Royal Gibraltar POLICE

OPERATION

GIB WATCH

Working Together to put Crime between A Rock & a Hard Place

Your Practical Guide to basic Cyber Safety

Royal Gibraltar POLICE

Working Together to make Our Community Safer

OPERATION GIBWATCH

Working Together to put Crime between A Rock & a Hard Place

Contents: **Page:**

- Using the Internet safely 4
- Online Shopping 8
- Safe Email Use 13
- Creating Effective Passwords 17
- Online Banking 19
- Social Networks 21
- Some Popular Scams 23

Courier Fraud 23
Advanced Fee Fraud 23
Software Scams 24
Online Shopping Scams 26
Money Mules 27
Online Auctions 28
Lottery Scams 30
Holiday Fraud 32
Mass Market Fraud 33
Investment Fraud 34
Dating and Romance Scams 35
Mobile Phone Scams 36
Event Ticket Scams 38

Introduction

Businesses and the general public are increasingly being targeted by cyber criminals using a variety of methods.

Although this type of criminal activity has been around for several years, the methods employed by criminals evolve constantly, with scams becoming increasingly sophisticated as we ourselves become wiser as to what is and isn't legitimate.

Gibraltar is not immune from the threat of cyber-crime, and in recent months, there has been an increase in the number & type of cyber-based and traditional scams targeting our community generally.

We believe that prevention through education is key, and so we're delighted to bring you this informative guide which we hope will assist in preventing you from becoming a victim of crime.

This booklet looks at some of the main risks to our online activity, and describes most of the scams that have been targetting/continue to target our community. We hope this information will increase your awareness, improve your understanding of how some scams work, and provide you with some basic tools that you can use to protect yourself/others online.

Cyber crime costs the global economy billions of pounds annually, with fraudsters using a variety of methods to seek out potential victims. Scams/frauds can be difficult to investigate, as they are often complex, involving multiple victims & suspects worldwide

Keep the basics in mind when receiving phone calls from strangers asking for personal information such as passwords/PIN numbers, etc, text messages from persons/no's unknown to us or emails containing links or attachments from addresses/persons we are unfamiliar with.

Whether it's a phone call, letter, email or text message, ALWAYS take a moment to think carefully before answering any questions, provide any information, clicking any links within an email or responding to any letters. Scammers target people of all ages and backgrounds, therefore, it is important for all of us to think and act in a manner that will prevent us from being caught out.

Using the Internet Safely

The internet has revolutionised our lives, enabling us to read the news, enjoy entertainment, undertake our research, book our holidays, buy and sell, shop, network, learn, bank and carry out numerous other everyday tasks.

Despite the many benefits, there are a number of risks associated with "going" online. These can be as a result from visiting malicious websites or inadvertent disclosure of personal information.

The Risks

The risks of visiting malicious, criminal or inappropriate websites include:

- Viruses and spyware (collectively known as malware).
- Phishing, designed to obtain your personal and/or financial information and possibly steal your identity.
- Fraud, from fake shopping/banking/charity/dating/social networking/gaming/gambling and other websites.
- Copyright infringement – copying or downloading copyright protected software, videos, music, photos or documents.
- Exposure to unexpected & inappropriate content.

Websites

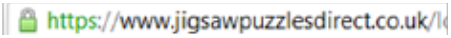
Cloning a real website is surprisingly not very complicated, and it doesn't take a skilled developer long to design a professionally-looking but malicious site. Be wary of malicious, criminal or inappropriate websites:

- Use your instincts and common sense.
- Check for the presence of a street address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity, or ask friends or family for advice.
- Check that the website's address appears to be genuine by looking for incorrectly spelt words, extra words, characters or numbers, or a completely different name from that which you would expect the business to have.
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser. Beware if this is different from what is displayed in the text of the link from either another website or an email.

- If there is **NO** padlock in the browser window or '**https://**' at the beginning of the web address to signify that it is using a secure link, **DO NOT** enter personal information on the site.

Examples:

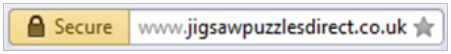
Google Chrome (address bar)



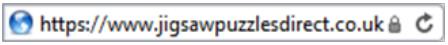
Mozilla Firefox (address bar)

Internet Explorer (far right of address bar)

Opera 9 (address bar)



Safari (far right of address bar)



A new type of secure server certificate, known as "extended validation" certificates will change the colour of the address bar to green when the certificate is valid.

- Websites which request more personal information than you would normally expect to give, such as user name, password or other security details **IN FULL**, are probably malicious.

- Avoid 'pharming' by checking the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed. This will avoid ending up at a fake site even though you entered the address for the authentic one – **for example 'eebay' instead of 'ebay**.

- Always get professional advice before making investment decisions. Sites that hype investments for fast or high return – whether in shares or alleged rarities like old wine, whisky or property – are often fraudulent.

- Be wary of websites that promote schemes that involve the recruitment of others, receiving money for other people or advance payments.

- If you are suspicious of a website, carry out a web search to see if you can find out whether or not it is fraudulent.

- Be wary of websites that are advertised in unsolicited emails from strangers.

Before entering private information such as passwords or credit card details on a website, you can ensure that the link is secure in two ways:

- There should be a padlock symbol in the browser window frame that appears when you attempt to log in or register. Be sure that the padlock is not on the page itself ... this will probably indicate a fraudulent site (See P5 above).

- The web address should begin with '**https://**'. The '**s**' stands for '**secure**' (See P5 above).

Measures such as these indicate that the website's owners have a digital certificate that has been issued by a trusted third party, such as VeriSign or Thawte, which indicates that the information transmitted online from that website has been encrypted and protected from being intercepted and stolen by third parties. When using websites that you're not familiar with, look for an Extended Validation (or EV-SSL) certificate that indicates that the issuing authority has conducted thorough checks into the website owner. The type of certificate held can be determined by clicking the padlock symbol in the browser frame which will launch a pop-up containing the details. Also note that the padlock symbol does not indicate the merchant's business ethics or IT security.

Cookies

Cookies are files placed on your computer, smart-phone or tablet by websites, and these are used to store information about your use during internet sessions. Most of the time they are innocuous – carrying out tasks such as keeping track of your username so that you don't have to log into a website every time you visit it, and storing your usage preferences. However, some are used

to track your browsing habits so that they can target advertising at you, or by criminals to build a profile of your interests and activities with a view to fraud.

- Set your browser to warn you when a cookie is installed. Note that some sites will not work if you block cookies completely.

- Some browsers will let you enable and disable cookies on a site by site basis so you can allow them on sites you trust.

Use an anti-spyware program that scans for so-called tracker cookies.

- There are also cookie management programs that can delete old cookies and help manage them. In addition, you can use settings in some browsers to delete unwanted cookies.

- Use a plain text email display instead of HTML email so that tracking files and cookies cannot be included in email files.

Safe Use of Browsers

The most common internet browsers enable you to manage your settings such as allowing and blocking selected websites, blocking pop ups and browsing in private. Respective browsers will tell you to do this in slightly different ways, so we recommend that you visit the security and privacy section of their websites, or the help area of the browsers themselves: Internet Explorer, Opera,

Chrome, Safari, Firefox.
Some browsers also have the ability to identify fraudulent websites by default. Ensure that you are running the latest version of your chosen browser that your operating system will support. Also, ensure you download & install the latest updates.

It is important to remember that turning on the private browsing setting or deleting your browsing history will only prevent other people using your computer from seeing which sites you have visited. Your internet service provider, search engine, law enforcement agencies and possibly (if browsing at work) your employer, will still be able to see which sites you have visited or keywords you have searched for.

Always remember to log out of a secure website when you have completed your transaction, and before you close the browser. Closing the browser does not necessarily log you out. Ensure you have effective

and updated antivirus/antispyware software and firewall running before you go online.

What to do if you Encounter Illegal Material

- If you come across content that you consider to be illegal, such as child abuse images or criminally obscene adult material, you should report this to the Internet Watch Foundation (IWF) www.iwf.org.uk and the Royal Gibraltar Police.

- If you come across content that you consider illegal such as racist or terrorist content, you should report this to the Police.

Online Shopping

We've all heard how great Internet Shopping can be; some say you can find goods at prices far cheaper than at traditional stores, as online platforms don't have to manage expensive overheads.

Online shoppers enjoy the convenience of shopping "whenever you want to", the "broad range of products available", "easy comparison of prices", "no queues" and "no need to search for parking". However, if you do choose "online" over traditional shopping, there are known risks associated with online shopping that everyone should be aware of. You need to take care with **WHAT** you're buying, **WHO** you're buying from, and **HOW** you pay for your purchases. Most online shopping sites use some form of shopping cart, your virtual shopping trolley into which you place items and take them to a "checkout" once you are ready to pay.

BUT...

Before you start shopping on the Internet, there are a number of questions you need to ask yourself:

1. Do you trust the retailer you're buying from?
2. What are their delivery times?
3. Can you contact them if the order goes wrong?
4. Are there any hidden charges?
5. Are you confident your payment will be kept secure?

Secure Online Payments

Secure encryption sessions between your computer and a merchant's website and keep your data safe

when interacting with online payment systems. Secure server certificates are created for a particular server, a specific domain and a verified business entity which allows web site visitors to safely transmit sensitive information and get a better idea of who they are entrusting it to.

Payment Methods

Using a credit card to pay for items online through electronic payment systems is a favoured method given the level of protection afforded.

For small purchases, electronic payment systems such as PayPal are one of the common alternatives.
These systems allow you to send or receive payments securely over the web without sharing your financial details or credit card number with anyone else.
To open an account, go to the PayPal website and choose 'sign up now' and then you can put money into the account using your debit card to use for future shopping.

The Risks

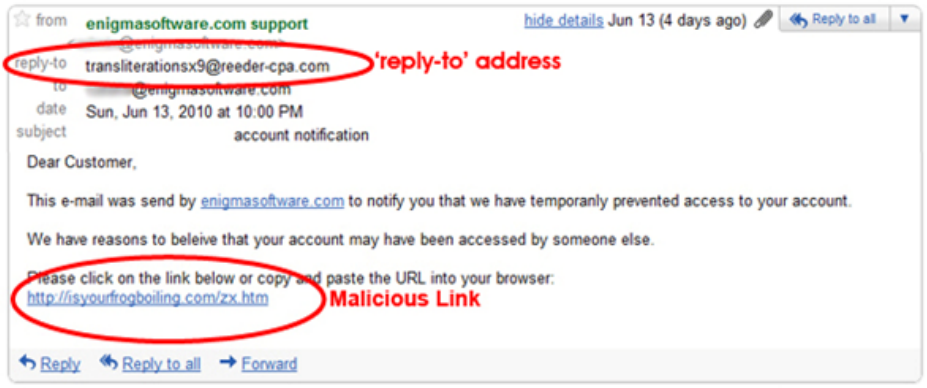
- Fraud resulting from making payments over unsecured web pages.
- Bogus online stores/shops – fake websites and email offers for goods and services that do not exist.
- Buying counterfeit goods intentionally or unintentionally, discovering they are of inferior quality and also possibly funding more serious crimes in the process.
- Receiving goods or services which do not match the advertiser's description.
- Being offered tailored prices based on information gathered by the retailer about your online shopping habits and websites visited.

Safe Shopping Tips

1. Trust your instincts – if an offer looks too good to be true it usually is. Legitimate popular technology and genuine designer items are rarely discounted. Ensure that any unfamiliar online retailer is reputable by conducting some research. Establish a physical address and telephone contact details. Remember that the best way to find a reputable retailer is via recommendation from a trusted source. Check a sellers' privacy and returns policy.

2. Keep security software and firewalls up-to-date. Regularly update your internet browser when a new patch-security update is released. If using the latest version of your browser, the address bar or the name of the site owner will turn green. Ensure you have effective and updated antivirus/ antispyware software and firewall running before you go online.

3. Do Not Reply To Unsolicited Emails, open/download any attachments OR access links within emails from companies/persons you do not know. Always type in the website address or use a search engine to find a site. If in doubt seek advice or try and call the person/company directly.



4. Avoid paying by money transfers direct to people you don't know. Use an online payment option such as PayPal, which offers protection by transferring money between independent electronic accounts.

5. Check the URL in the web browser. Don't be fooled by spoof websites where the address has been slightly changed.

6. If your bid for an online auction item is unsuccessful, don't be tempted to trade off-site if another seller approaches you with a similar item. This is likely to be a scam and you won't be covered.

7. Don't store your details on any website. Many businesses will ask you to save your payment details for future purchases. Although this makes purchasing easier, it means that your payment details have been stored in a database somewhere and are vulnerable to misuse by third parties.

Safe Shopping
(The Payment Stage)

Remember that paying by credit card offers greater protection than with other methods in terms of fraud, guarantees and non-delivery.

- Double check all details of your purchase before confirming payment.

- Watch out for pop-ups appearing asking you to confirm your card details before you are on the payment stage. Never enter your PIN number online.

Some websites will redirect you to a third-party payment service (such as WorldPay). Ensure that these sites are secure before you make your payment.

Before entering payment card details on a website, ensure that the link is secure, in two ways:

1. There should be a padlock symbol in the browser window frame, which appears when you attempt to log in or register. Be sure that the padlock is not on the page itself ... this will probably indicate a fraudulent site.

2. Remember that the web address should begin with **'https://'.**

Safeguard and remember the password (*See our separate note on advice for passwords*) you have chosen for the extra verification services used on some websites, such as Verified by Visa.

Once you have completed your shopping/made payment, always log out of sites into which you have logged in or registered details. Simply closing your browser is not enough to ensure privacy.

Keep receipts, and check credit card and bank statements carefully after shopping to ensure that the correct amount has been debited, as well as to ensure that no fraud has taken place as a result of the transaction. If you notice or suspect fraud, report this immediately to your card issuer/ bank and Police.

Scams change and adapt as trends come and go. They have also become more sophisticated as we get wiser to what is and isn't legitimate,

so it's understandable that people sometimes still get caught out. What the RGP urge consumers to do is to keep the basics in mind as a good preventative measure. It's easy to get carried away when you spot a bargain online for that gift you've been all over shops or shopping centres trying to find, but take a step back and think before you buy it.

Is it too good to be true?

Online shopping has revolutionised the way we buy our gifts during the year, particularly during the Christmas period, with more and more people choosing to search for gifts over the internet rather than heading to the shops. However, the result of this is that online fraud has been top of the festive scam list.

To reverse this trend we all need exercise caution with regards what we're buying online and from whom, especially if it is popular technology at a reduced price. By carrying out all the necessary checks you should guarantee that your gifts will be enjoyed by friends and family and not lost to fraudsters.

If you think you have been a victim of fraud, report it to your bank immediately, as well as to the Royal Gibraltar Police.

Safe Email Use

Email is an excellent communication tool and also a way in which companies can inform you about their latest products and services. However, email is frequently used to deliver unwanted material which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself, these include Spam (or Junk) Email.

The vast majority of email sent every day is unsolicited junk mail. Examples include:

- Advertising, for example online pharmacies, pornography, dating, gambling.
- Get rich quick and work from home schemes.
- Hoax virus warnings.
- Hoax charity/disaster relief appeals.
- Chain emails which encourage you to forward them to multiple contacts to bring 'good luck'.

How spammers obtain your email address

- Using automated software to generate addresses.
- Enticing people to enter their details on fraudulent websites.
- Hacking into legitimate websites to gather users' details.
- Buying email lists from other spammers.
- Inviting people to click through to fraudulent websites posing as spam email cancellation services.
- From names/addresses in the cc line, or in the body of emails which have been forwarded and the previous participants have not been deleted.

The very act of replying to a spam email confirms to spammers that your email address actually exists.

How to spot spam

Spam emails may feature some of the following warning signs:

- You don't know the sender.
- Contains misspellings (for example **'p0rn'** with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example "Buy now and get 50% off").
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.

- Contains attachments, which could include .exe files.

The Risks

- It can contain viruses and spyware.
- It can be a vehicle for online fraud, such as phishing.
- Unwanted email can contain offensive images.
- Manual filtering and deleting is very time-consuming.
- It takes up space in your inbox.

SCAMS – GENERAL EMAIL

Scams are generally delivered in the form of a spam email (but remember, not all spam emails contain scams). Scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

Email scams include:

- Offers of financial, physical or emotional benefits, which are in reality linked to a wide variety of frauds.

OR

- Emails purporting to be from 'trusted' sources such as your bank, Tax/Other Govt Authorities or anywhere else with whom

you may have an online account with. They may ask you to click on a link and disclose personal information/transfer monies, etc.

Phishing emails

Phishing involves the sending of emails to thousands of people, whilst

pretending to come from banks, credit card companies, online shops and auction sites, amongst other trusted organisations. They will usually try to trick you into downloading an attachment or clicking an embedded link in the email itself that will direct you to a website that looks exactly like the real thing, but is actually a fake designed to trick victims into entering personal information.

The email itself often looks as if it comes from a genuine source. Phishing emails often (but not always) display some of the following characteristics:

- The sender's email address is different from the trusted organisation's website address.
- The email is sent from a completely different address or a free webmail address.
- The email does not use your proper name, but uses a non-specific greeting such as "Dear customer."
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format. The image contains an embedded link to a bogus site in case a legitimate email gets through by mistake.

Use email safely

- Do not open/forward emails which you suspect as being spam.

- Do not open/download attachments from unknown sources.

- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.

- Do not respond to emails from unknown sources.

- Do not make purchases or charity donations in response to spam email.

- When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails.

- Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.

- If you are suspicious of an email, you can check if it is on a list of known spam and scam emails that some internet security vendors such as McAfee and Symantec feature on their websites.
- Most email clients come with spam filtering as standard. Ensure that yours is switched on.

- When choosing a webmail account such as gmail, Hotmail and Yahoo!

Mail, make sure you select one that includes spam filtering and that it remains switched on.

- Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.

- Most internet security packages include spam blocking. Ensure that yours is up to date and has this feature switched on.

Creating Effective Passwords

Passwords are the first line of defence against Cyber Criminals, therefore it's essential to pick strong passwords that are different for each of your important accounts (Banking, Email & Social Media). Follow these handy tips to create strong passwords and keep them secure.

1. Use a unique password for each of your important online accounts. Choosing the same password for all your online accounts (online banking, email, social media, website accounts) is like having one single key for your home, vehicles and workplace. If a criminal had access to that one key, everything would obivously be compromised, therefore, imagine what a hacker or scammer could do with one password that unlocked/accessed ALL your accounts! It may well be less convenient and practical, but **having multiple passwords keeps you safer.**

2. Keep your passwords in a secret place that isn't easily visible or accessible. Writing down your passwords isn't necessarily a bad idea, but if you do this, don't leave any notes containing passwords in plain view at home or at work, and **DON'T** carry them with you in your wallet/purse/bag. Ensure your passwords are stored in a safe/secure place (eg a small safe) and disguise what each one is for as an added security feature. If you're comfortable with software programs or applications, consider using a secure online password manager. (Eg: KeePass Password Safe, which is a free, open source, cross-platform and light-weight password management utility for Microsoft Windows. KeePass stores all usernames, passwords, other fields, including free-form notes, in a securely encrypted database, protected by a single master password and/or key file).

3. When given the opportunity, it's advisable to use 2-factor authentication (or 2-step verification). Services such as Google and Twitter allow you to provide a "Second one-time password". Using this additional feature when available means that even if someone discovered your username and password they would still be unable to access your account without the "2nd part".

4. Regularly changing your passwords is one of the best ways of ensuring that all your online accounts remain safe. Set a phone/calendar reminder at regular intervals (Recommended period is every 3-4 months) and try to stick to it. Remember that the amount of time that you will spend every now and then (a few minutes every 3-4 months) will be much less that than the time spent dealing with the inconvenience of someone accessing/stealing your personal information or even money from your bank account.

5. The longer your password is (preferably no less than 8 characters), the harder it will be to guess. Combining numbers, symbols and mixed case letters makes passwords harder for anyone to guess/crack. Please DON'T use "12345" or "password" and avoid using publicly available information such as your name/ surname, Date of Birth or even your address/phone number. This isn't very original and definitely NOT very safe!

6. Consider using phrases or themes that only you will remember, such as combining a place's / someone's initials with a combination of numbers/ symbols that mean something to **YOU ONLY**. For example, if one of your neighbours was named Mike Smith residing at No 48, you could consider something like +MiSmi48/. Relating your password to your favourite sport could mean **I Love To Play = (Iluv2Play4utb0ll)**

7. NEVER allow your browser or website, etc, to save your username and password for convenience. There are ways that these can be stolen.

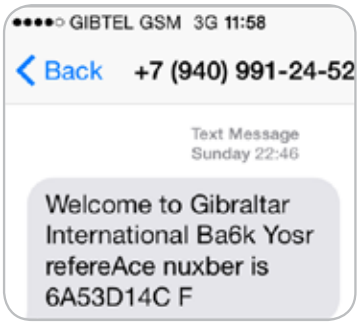
Online Banking

Banking online is very convenient, however, you must always ensure that your password and personal details remain far away from cyber criminals.

The Risks

- You could be tricked into disclosing your password/personal details through a "Phishing" email and/or fake website.

- Identity theft caused by viruses or spyware, granting criminals access to your bank account and other personal information stored on your computer.



- Malware on your computer that sends information to your bank that is different from that which you intended - for example the recipient of a payment. Malware could also introduce false fields such as 'enter your complete password' on an otherwise genuine site, by interfering with your browser. This is sometimes called a 'Man in the browser' attack.

Safe Banking

Never disclose passwords or other personal information in response to an email, phone call or letter purporting to be from your bank or other financial institution. **Banks will never send you emails asking you to divulge such information.**

Any official communication from banks will use your actual name (not 'Sir' or 'Madam') and possibly another verification of authenticity such as your postcode or part of your account number. If you are unsure if an email is genuine, ALWAYS contact your bank via other means.

- Always make sure you are using a secure internet connection to connect to your bank. Look for **'https'** at the beginning of the address and the padlock symbol in the browser frame.

Only ever visit your bank's website by entering the address into your browser or using a bookmark you have created using the correct address. If you believe your details may have been compromised in some way, always contact the bank

- Use strong passwords and PINs and a different password for each website.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you log in to your bank account.
- Do not reveal your passwords or PINs to anybody else or write them down to remember them.
- Always check your statements, and if you notice any unusual transactions, report them immediately.
- Switch off paper statements and register for online banking with mobile alerts. Paper statements can be intercepted and read.
- Get the latest updates for your computer's / device's operating system (ie Windows, etc).
- Avoid using public computers/ open WIFI networks to access your bank.
- Be aware of 'shoulder surfers' viewing your screen.

Two / Multi-FactorAuthentication

Many banks use two factor authentication to obtain stronger evidence of who you are than simply using passwords. Two factors are 'something you know' (typically your user name and password) and 'something you have' which is either your bank card with a card reader, or a standalone device such as a SecurID fob. The code generated is personal to you, and different each time you log in.

It is expected that more banks and other financial services providers will increase security levels in the light of mobile and app-based banking. Ths could mean up to five-factor authentication which could include using location-based services to prove that the mobile device is in the same place as the account holder, and sophisticated voice recognition.

Additional Security Software

Some banks offer additional security software specifically designed to

protect you during online banking. Such software usually involves a free download from banks' websites, and secures financial transactions in addition to normal internet security software. All banks carry online security information on their websites, including information about known frauds.

Social Networks

Social networking is a global revolution, enabling around a billion people worldwide to stay in touch with their friends, share experiences and photographs and exchange personal content. In many ways it has replaced the telephone and email. For many users, it has become a way of life.

Social networking sites are also valuable tools used by many businesses and individuals to extend their contacts and deliver marketing messages.

The nature of social networking – having such a massive base of users who are unknown to you – means that using it carries a degree of risk including becoming a target for cyber-criminals.

The Risks

- Disclosure of private information by either yourself or friends/ contacts.
- Bullying
- Cyber-stalking.
- Access to age-inappropriate content.
- Online grooming and child abuse.
- Prosecution or recrimination from posting offensive or inappropriate comments.
- Phishing emails allegedly from social networking sites, encouraging you to visit fraudulent or inappropriate websites.
- Friends' / other people's / companies' posts encouraging you to link to fraudulent or inappropriate websites.
- People hacking into or hijacking your account or page.
- Viruses or spyware contained within message attachments or photographs.

Safe Social Networking

You can avoid these risks and enjoy using social networking sites by following a few sensible guidelines:

- Do not let peer pressure or what other people are doing on these sites convince you to do something you are not comfortable with.

- Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace or school, your address or birthday. Remember, what goes online stays online.

- Consider picking a user name that does not include any personal information. For example, "joe_glasgow" or "jane_liverpool" would be bad choices.

- Set up a separate email account to register and receive mail from the site. That way, if you want to close down your account/page, you can simply stop using that mail account. Setting up a new email account is very simple and quick to do using such providers as Hotmail, Yahoo! Mail or gmail.

- Use **STRONG** passwords.

- Keep your profile closed and allow only your friends to view your profile.

- Do not say anything or publish pictures that might later cause you or someone else embarrassment.

- Never post comments that are abusive or may cause offence to either individuals or groups of society.

- Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.

- Remember that many companies routinely view current or prospective employees' social networking pages, so be careful about what you say, what pictures you post and your profile.

- Learn how to use sites properly. Use the privacy features to restrict strangers' access to your profile. Be guarded about who you let join your network.

- Be on your guard against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.

- If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account.

- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

SOME POPULAR SCAMS

1 - Courier Fraud

This type of scam is uncommon in Gibraltar, however, this kind of fraud is becoming prevalent & increasingly sophisticated worldwide. Elderly people are particularly vulnerable, with scammers claiming to be calling on behalf of a bank or police to try and obtain your card number/PIN. They'll say there's a problem with your card/account & will either ask you to tell them your PIN/key it into the phone. They'll then send "someone" to collect your card. They may try to reassure you by asking you to phone the bank, but will leave the line open so you unknowingly remain connected to them.

Some Useful Tips:

- Banks will **NEVER** call to collect your card. Neither will the police!

- Never hand your card to a 'courier' or any other stranger

- Never share your PIN with anyone or enter it into a telephone.

- Before calling back to verify a call from your bank/police/or others asking for your details, **MAKE SURE** your phone has a dial tone. Better still, use a different phone or call someone else you know and trust first.

If you HAVE been scammed, contact your bank immediately and then report the matter to the Police.

2 - Advance Fee Fraud

This type of scam usually involves the promise of a substantial amount of money or other opportunities.

This could be a lottery/prize draw, an inheritance claim, career prospects or money transfer schemes. You'll be asked to pay an upfront fee to collect your money. However, the fraudster will take this and you will see nothing in return.

Some Useful Tips:

- Scammers could phone, email, write letters or even visit in person. They will often look and sound very convincing.

- Don't respond to unsolicited promises of money in return for payment. Genuine lotteries, prize draws or inheritance payments never require you to pay a fee to make a claim.

- If you haven't entered a particular lottery or prize draw, **YOU CAN'T WIN IT!**

- Treat any such offers with suspicion and remember I**F IT SEEMS TOO GOOD TO BE TRUE, THEN IT PROBABLY IS!** Report any possible advance-fee fraud to your bank/Police.

3 - Software Scams

If you receive a phone call from a security 'expert' offering to fix your PC or operating system, **IT'S A SCAM**!

Here's how to avoid one of the more frequent software scams, commonly referred to as the '**Microsoft Windows Scam**', and what to do if you fear you

have fallen victim to it.

The '**Microsoft Windows Scam**' dates back to mid-2009, and peaked worldwide in September 2011. The scam continues, and Gibraltar households are targeted every couple of months. Scammers have been successful with this scam across the world, so it's important that we continue to raise awareness.

Microsoft Windows Scam: How it Works:

A scammer calls you, and asks for

you by name. They say they are a computer security expert from Microsoft (or other legitimate IT company). The 'security expert' is polite and sounds convincing. They say that your computer/ laptop has been infected with malware, and that they can help you solve the problem.

What happens now depends on the particular version of the scam that they are targeting you with. Some callers will ask you to grant them remote access to your computer or laptop, and then use the access to control your personal data.

Other callers get you to download malware that will give them the remote access they want.

Another type of scam is to simply ask for money in return for a lifetime of 'protection' from the malware they claim is already in your computer or laptop.

No legitimate IT security company or technician is EVER going to call you in this way. For starters, they CAN'T tell that your computer is infected.

They've obtained your name from the telephone directory, social media, or any of the many marketing lists where your details probably reside from previous shopping online, etc. They know ABSOLUTELY NOTHING about your home computer set up, so what they're doing is simply fishing for victims who actually TAKE THE BAIT AND PROVIDES ACCESS OR MONEY.

Microsoft Windows Scam: What to do if you ARE called:

1. Put the Phone Down and carry on with your day. It's not a legitimate call, so you have nothing to worry about other than the inconvenience.

2. During your conversation, don't provide any personal information. This is a good rule for any unsolicited call, & certainly never hand over your credit card or bank details. **JUST DON'T DO IT.**

3. If you've got this far, we can only reiterate Point 1: **GET OFF THE PHONE!** Whatever you do, DON'T allow a stranger to direct you to a certain web-page, OR instruct you to change a setting on your computer, OR instruct you to download software.

4. If possible, get the caller's details. You should certainly report any instance of this scam to the Royal Gibraltar Police.

5. Finally, change any passwords and usernames that could have been compromised, and run a scan with up to date security software. Ensure that your firewall and anti-virus are up to date.

6. **TELL EVERYONE ABOUT IT AND SPREAD THE MESSAGE.**

7. This scam targets people's insecurity about their lack of computer/internet knowledge. It's very easy to fall victim, therefore, the best defence is sharing knowledge. It's much easier to put the phone down if you are warned about this in advance.

Microsoft Windows Scam - What to do if you become a victim:

This could happen to ANYONE (and actually does in some cases). You need to change all personal data that you're able to change ASAP. As much as you might like to, you CAN'T actually change your date of birth, and changing your name and address seems quite extreme. However, you CAN change all your passwords and usernames, starting with your main email account and any bank and credit card logins. Also, contact your bank to ask them to be on the lookout for any suspicious activity. Again, use up to date security software to scan and "disinfect" your computer, and if the scammer did get you to do something to your computer, using "System Restore" to roll back the settings is always a good idea. Report it to Police. If you have lost money, it's possible your credit-card company or contents insurance will cover the loss.

Some Useful Tips:

1. Legitimate computer companies and banks will never call you and say that your computer needs repairs.

2. Never allow any unsolicited person to access or install software on your computer.

3. If someone calls you out of the blue, don't follow their instructions to go to a website, type anything into your computer or install software.

4 - Online Shopping Scams

Online shopping scams involve advertised goods or services that don't exist or aren't the sellers to sell. Often, the seller will request that payments are made directly to a bank account, rather than via secure

methods such as Paypal or credit card. The goods DON'T arrive and the buyer is unable to contact the seller after the money has been sent.

Common tactics

- Fraudsters use well-known auction sites such as eBay to sell fictitious vehicles, tickets, and electrical goods.

- Fraudsters use genuine vehicle trading websites to advertise and accept payments for goods that don't exist.

- Fraudsters advertise holiday lets online and people enter into agreements to pay the fraudster, without realising the fraudster isn't the owner of the property or the property doesn't even exist.

Some Useful Tips:

1. When buying online, always use the internet site's insured payment methods – avoid making payments direct to a seller's bank account

2. Do some research to make sure the site/seller is genuine – read independent review sites because they will be more inclined to be truthful. Consult friends/family.

3. Be cautious of sellers who don't have a track record for selling similar items. and NEVER buy from a bidder with a poor rating

4. Don't pay for high-value items (eg Cars) on online auction sites without first inspecting the goods.

5. **Remember - if a deal seems too good to be true, it probably is!!!!!!**

5 - Money Mules

This scam offers you the chance to earn some easy money for a few hours' work each week, but **BEWARE** – handling money that's been obtained fraudulently is a crime, even if you're not knowingly complicit in the original fraud.

'Money mules' or 'money-transfer agents' receive funds into their accounts and then move the money on, typically sending it overseas. The funds are money that fraudsters have stolen from other people's bank accounts. Money mules are often ordinary people recruited through a variety of methods, including spam emails, genuine job-search websites, email responses to an online CV, instant messaging and newspaper ads. Payment will be offered in return for moving the money, either in the form of a basic 'salary' or by keeping a percentage of the funds.

Help protect yourself from becoming involved by:

- Treating any unsolicited job offers with suspicion, especially if the company is based overseas.

- Verifying the details of any company that you're considering working for.

- Not giving your bank account details to anyone whom you don't know and trust.

Remember the golden rule: If it sounds too good to be true, it probably is!!!!!!

6 - Online Auctions

Online auction sites are a highly popular way of buying and selling both new and second hand goods. There are, however, risks associated with using auction sites – some of which are different from normal online shopping. Therefore you need to take care with what you are buying, who you're buying from, who you are selling to, how you pay for your purchases or how you yourself will get paid for items you are selling.

The Risks

- Bogus stores/shops – fake websites and email offers for goods and services that do not exist.

- Receiving goods which do not match the advertiser's description.

- Not receiving goods which you have paid for.

- Not receiving payment for goods which you have despatched.

- Being persuaded into selling early or at a low price. The best bids usually come towards the end of the auction period.

- Having your auction identity stolen and used fraudulently.

- Having your personal/financial information stolen and used fraudulently.

- Phishing emails, appearing to be from an auction or online payment sites but actually from criminals trying to lure you to a fake website to get your personal information such as login details for your online payment account.

Online Auctions Sites

If you are new to online auctions, take the time to read the online guides provided by the auction company so you understand how the system works and what the rules are.

Understand what the auction company can do (and won't do) if something goes wrong.

Use a login name for the auction site that is different from your email address.

Keep your contact information including email address, up to date.

Look into the seller or buyer – whether a private individual or online store. Look at their profile, their rating and transaction history. New sellers and buyers may not have a very comprehensive history, so be a little more cautious.

If the seller is a business, check their real-world existence. If they provide a phone number or address, give them a call. Sellers outside the UK may be harder to chase in the event of a problem.

Check online stores' privacy and returns policies. Be clear about shipping and delivery costs (for example, whether or not they are included and if not, if they are clearly stated).

Be clear about methods of payment and whether any of these incur a surcharge.

Provide only the minimum necessary personal information to sellers and buyers, such as your address for collection or despatch purposes.

Double check all details of your purchase before confirming payment. Check that notifications of communications between yourself and your buyer or seller are not being blocked by spam filters, by regularly checking your spam folder.

Do not fall for requests to close auctions early.

Always make sure you have received payment before despatching goods. When making a payment to an individual, never transfer the money directly into their bank account but use a secure payment site such as PayPal, where money is transferred between two electronic accounts.

7 - Lottery Scams

Lottery, sweepstake or prize draw fraud occurs when fraudsters contact a person(s) to advise them that they have won a large sum of money in an international lottery, sweepstake or other prize draw.

Persons are told via email or letter that they have won a large amount of money on an overseas or online lottery. Spanish/European lotteries are among the most common.

The letter or email will ask you to contact someone who claims to be an official of the lottery company in order to process the winnings. On occasions, you may be asked to keep your good luck a secret and, if you don't respond quickly, you may not be able to claim your winnings.

In most cases, either the lottery itself doesn't exist or the fraudsters are misusing the name of a genuine lottery. You can be sure there is no prize money for you to win when contacted in this way.

If you respond to the fraudster, you'll be asked to supply personal information and copies of official documents, such as your passport, as proof of identity. The fraudsters are then able to use such information to steal your identity and perhaps commit further crimes.

In some cases, once you have provided your personal information, fraudsters will ask you to pay various fees ranging from taxes, legal/banking fees etc so that they are able to release your "non-existent" winnings. Should you make any payment of this type, fraudsters will then provide an excuse as to why your winnings can't

be paid out unless you make another payment. Fraudsters may also ask for your bank details, claiming they will pay your winnings directly into your bank account. Should you hand over your bank details, the fraudsters will use them to empty your account.

- People who have already fallen victim to fraudsters are particularly vulnerable to the fraud recovery fraud. This is when fraudsters contact people who have already lost money through fraud and claim to be law enforcement officers (Police) or lawyers. They advise the victim that they can help them recover their lost money – but request a fee.

- **Protect yourself against lottery fraud**

- NEVER disclose your bank details or pay fees in advance.

- Never respond to any such communication. If you haven't entered a lottery then you couldn't have won it!

- Official lotteries worldwide operate in much the same way, therefore, lotteries will NEVER contact individual to advise them they have won.

- If someone has provided you with an email address to respond to, be very suspicious of addresses such as **@hotmail.com or @ yahoo.com**, or any numbers commencing with (**0044) 07 or (044) 0843**, as these are free to obtain.

- Official lottery operators **WILL NEVER** ask for fees to collect winnings, therefore, requests for fees are good indications of fraud.

- Official lotteries thrive on the publicity surrounding a win, therefore, if a letter/email asks you to keep your win a secret, it's likely to be a fraud.

- Most fraudulent lotteries involve bad spelling and grammar – see this as a warning that a letter/ email has been computer-generated and that fraudsters are at work.

Are you a Lottery Fraud victim?

- Have you received an official looking email or letter telling you that you've won a large sum of money in a lottery?

- Have you responded to the email/ letter and supplied personal information?

- Have you paid a fee to release your winnings?

What should you do if you're a victim of lottery fraud?

- Report the fraud to the Royal Gibraltar Police.
- If you have responded to the email/letter, break off all contact with the fraudsters at once.
- If you have provided fraudsters with your bank account details, alert your bank immediately.
- Be aware that you're now likely to be a target for other frauds. Fraudsters often share details about people they have successfully targeted or approached, using different identities to commit further frauds.

8 - Holiday Fraud

Holiday frauds are on the increase, with victims scammed out of millions of pounds a year by fraudsters. Scammers target online holiday booking and accommodation websites to scam unsuspecting customers into paying for accommodation that is not available or doesn't even exist. Victims sometimes only become aware of the scam when they arrive at their accommodation or destination and find that no booking was ever made.

Some Useful Tips:

Scammers often ask for payment by direct bank transfer instead of through the website, and may encourage you to do this by offering discounts for direct bank transfer payments.

Scammers use photos of accommodation taken from other websites.

The scammer's advert may state that they belong to a trade body or consumer protection scheme, and if so, contact the body or scheme to check their credentials.

Try and research the property to see if it has its own website. Always try and call the owner of a property

to confirm they are aware of your potential booking. If their phone number is not provided send an email requesting it. Ask friends/family for recommendations/advice.

Holiday Fraud - A True Story

Michael lost £2500.00 after attempting to book a holiday villa via the internet for 2 weeks. He had contacted a reputable website via email and was in the process of confirming his booking. However, he received a "Spoof" email claiming to be from an employee of the holiday company, telling Michael he would receive a discount if he paid for the villa directly to the owner's bank account, the details of which were included in the "spoof" email.

Michael became worried when he received no confirmation from the holiday website regarding his payment to the owner. He called them on a number provided on their website, however, he was told that there was no record of his booking and the company's database showed Michael had emailed them a few days earlier to say he was no longer interested in booking the villa.

After several weeks, Michael learned that his email account had been hacked weeks earlier through an **"Attachment he had downloaded"** from an email sent to him (Phishing), and that scammers then became aware of his interest in the holiday villa. The scammers had sent him an email where they "spoofed" the holiday website's address, and had deceived him into transferring monies into an account overseas, in order to receive a discount.

Michael was unable to reclaim the funds he had paid as he had made a bank to bank transfer to an overseas jurisdiction where an account had been fraudulently opened and later closed. The scammers were never identified.

9 - Mass Market Fraud

Victims worldwide are sometimes easily lured by the thrill of a surprise win, and find themselves parting with large amounts of money in order to claim fake prizes. Victims of these types of scams are usually the elderly and vulnerable. Some of these scams will be obvious whilst others will not. You should always be wary of anything you receive, especially from person(s) unknown to you.

Y**ou CANNOT win money or a lottery prize if you HAVEN'T entered it**, in the same way as **you cannot be "chosen at random" if you do not have an entry.** Many Mass Market scams will deceive you into sending money or providing your banking/ personal details in the belief that you will win a cash prize. You DO NOT have to pay a fee to claim a legitimate prize.

One single response to a scammer will be followed by further scam mail. Your name and address will be included on what's known as a '**Sucker's List'** and you may receive large amounts of scam mail on a daily basis.

A fake prize scam will tell you that you have won a prize or competition, and you may receive confirmation of this by post, email or text message. There are often costs involved in claiming the prize and even if you receive a prize, it may not be what was promised to you.

Items advertised in any mail you receive may be marketed as High Quality Exclusive Goods' but in reality can be extremely poor value for money. Another marketing technique is to offer a share of a cash prize but to win you must place an order for goods that in fact are not value for money.

Be wary when sending money to/ receiving money from someone you do not know and trust. A scammer may be trying to get you to pass stolen money through your bank account. Technically, you may be money laundering and become what is known as a 'Money Mule'. If convicted of money laundering you could be sent to prison, and having a criminal conviction could make it difficult for you to obtain financial products from a bank in the future.

10 - Investment Scams

The Investment market is extremely vulnerable to abuse by fraudsters. Many emerging markets remain unregulated making it very difficult for authorities to enforce good working practices. Common investment scams include buying rare metals, diamonds or other gemstones, wine, land, carbon credits and alternative energy. Many people have lost their entire life savings to investment scammers.

Don't let it be you!

Scammers will telephone you and try to sell you investments in emerging markets, which they claim will lead to financial gains above the rates of established investments like ISAs. In reality the item offered may not exist or is worthless.

Be wary of any investment company cold-calling you – they may be fraudsters!

Scammers will usually provide you details that you might think only a genuine investment company will have. They **MAY** have details of previous investments you have made, shares you hold and may even know your personal circumstances. **BE AWARE** that scammers will do their homework and make it their business to know as much about you as possible.

Scammers will often call you a number of times in an attempt to form a friendly relationship. If you respond in any way they will persist, try and build trust and may eventually persuade you to part with your money. Having obtained some money from you they will probably call again and try to persuade you to "invest" more money, perhaps in a different commodity.

Scammers may say they are from a reputable investment company, some will say they are stockbrokers or consultants. Always seek independent financial advice before you commit to any investment, and this could include checking with the Financial Services Commission to see if they are a registered company – do not rely solely on Companies House Data. Be wary of companies trying to recover money from lost investments on your behalf for a one off' fee – this could be a recovery room fraud trying to scam you again!
Similar to the initial investment, they are likely to know all about your previous investment history.

11 - Dating & Romance Scams

Although many dating websites and chat rooms operate legitimately in various countries, individuals using them may try to scam you. Dating and romance scammers lower your defences by building an online relationship with you. Both men and women have lost huge amounts of money to online dating scammers.

Always consider your personal safety if you arrange to meet someone through a dating website.

Be wary of providing personal information on a website or chat room.

Scammers will quickly interact with you, often showing you glamorous photos of themselves and gaining

your trust. However, **HOW** do you know they are actually the person you are communicating online with? **YOU DON'T !**

Scammers will make conversation more personal to draw information from you, but will never really tell you much about themselves that you can check or verify.

Scammers will normally try to steer you away from communicating on a legitimate dating website that could be monitored by staff. Their preference is to communicate via email, text and possibly telephone, rather than through the dating website or chat room where you met.

A scammer will use a variety of scenarios to target your emotions and get you to part with your money (e.g. they have an ill relative or they are stranded in a country they don't want to be in and need money).

Never send money abroad to a person you have never met or to anyone you don't actually know and trust. Scammers will sometimes tell you to keep your online relationship a secret. **NEVER AGREE TO THIS.**

Relationship Secrecy is a method used by criminals to stop family/friends from recognising such scams and warning potetial victims about them.

The scammer may ask you to accept money from them into your own bank account. They will come up with a convincing story as to why they can't use their own bank Account, such as loss of employment, emergency medical care, etc.

The circumstances may appear to be genuine; but, you may be committing a criminal offence of money laundering. Depending on who you bank with, the security questions asked by the bank may vary (e.g. the last 4 digits of your account number, or part of your password) **but your bank will NEVER ask you to authorise anything by entering your PIN into the telephone.**

12 - Mobile Phone Scams

Mobile phones have developed rapidly over the last few years and most now offer a huge range of functions. Smart-phones are mini-computers so take all the precautions you would with your own computer at home.

If you use an app to access your online banking, only use the official app provided by your bank. If in doubt, contact your bank & check.

Only download apps from official app stores, such as Apple iTunes, Android Marketplace, Google, Play Store and BlackBerry App World. Free apps are

great but downloading them from unofficial or unknown sources could lead to your device becoming infected with a virus.

Keep your smart-phone's operating system updated with the latest security patches and upgrades. These will normally be sent to you by your operating system provider.

DO NOT give your mobile banking security details, including your passcode, to anyone else and don't store these on your device. For added security you should set up a password or PIN to lock your mobile phone or tablet device.

Just like on your computer, there are anti-virus tools available for your mobile device. Consider using a reputable brand of software. Some banks offer customers free anti-virus software for their mobile phones, so check your bank's website for more information.

Be wary of clicking on links contained in a text message or email. Don't respond to unsolicited messages or voicemails on your phone. Your bank will never email you or send you a text message that asks you to disclose your PIN or full password.

Text scams offering money for an accident you may have had is often a ploy to obtain personal details. **Do not reply – not even to 'STOP' texts.**

You may receive a text message or advert encouraging you to enter a competition for a great prize. The scammers make money by charging extremely high rates for the messages sent from you them. These could be as high as £2 per text message. Do not reply.

With trivia scams, the first few questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions you need to answer in order to claim your 'prize' could be very difficult or even impossible. Do not enter.

If you try to claim your prize, you may have to call a premium rate number (that begins with 0906 for example).

You may then have to listen to a long recorded message and there's unlikely to be a prize at the end of it. **Do not phone back to claim.**

'**SMiShing**' occurs when a scammer sends you a text message asking you to provide personal and/or financial information. The message may appear to be from a legitimate company, like a mobile phone provider. Legitimate companies will not ask you to provide sensitive information by text. NEVER reply to these types of text messages. Unless you are using a secure web page, do not send or receive private information when using public Wi-Fi. Be aware of who is around you when using a mobile device to go online.

13 - Event Ticket Scams

Getting tickets to see your favourite band, football team, theatre production or festival can be very difficult, as tickets can often sell out quickly. Scammers take advantage of this by tempting you to buy tickets that do not exist or are fake. Scammers set up websites offering tickets that they do not have access to and cannot provide, but are happy to take payment for.

The scammer's website will offer tickets to events that are sold out or tickets that have not gone on sale yet. You may receive the tickets you have paid for but when you arrive at the event you find out they are fake or have been reported as lost or stolen and are therefore invalid.

Some Useful Tips:

Scammers may tell you a representative will meet you at the event with your tickets and they do not arrive.

Depending on the circumstances, paying for tickets using your credit card may offer protection if you are scammed.

Checking online may provide details of any negative reviews of the website you intend to use.

Remember the only way to avoid being scammed is to buy tickets from the promoter, the venue box office, a reputable ticket exchange site or an official agent.

If a website shows the STAR – Society of Ticket Agents and Retailers logo

STAR SECURE TICKETS from AUTHORISED RETAILERS

then check that they really are members by contacting STAR directly.

FINALLY...REMEMBER

If you think you have uncovered a scam, have been targeted by one and fallen victim, you should contact your bank and Police immediately. You should also spread the word to friends and family.

Reporting crime, including fraud, is important. If you don't tell the authorities, how will they know of its existence and be in a position to investigate further. Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target again.

The quicker you act, the more chance you'll have of reducing your losses. We'll will be able to warn the community about the circumstances surrounding the scam & provide advice to minimise the chances of the scam spreading further. At the same time, you yourself should warn your friends and family immediately.

Spreading the word and generating awareness is important, particularly because scammers quickly identify new methods through which to target potential victims.

Although this booklet cannot hope to provide all the answers, you can easily apply the principles and advice given on these pages on identifying the signs and protecting yourself from the scams covered to pretty much anything.

ALWAYS BE SUSPICIOUS & ALERT ONLINE - Double check & verify anyone asking you for money or personal information - If it's too good to be true, then it probably is !

Royal Gibraltar POLICE

Working Together to make Our Community Safer

www.police.gi

/royalgibraltarpolice

@rgpolice

cpru@royalgib.police.gi

Emergency Line: 199
General Enquiries: 20072500

OPERATION GIB WATCH

Working Together to put Crime between A Rock & a Hard Place

Produced by
Crime Prevention & Reduction Unit,
Force Intelligence