market.

- If a virus alert appears on your screen, do not touch it. Do not use your mouse to eliminate or scan for viruses, and do not use your mouse to close the window. Instead, hit control + alt + delete to view a list of programmes currently running. Delete the “rogue” from the list of running programmes and call your computer maker’s phone or online tech support service to learn if you can safely use your computer.
- Install a pop-up blocker and keep it turned on.
- Some scareware is difficult to close and is designed to trick you into accidentally

starting a download. It is best to close your browser rather than the individual pop-up ad. If the pop-up ad will not let you close the browser on your PC, try Ctrl-Alt-Delete to shut things down (if you are a Mac user, try Command-Option-Esc to open the Force Quit applications window). If you cannot close your browser, do a hard shutdown of your computer.

- Do not download freeware or shareware, such as a torrent site, unless you know it is from a reputable source. Unfortunately, freeware and shareware programmes often come bundled with spyware, adware or fake anti-virus programmes.
- Reset your current security settings to a higher level and clear your cache.

MONEY MULES

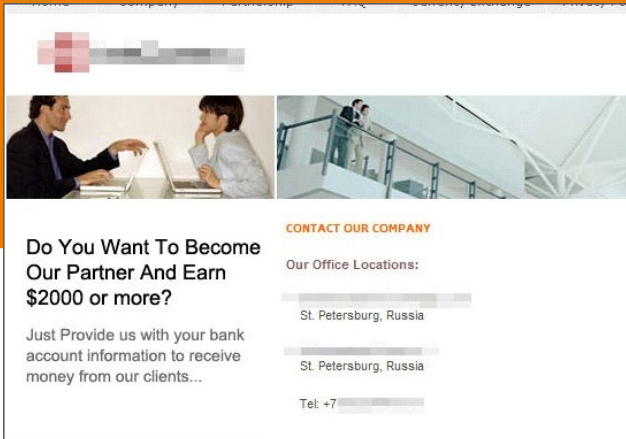
Once scammers get a victim's money, they are far from done. They often need to move the money – and they are not going to do it themselves.

That is where they employ the help of others – some knowingly, but many not: “money mules”. A “money mule” is someone who transfers illegally acquired money on behalf of a criminal – whether unknowingly or willingly. Mules are recruited by scammers, so they hold and move money on their behalf. Scammers do this so that they create layers between themselves and the scammed money to make it difficult for them to be traced. The most common money mule solicitations are disguised as “work-from-home” opportunities. The adverts offer the opportunity to make ‘easy money’, ‘free money’, ‘easy cash schemes’, or ‘no risk money’. These advertisements are often appealing to young persons who are interested in the convenience and flexibility of these types of jobs, or persons who are down on their luck and looking for a job. Because there are companies that



legitimately offer opportunities to work from home, users may not recognise malicious offers. Criminals often try to make the offer seem as legitimate as possible and may use the following approaches:

- Carefully crafting the wording so that an email does not appear to be spam and is not caught by spam filters.
- Linking to fake (but professionally designed) websites that appear to belong to recognised companies or that promote a company that does not even exist.
- Posting some of these jobs on legitimate websites, including websites specifically for job seekers.

A screenshot of a website designed to look like a legitimate business. At the top left, there is a logo consisting of a grid of colored squares. Below the logo are two images: one showing a man and a woman in business attire looking at a laptop, and another showing a modern office interior with a glass railing. The main text on the page reads: "Do You Want To Become Our Partner And Earn \$2000 or more?". Below this, it says "Just Provide us with your bank account information to receive money from our clients...". To the right, there is a section titled "CONTACT OUR COMPANY" with the heading "Our Office Locations:". Underneath, there are three entries, each with a redacted name and address: "St. Petersburg, Russia", "St. Petersburg, Russia", and "Tel: +7" followed by a redacted number.

Do You Want To Become Our Partner And Earn \$2000 or more?

Just Provide us with your bank account information to receive money from our clients...

CONTACT OUR COMPANY

Our Office Locations:

St. Petersburg, Russia

St. Petersburg, Russia

Tel: +7

This is an example of a mule scam

Typically, the process followed by scammers is as follows:

- The “company” collects information from the “employee.” The information may include personal data such as the individual’s Social Security number and bank account information. The company may also ask the employee to sign a seemingly official contract.
 - The company (or the employee under the direction of the company) creates a financial account that the employee can use to collect and transfer funds.
 - The employee receives funds or some type of merchandise.
- The employee is instructed to transfer the funds, usually keeping some percentage, to some other financial account or to deliver the merchandise to some third party. Often, the scammer asks the mule to move the money by one of these methods:
 - By wire/telegraphic transfer of the the money through, say, Western Union, into a third-party bank account.
 - By cashing out the money received, possibly via several cheques.
 - By converting the money into a virtual currency, like Bitcoin.

This is what you should look out for:

- Receiving an unsolicited email or contact over social media promising easy money for little to no effort or requesting you to respond accordingly to an advert promising as much.
- The “employer” you communicate with uses web-based email services such as Gmail, Yahoo Mail, Hotmail or Outlook.
- You are asked to open a bank account in your own name or in the name of a company you form to receive and transfer money.
- As an employee, you are asked to receive funds in your bank account and then “process funds” or “transfer funds” via a variety of means, such as wire/telegraphic transfer, mail, cryptocurrency or a money service business.
- You can keep a portion of the money you transfer.
- Your duties have no specific job description.
- Your online companion, whom you have never met in person, asks you to receive money and then forward these funds to an individual you do not know.

Action you should take:

- A legitimate company will not ask you to use your own bank account to transfer their money. Do not accept any job offers that ask you to do this.
- Be wary when an employer asks you to form a company to open a new bank account.
- Never give your financial details to someone you do not know and trust, especially if you met them online.
- Contact your bank immediately.
- Stop all communication with suspected criminals.
- Stop transferring any money or valuable items.
- Keep all receipts, contacts, and communications, such as texts, emails or chats.
- Notify the Malta Police Force immediately.

It is common for money mules to never see a pay cheque or a commission they thought they would be earning. Even worse, there is the chance of being arrested for being part of a crime, even though the mule did not know what was going on.

COVID-19 VACCINE SCAM

In 2020, with the start of the pandemic, Covid-19-related fake shops began circulating, promising cures and dubious pandemic survival tips.

As the vaccine gets rolled out and makes its way into the market in 2021, it is logical to assume that many people will seek a variety of different ways to get

hold of the vaccine first - and that scams would be launched via fake shops and ads on social media with regard to the sale of fake Covid-19 vaccine.

The screenshot shows a webpage for 'VIRAL SANITIZER'. The header includes navigation links: Home, SHOP NOW, Order by Phone, JOIN, and Customer Service. The main product image shows three bottles of hand sanitizer in different sizes. The text on the page reads: 'Viral Sanitizer – Kills 99.9% Germs, Bacteria, Virus - Pump Dispenser'. Below this, the price is listed as '\$44.99 \$12.99'. There are three size options: 8 FL. OZ., 16 FL. OZ., and 32 FL. OZ. A quantity selector is set to 1, and there is a red 'ADD TO CART' button. Below the product image is a video player with a play button and the text 'Viral Sanitizer - Protect yourself against...'. At the bottom, it says 'Viral Sanitizer - Hand Sanitizer - Kills 99.9% Germs - Made in USA by Survival.Technology'.

This is an example of a COVID-19 scam

This is what you should know to avoid a vaccine-related scam:

- You likely will not need to pay anything out of pocket to get the vaccine during this public health emergency.
- You cannot pay to put your name on a list to get the vaccine.
- You cannot pay to get early access to the vaccine.
- No legitimate entity will call you about the vaccine and ask for your ID number, your credit card number, or your bank account number to make sure you can get the coronavirus vaccine.
- Beware of providers offering other products, treatments, or medicines to prevent the virus. Check with your health care provider before paying for or receiving any COVID-19-related treatment.

Action you should take:

- If you get a call, text or email, or even someone knocking on your door, claiming they can get you early access to the vaccine – abort. This will be a scam.
- Do not click on e-mailed Coronavirus Vaccine links or open attachments.





HOW TO PROTECT YOURSELF FROM SCAMS & FRAUD

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

To visit this page, click on this URL:

www.mfsa.mt/consumers/scams-warnings/

On this page, you will find the following sections:

Scam Detection Guidelines

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

MFSA Warnings

On this page the MFSA warns the public with regard to unlicensed entities that claim to operate from Malta. Avoid investing in any of these companies. To visit this page, click on this URL:

www.mfsa.mt/news/warnings/MFSA-Warnings/

Foreign Warnings

On this page you will find a list of warnings issued by European counterparts of the MFSA. Before you decide to invest with a firm over the Internet make sure that you visit this page. To visit this page, click on this URL:

www.iosco.org/investor_protection/?subsection=investor_alerts_portal

Consumer Notices

On this page you will find a list of consumer notices issued by the MFSA. These notices, which are in Maltese and English, bring to the 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 MFSA has issued a consumer notice unless you have ascertained that the entity with whom the transaction is being made is authorised to provide such services by the MFSA or by another reputable financial services regulator. To visit this page, click on this URL:

www.mfsa.mt/news-item/mfsa-notice-ahb-consulting/

Entities licensed by the MFSA

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

www.mfsa.mt/financial-services-register/





GEMMA
know, plan, act.



WHAT TO DO IF YOU GET SCAMMED

If you believe that you have uncovered a scam or was the target or victim of one, 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.

You can contact the Unit as follows:

Online: computer.crime@gov.mt

Telephone: 356 2294 2231/2

In person: Call or visit any Police District station and lodge a report.
The District Police Officer will request the assistance of a member from the Cyber Crime Unit as required.

European Consumer Centre Malta

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

You can contact the Centre as follows:

Online: ecc.malta@mccaa.org.mt

Telephone: 356 2122 1901

In person: 'Consumer House', No 47A, South Street, Valletta

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

Your Bank

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

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

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

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

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

You can contact the centre as follows:

Online: info@mcaa.org.mt

Online form: mcaa.org.mt/home/complaint

Freephone: 356 8007 4400

In person: Malta: Mizzi House, National Road, Blata l-Bajda

Gozo: Elizabeth Street, Xewkija, Gozo

MORE INFORMATION ON SCAMS & FRAUD

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

Cyber Security Malta: cybersecurity.gov.mt/

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

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

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

ĠEMMA RESOURCES ON SCAMS AND FRAUD

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

Aghżel minn fejn tixtri bil-karta ta' kreditu
www.youtube.com/watch?v=9K8ZhFfalJY

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

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

Fares il-karta ta' kreditu tiegħek
www.youtube.com/watch?v=qJhFg8HbIKM



ĠEMMA
know, plan, act.