CONSUMER AFFAIRS

BERMUDA

Promoting Confident Consumers and Responsible Traders

# Consumer Goods and Services

# SCAMS and Consumer Risks Handbook

# TABLE OF CONTENTS

# 1. Scams and Consumer Risks

Whenever you are faced with a form of communication that appears suspicious (e.g. promotional contests you have won yet did not enroll in) it is important to consider the following:

- Whether it seems too good to be true (e.g. a holiday that's much cheaper than you'd expect);
- Whether the communication came from someone you don't know;
- Whether you are receiving communication from an authentic company (e.g. no postal address, official website, questionable contact details);
- Whether you have been asked to transfer money quickly;
- Whether you have been asked to pay in an unusual way (e.g. by iTunes vouchers or through a transfer service Western Union) in order to become eligible to receive an award or promotional prize; and
- Whether you have been asked to give away personal information (e.g. passwords, social security number, banking details)

It is important to note that paying more for something than it is worth (i.e. above fair market value) is not the same as being scammed. Usually a scam will involve theft or fraud where you will not receive the benefit of what is being sold. For further guidance on the types of scams commonly faced by consumers, and how to minimize the risks that may be faced, please see below.

# 2. Types of Scams

Every consumer is vulnerable to being exposed to scams; which is why it is important to be able to identify and avoid scams. You should be suspicious of anything that sounds too good to be true as it usually is.

Have you received an offer that seems too good to be true or received a threat to pay money for debts you do not owe? Or have you received suspicious notifications from an unknown source asking for your personal information?

Scammers know how to discretely get your personal information and are getting smarter as technology advances and commercial businesses continue to offer new products and services. It important that you must remain skeptical of any suspicious, unsolicited promotional activities and research any free offers, "giveaways" or special promotions.

To assist in your identification of SCAMs, please see below for a list of some of the more popular scams consumers are exposed to:

## 2.1 Unexpected Money, Rebate and Inheritance Scams

One of the more common scams currently faced by consumers, an unexpected money scam occurs when a scammer contacts a consumer out of the blue to inform them that if they make an **upfront lump sum payment** they would be entitled to a prize, money or an inheritance.

Under an unexpected money scam the victim will transfer the upfront lump sum payment and will never receive what was promised. Where if they chase up with the scammer they will be greeted with an excuse as to why they have not received their entitlement and that in order to receive their entitlement **additional payments are required**.

Unexpected money scams can also involve scammers informing their target that they need their target's help to secure a large fortune which they are trying to transfer out of their country. The scammer may state that the fortune is money and/or assets abandoned by a corrupt government or government official. If you agree to make an upfront lump sum payment to assist transferring the funds out of the country the scammer will provide you with a share of the fortune.

A rebate scam involves a scammer contacting a target informing them that they are owed money (i.e. a tax refund, reversal of bank fees, etc.). However, much like an unexpected money scam a rebate scam requires the target of the scam pay a small **administrative fee**.

An inheritance scam often occurs when a scammer poses as a lawyer, banker or foreign official and informs their target that they are entitled to a large inheritance from a long-lost relative. In order to create a sense of authenticity the scammer will use official-looking documents in order to generate trust in their target.

Once trust has been established the scammer will inform their target that in order to receive their inheritance they will need to pay an **administrative fee and/or inheritance taxes**. The scammer may also ask for personal details in order to complete legal documentation needed to complete the administration of the estate and transfer your inheritance. In this instance you may face losing your money **and** being subjected to identity fraud.

The above-mentioned scams are typically implemented by a scammer located overseas. If you fall for these scams you will never receive anything from the scammer and will lose any money sent. In order to minimize your risk of exposure to unexpected money, rebate or inheritance scams, Consumer Affairs advises that you:

- Remember to be careful of "get-rich-quick" schemes; if it sounds too good to be true it is because it probably is;
- Avoid any arrangement with a stranger that asks for an upfront payment (i.e. money order, wire transfer, international funds transfer, cryptocurrency transfer);
- If an e-mail from an unknown contact appears suspicious, delete the e-mail and do not download any attachments;
- Remember that Bermuda Government departments, banks and public utility providers will never contact you asking for an upfront payment in order to claim a rebate;
- Confirm the identity of the unknown contact and do not use the contact details provided to you;
- Conduct a search online using the exact wording of the offer as many scams can be identified this way.

## 2.2 Prize and Lottery Scams

Much like unexpected money, rebate and inheritance scams, a prize or lottery scam involves the scammer trying to get their target to provide money up front and/or their personal details in order to become eligible to receive a prize for a lottery, sweepstake or competition that they never entered into.

As part of a prize or lottery scam the scammer will state that you need to pay an administrative fee or tax before your "winnings" or prize can be released to you. The scammer may also inform their target that in order to receive their prize they will need to call and/or send a text message to a premium rate phone number (i.e. not a toll free number which will incur charges for being used).

Although Bermuda does not currently have a local lottery, overseas based scammers may use the name of a real overseas lottery to claim that you've won cash; even though you never entered into the lottery and/or are not eligible to receive the cash as participants must be legally registered citizens of the country the lottery is based.

As part of a lottery scam the scammer will normally ask for payment of an **administrative fee and/or state income taxes** to release the "winnings". The scammer may also ask their target to provide their personal details to prove you are the correct winner. In this instance the target faces the risk of losing money and being subjected to personal identity fraud. In order to minimize your risk of exposure to prize and lottery scams, Consumer Affairs advises that you:

- Remember that you cannot win a competition or lottery that you have not willingly entered into;
- Remember that competitions and lotteries do not require you to pay an administrative fee to collect winnings;
- Think twice before calling or text messaging an unknown phone number, as you may be subjected to usage fees.

## 2.3 Dating and Romance Scams

Dating and romance scammers create fake profiles on legitimate dating websites, mobile applications or social media platforms (i.e. Facebook, Instagram, etc.) using photos and identities stolen from other people.

Scammers will use these fake profiles to try and solicit people to enter into a fake relationship in an attempt to gain access to individual finances; either directly through obtaining personal details (i.e. access to bank account details) or indirectly through gifts (i.e. financial assistance with medical bills, travel costs, personal items, etc.)

Scammers will usually be based in foreign jurisdictions (i.e. overseas) and physically unavailable due to "personal circumstances". In an attempt to justify their inability to be physically available, scammers will say that their personal circumstances may include, but are not limited to:

- Military deployment overseas;
- Employment obligations requiring them to work abroad;
- An active caregiver that restricts their physical availability due to unusual work hours (i.e. expected to be available outside of typical work hours).

In order to create a sense of authenticity scammers may send small gifts to eliminate the appearance of the scam victim being exposed.

Consumer Affairs advises that you exercise extreme caution when entering into conversations with individuals found on dating websites or mobile applications. In order to minimize your risk of exposure to dating scams Consumer Affairs advises that you:

- Never send money or provide your personal details to someone you have met online;
- Watch out if an online admirer asks to communicate outside of the dating website or mobile application after only a few "contacts" or conversations;
- Conduct an image search of the admirer through an image search engine (i.e. Google or TinEye) to determine if their profile is valid;
- Remain cautious when sharing intimate photos or videos with an online admirer as scammers are known to blackmail their victims.

## 2.4 Threat and Penalty Scams

As opposed to your standard consumer scam offering a prize, money or a rebate, threat and penalty scams use threats to instill fear into their targets in an attempt to coerce them into providing their personal details and/or access to their finances.

A scammer of a threat and penalty scam will likely call and/or e-mail their target out of the blue threatening them with the risk of an arrest for an outstanding bill, speeding ticket or outstanding unpaid taxes (i.e. payroll tax, social insurance or land tax, etc.)

During the initial contact (i.e. phone call or e-mail), the scammer will attempt to pressure their target into paying immediately and that failure to do so will result in the police being sent to your house to pursue an arrest.

Scammers using threat and penalty scams typically target vulnerable consumers. Such vulnerable consumers may include, but are not limited to, elderly consumers or foreign workers whose first language is not English and are unfamiliar with the laws of Bermuda.

When dealing with vulnerable consumers, scammers will present themselves as officials for various tax departments (i.e. Department of Social Insurance, Land Tax Office, etc.) where they will threaten their targets with arrest if they do not pay an outstanding tax bill. When dealing with foreign workers, scammers will present themselves as Immigration Department officials and threaten their targets with deportation unless fees are paid to correct errors in their work visas.

Threat and penalty scammers also pretend to be employees of **trusted companies** (i.e. your bank, BELCO, OneComm, Digicel, etc.) where they will threaten to cancel your service or charge penalties if you do not pay an outstanding bill immediately.

In either circumstance a threat and penalty scammer attempts to instill fear in their target and coerce them to act to their own detriment without first thinking about whether the scammer's story is true.

If you receive a threat and penalty scam through your e-mail, the e-mail will likely include an attachment or link to a fake website where you will be asked to download "proof" of the outstanding bill or fine the scammer is threatening you to pay. Consumer Affairs advises that you **do not** download any attachments as this may expose your computer to being infected by a computer virus and/or malware.

In order to minimize your risk of exposure to threat and penalty scams, Consumer Affairs advises that you:

- Stop, think and consider whether the scammer's story is true;
- Do not feel pressured by a threatening call or e-mail;
- Remain mindful that a Bermuda Government department or trusted company will never ask you to pay by unusual methods (i.e. gift card, wire transfers or cryptocurrency); and
- Verify the identity of the person who contacted you by calling the relevant organization directly;
    - You should be able to find the relevant organization's contact details through the Bermuda Yellow Pages, a past bill or checking their official website;
    - DO NOT use the contact details provided in any suspicious e-mail you receive or are given during a phone call with a suspected scammer.

## 2.5 Online Shopping Scams

As consumers and businesses continue to increase their reliance on online shopping Consumer Affairs has observed an increase in online shopping scams.

Scammers utilizing online shopping scams will create very convincing **fake retail websites and social media pages** that look authentic. The one common feature that reveals the inauthenticity of the scammer's page is the method of payment.

Consumer Affairs advises that you exercise caution when visiting online retail stores where unusual methods of payment are required (i.e. wire transfers, crypto currency transfers). In order to minimize your risk of exposure to online shopping scams Consumer Affairs recommends that you:

- Find out exactly who you are dealing with. If you are using a Bermuda based retailer, it is advised that you contact the Registrar of Companies to verify whether the retailer is authorized to operate;
- Confirm whether the retailer is reputable, has a refund policy and a complaint handling policy;
- Avoid any arrangement that requires upfront payment (i.e. money order, wire transfer, international funds transfer, crypto currency transfer);
- Never send money or give credit card or online banking details to anyone you do not know or trust;
- Only pay for goods purchased online after you have confirmed that the website is secured and the payment method is secured (i.e. web address should start with "http" and have a closed padlock symbol).

## 2.6 Computer and Mobile Device Scams

As technology advances scammers become more and more intrusive into their targets lives. It has been observed that scammers will contact their targets (i.e. phone call and/or e-mail) and inform them that their data security has been compromised and assistance is required to resolve their issue.

The scammer will communicate that by granting remote access to your personal computer (i.e. laptop and/or desktop) and following their instructions they will help fix your data security issue. Instead of helping, the scammers will either steal their target's personal data and/or install malware into their computer.

For clarity "malware" is dangerous software that is commonly delivered by e-mail and can appear from legitimate sources and installed on your computer (or other devices). If malware is introduced on your computer or mobile device it may introduce:

- Viruses;
- Spyware;
- Ransomware
- Trojan horses; and
- Keystroke loggers.

Ransomware allows scammers to encrypt your device (i.e. lock and or restrict access) to prevent their target from using the device until a payment is made to unlock it. However, Consumer Affairs notes that payment to the scammer does not guarantee that yo ur device will be unlocked/unrestricted or free from hidden viruses.

Keystroke loggers and spyware allow scammers to record exactly what their targets type into their computer keyboard to find out their target's personal details, including: login details, passwords, banking details or personal information. When this happens the scammer may either use this personal information against their target or sell their target's personal information to someone else who may do further harm.

Once installed, keystroke loggers and spyware allow the scammer the ability to control the contents of your computer (i.e. e-mail and social media accounts, banking, etc.). The scammer may then access their target's contact list and attempt to replicate their scam with their target's friends and family.

To avoid having your computer or mobile device being exposed to malware, Consumer Affairs advises that you do not open e-mails from unknown sources as they may contain links or attachments that contain malware.

In order to minimize your risk of exposure to computer and mobile device scams Consumer Affairs advises that you:

- Exercise caution when encountering free downloadable content (i.e. music, games, movies, access to adult sites);
- Keep your office networks, computers and mobile devices secure (i.e. regularly update security software, change passwords and periodic data backups);
- Keep your data backups stored offsite and offline; and
- Do not open attachments or click links in suspicious e-mails or social media messages you have received from unknown sources.

## 2.7 Identity Theft and Phishing Scams

Identity theft and phishing scams occurs when scammers attempt to obtain the personal information of their targets in order to commit fraudulent activities such as:

- Making unauthorized purchases through credit cards or online banking;
- Opening fake bank accounts or public utility accounts (i.e. electricity or electronic communications);
- Taking out personal loans under the name of their target;
- Carrying out illegal business under the name of their target;
- Selling their target's personal information to other scammers for further illegal use.

The theft of identity and personal information can be both financially and emotionally impactful for the victims of identity theft and phishing scams. It can take months for the victims to reclaim their identity and years to fix any damages caused.

**Phishing** occurs when a scammer contacts their target out of the blue (i.e. e-mail, phone, social media, etc.) pretending to be from a legitimate business (e.g. bank, social utility provider, etc.). Often the scammer will direct their target to a fake version of the legitimate business's website.

Alternatively, a scammer may call their target portraying themselves as their target's bank or a luxury good provider claiming that someone is trying to use their credit or debit card. The scammer will advise their target to contact their personal lender or banker to resolve the "issue". However, the scammer will not hang up the phone and keep their line open in order to obtain your personal banking details.

When you try to call your personal lender or bank the scammer will simulate a real call by pretending to be your bank and ask that you provide your bank account and security details. Once the scammer has obtained your personal details the scammer will then have the ability to use your personal information at your detriment.

Under no circumstances will your bank or financial service provider send you an e-mail asking you for any personal information, including but not limited to: (i) debit/credit card numbers; (ii) account numbers; (iii) personal access numbers; or (iv) Internet Banking log-on information.

Consumer Affairs advises that you remain mindful of when you receive communication from an unknown commercial entity as phishing scams are getting smarter and more complex in order to appear authentic. Phishing e-mails can look genuine by using a legitimate company's logo and formatting and a link which leads to a website that seems genuine but isn't.

Remain mindful that genuine e-mails from financial service providers and utility service provider don't include suspicious links. If you get one of these e-mails do not respond and do not click on any of the suspicious links. Close the e-mail message immediately. If you receive suspicious e-mails forward them to your financial service provider.

In addition to stealing personal and financial information and your money, phishers can infect computers with viruses and convince people to participate unsuspectingly in money laundering.

**Fake surveys** are another way in which scammers may obtain your personal information and steal your identity. Through fake surveys scammers will offer their targets prizes or rewards (i.e. gift cards to well-known retailers) in return for completing an online survey. The survey will likely include a range of questions specifically designed to have the scammers target disclose their personal information.

It is important to remember that the crux of any identity theft scam is that the scammer will ask their target for personal information. Consumer Affairs advises that as a consumer you remember to keep your personal details to yourself and keep them secure. Giving away your personal information can be just as bad as giving away money.

In order to minimize your risk of being exposed to the risks associated with identity theft scams, Consumer Affairs advises that you:

- Think twice about what you say and do online (i.e. social media, blogs, online forums);
- Stop and think twice before you complete surveys, or participate in online competitions, that have been sent to you out of the blue;
- Stop and think twice before you click on links or attachments included in e-mails from unknown and/or suspicious contacts;
- Stop and think twice before "befriending", "following", "liking" or "sharing" something online;
- Remain mindful of the necessity to exercise caution when faced with requests to provide your personal details
- Use the phone book or conduct an online search to confirm the validity of a suspicious e-mail received from what appears to be a legitimate business and do not use the contact details provided in the suspicious e-mail.

## 2.8 Job and Employment Scams

Job and employment scams involve scammers offering their targets the opportunity for them to be a part of a new business start-up and/or invest in a "business opportunity". Scammers will often offer their targets a job, a high salary and/or a large bonus following an initial upfront "capital investment" into the "company".

The scammer may state that the upfront "capital investment" is needed in order for the business to develop a business plan, to cover the costs for training, cover the cost of purchasing computer hardware and/or software, the payment of taxes or fees, etc. When the scammer's target pays the upfront "capital investment" the scammer will not provide the job or employment opportunity that was promised.

Some "job offers" may be a cover for the scammer to hide any money laundering and terrorist financing activities they are participating in. In this instance the scammer, in addition to requesting an upfront "capital investment", will request their target to:

- Act as an "account manager" for the "company";
- Receive payments into your personal bank account for a "commission"; and
- Transfer the money received from the scammer to a foreign company.

Job and employment scams are often conducted through fraudulent spam emails and/or advertisements in classified sections in newspapers and online job boards.

In addition to the risk of being involved in money laundering and/or terrorist financing, job and employment scammers expose their targets to identity fraud as they may ask their targets to provide personal details (i.e. a copy of a passport or driver's licence, proof of citizenship, social insurance number etc.). In order to minimize your risk of being exposed to the risks associated with job and employment scams, Consumer Affairs advises that you :

- Exercise caution when receiving offers or scheme proposals where you a guaranteed income if you provide a lump sum payment upfront;
- Never agree to receive and transfer money for someone else as money laundering is a criminal offence; and
- Do not provide your personal details (i.e. drivers licence, passport, social insurance number) when applying for a job as such details should only be provided after you have signed an employment contract and have started work.

## 2.9 Charity and Medical Scams

Scammers are heartless and are likely to identify their targets during desperate times of need. Recognizing the generous nature of people trying to help those that are facing difficult times, scammers will attempt to take advantage of people seeking to donate to a good cause.

**Charity scams** involve scammers collecting money from people making donations to charitable efforts. In order to develop a false sense of authenticity, scammers will portray themselves as employees or officials for a legitimate cause or charity. Alternatively, scammers may create a fake charity. Often scammers will use charity scams following the onset of a natural disaster or crisis.

Charity scams have the duel effect of stealing money from people seeking to donate towards a good cause and diverts much needed financial support away from legitimate charities. Consumer Affairs cannot overstate the importance of verifying the authenticity of a charity prior to making any donations (i.e. verify the registration of an unfamiliar charity with the Registrar of Companies).

Alternatively, scammers may also seek to take advantage of vulnerable consumers seeking medical help. **Miracle cure** scams are designed to take advantage of desperate consumers suffering from serious medical conditions by offering a range of medical products and services which are often sold as being "holistic" and "alternative" medical treatments which promise quick and effective results. Such medical products are often promoted using false testimonies from people who have been "cured".

**Weight loss scams** promise dramatic weight loss with little or no effort. These types of scams often involve the target being required to adopt an unusual or restrictive diet, practice "revolutionary" exercise, use "fat-burning" devices, weight loss pills, patches or creams. As part of a weight loss scams, scammers will often require their target to make a large lump sum payment up front or enter into a long-term contract to receive goods or services.

**Fake online pharmacies** offer consumers counterfeit drugs and medicine at very cheap or discounted prices and do not require a doctor's prescription. The drugs made available through fake online pharmacies often have limited or no active ingredients which can have adverse or lethal consequences for the user. In order to minimize your risk of being exposed to the risks associated with charity and medical scams, Consumer Affairs advises that you:

- Ask to see proof of registration if you are approached by a representative of a charity or relief aid fund;
- Consult your healthcare profession if you are considering a "miracle" or "instant fix" medicine, supplement or other treatments;
- Ask yourself if this is really a miracle cure and why hasn't your healthcare profession not told you about this before?

## 2.10 Social Networking Scams

Social networking scams are growing in popularity. People are using fake profiles or fake groups impersonating people and organizations for malicious purposes. Not only do these criminals cause financial losses for victims but they can also damage reputational damage.

Consumer Affairs advises that you review your social media privacy settings and stay away from people you do not know. Scammers are very smart and can provide you with a false sense of security. To avoid being subjected to a social network SCAM, Consumer Affairs advises that you always remain mindful of the following:

- Do not share your personal details and be very careful what information you share and post online and with whom you share it.
    - It is very possible that anyone who really wants to see this information will find a way to see it;
- Do not post your date of birth, address, information about your family, your daily routine, holiday plans, or any information about your children;
- Set your online social networking profiles to private and check it regularly to ensure it stays private.
    - Never give out your account details or passwords.
    - Update your computer security software on a regular basis and make sure that your security software is strong and up-to-date;
- Make sure that you have strong passwords and change them regularly
    - have a different password for each of your social networking sites so that if one password is stolen, not all of your accounts will be at risk;

- Beware of any hoax password reset e-mails and messages on social networks;
- Do not accept a "friend" request, a request to join a group or a "follow" request from a stranger.
- If you receive an unexpected request for money from what appears to be a friend or family member, contact your friend via another means to confirm that the request is genuine before responding or providing money.
    - Do not use any of the contact details in the message;
- Never click on suspicious links on social networking sites – even if they are from your friends.

## 2.11 Investment Scams

Consumer Affairs advises consumers to remain mindful of the fact that investment scams come in many forms. Investment scams are often, but are not limited to the folllwing types of investment platforms:

- Cryptocurrency purchase and mining schemes;
- Binary trade options;
- Business ventures;
- Managed funds; or
- Sale or purchase of shares or property.

In order to create a sense of authenticity behind their investment scam and fraudulent activities, scammers will produce professional looking brochures and websites in order to mislead their targets.

As part of their attempt to solicit business and exploit their targets, scammers will often contact their targets either through a “cold”, “out of the blue” phone call or e-mail with the promise of “high investment returns” or a “guaranteed return on investment”. These investment scammers often operate abroad and do not possess an operating license from the Bermuda Monetary Authority.

As technology continues to rapidly advance Consumer Affairs has observed the uptake of computer prediction software scams. These computer prediction software scams are sold to the targets of scammers on the basis that the software promises to accurately predict:

- Stock market movements;
- Foreign exchange market movements;
- Gambling results; or
- Lotteries.

Computer prediction software scams are simply a form of gambling disguised as an investment platform with guaranteed results. However, most computer prediction software scams do not work and leave the victims of such scams unable to get their money back a s the scammer often disappears once they have received their target’s funds.

To avoid being subjected to an investment scam, Consumer Affairs advises that you:

- Do not let anyone pressure you into making financial decisions, especially if the offer has come out of the blue.
- Do your own research on the investment company and confirm with the Bermuda Monetary Authority to confirm that they have a license to operate in or from within Bermuda.
- Ask yourself: if a complete stranger new a secret to making money, why would they share it with a complete stranger for free?

## 2.12 Multi-Level Marketing Schemes

On the surface a multi-level marketing scheme appears to be an attractive business opportunity to involve your network of friends and family, sell products and collectively make a lot of money. You have the support of a multi-level marketing company who supplies the product, with marketing support and sometimes training.

Multi-level marketing schemes will not call themselves a multi-level marketing scheme and some do not actually sell a product or service; they may just offer an investment opportunity. Most multi-level marketing businesses offer a plan that claims that you will receive commissions by selling their product as well as commissions on the sales of people you recruit.

The whole scheme depends on you recruiting people to distribute the product and of course the people you recruit must recruit and on and on it goes. Not all multi-level marketing schemes are fraudulent. A legit multi-level marketing business is designed to move product through a large distribution network.

If you are considering joining a multi-level marketing business, do your research. As with any business venture, it is advised that you investigate the business and its products first. Get as much information as you can, including copies of their sales literature, business plan and/or marketing plan. There is alot of information available on the Internet; use it to your advantage.

Where possible talk to other people who have experience with the multi-level marketing company and the products to determine whether the products are actually being sold and whether they are making good money.

If the investment scheme is designed so that your investment income is derived solely from signing up people (i.e. you receive a commission on your new recruits rather than selling the product) it is likely fraudulent and a pyramid scheme and you will be wasting your time; and more importantly throwing away your money.

Fraudulent multi-level marketing schemes and/or pyramid schemes are designed so that those at the top continue to make money off of a continuous influx of new investors. Most of these schemes are operated from overseas entities where if things go wrong there is very little recourse if you suffer financial damages.

However, if you are subjected to a multi-level marketing scheme operating from within Bermuda you will likely have a measure of recourse if you suffer financial damages. Under the Consumer Protection Act 1999 it is illegal to operate a multi-level marketing scheme.

## 2.13 Scams and Covid-19

With the onset of Covid-19 Consumer Affairs has identified a number of new consumer scams which are targeting vulnerable individuals that have been financially impacted (e.g. employment redundancies or termination due to business closure).

Consumer Affairs advises that you look out for scams which may include:

- advertising face masks or medical equipment and supplies at high prices
- e-mails or text messages pretending to be from the Government of Bermuda or credit unions offering financial relief
- emails offering life insurance against Covid-19
- people knocking at your door asking for money for charities

# 3. How Scams Work

Having discussed some of the many different types of scams that consumers of goods and services may be exposed to (see above), the purpose of this section is to discuss the stages a scam will go through in order to be effective. By understanding the fundamental stages of an effective scam, as a consumer you will be able to better identify a scam and avoid being exposed to harm.

## 3.1 Approach – Method of Delivery

When a scammer approaches their target it will always come with a story specifically designed to make the target believe in what they are saying. In support of their story, the scammer will pretend to be something they are not (i.e. a government official, an investment advisor, a business representative, etc.). To deliver these lies a scammer will use a number of different forms of communication.

Online Communication

- Email: E-mail is a commonly used method of delivering a scam as it is a cheap method of communication which can reach a large number of people;
- Social Media: Social networking platforms, dating sites and online forums allow scammers to obtain personal details and create an artificial sense of trust with potential targets of a scam;
- Online shopping: Online shopping, classifieds and auction sites are used by scammers to target buyers and sellers. Initial communication with their targets is often made through authentic appearing, fake websites. If you suspect you are exposed to an online shopping scam, Consumer Affairs advises that you confirm the availability of secure payment options and beware of unusual payment methods (i.e. wire transfer, international wire payments, cryptocurrency transfer).

Over the Phone

- Phone Calls: Scammers will often call their target's mobile phone or home as part of their scam method of delivery. With the availability of cheap Voice Over Internet Protocol (VOIP) calling, this means that call centers can operate overseas while using telephone numbers that look like they are Bermuda numbers.
- Additionally, caller identification can easily be manipulated or disguised to make the scammer's phone call appear authentic.
- SMS Tet Messages / Chat Applications: Scammers will often send their targets text messages as part of competition or prize scams. If their target responds to the text message they will be subjected to premium rate charges and/or find themselves signed up to a subscription service that is difficult to exit. Text messages can also contain attachments or links to malicious software (i.e. photos, songs, games or apps). Consumer Affairs advises that you do not respond to or click on links in text messages unless you can confirm the source of the text message.

Home Communication

- Door-to-Door: In some instances scammers will visit your home in an attempt to promote the sale of goods or services that they have no intention of delivering or are of poor quality (i.e. misrepresentation).
- Bulk Mail: Scammers will often use bulk mail to send lottery and sweepstake scams, communicate "investment" opportunities and unexpected money scams and send fake inheritance letters to the homes of their targets.

Regardless of the method of communication that is used by a scammer, the story communicated is always the bait. If you are found nibbling on the bait the scammer will then seek to move you to the next stage of their scam.

## 3.2 Communication

If you take the bait on a scam and begin entertaining the scammer, the scammer will rely on a number of different tools and approaches to generate trust and convince you to disclose personal information and/or part with your money.

A scammer's tools are specifically designed to get their target to lower their defenses and build a sense of trust with their target. The different tools and approaches a scammer may use include, but are not limited to, the following:

- Scammers will spin elaborate, convincing stories;
- Scammers will use a target's publicly available details (i.e. social media information) to make them believe they have dealt with the scammer before to make the scam appear legitimate;
- Scammers may contact a target regularly (i.e. numerous follow-up calls) to build trust and convince their target that they are friends or romantically interested;
- Scammers will play with their targets emotions by using: (i) the excitement associated with winning a prize; (ii) the promise of love; (iii) sympathy for an unfortunate accident; (iv) guilt for not helping them; and (v) fear of an arrest or fine.
- Scammers will create a sense of urgency which will limit the amount of time their target has to think through things and force their target make a decision based on emotion rather than logic;
- Scammers will use high pressure sales tactics by stating that: (i) their offer is available for a limited time; (ii) prices will rise if they reject their offer and return to purchase their good or service; or (iii) the market will shift and the opportunity will be lost;
- Scammers will use professional looking publications (i.e. glossy brochures, consumer product handouts, etc.) with technical and/or legal jargon which will be backed up with office fronts, call centers and professional looking websites.

## 3.3 Sending the Money and/or Providing Personal Information

Once a scammer has developed a sense of trust with their target the scammer will then attempt to have their target make a payment and/or provide personal information. Sometimes the biggest clue that you are being subjected to a scam is the way in which the scammer asks you to pay. A scammer will often ask their target to make a payment and/or provide personal information within minutes of starting their scam or after months of careful grooming.

Scammers have been known to direct their targets to their bank, credit union or even their local post office to send money. Scammers will often stay on the phone with their target, give their target specific instructions and may even send their target a taxi if they have issues with transportation.

Scammers are often willing to accept payment in many different forms, including, but not limited to the following:

- Direct bank transfers;
- Debit cards / credit card payments;
- Gift cards; and
- Cryptocurrency.

Any request for payment by an unusual method is a clear sign that it is likely a scam. Consumer Affairs further advises that you remain mindful of the fact that scammers will also accept payments other than money; including valuable goods and expensive gifts (i.e. jewelry or electronics).

Paying money or providing personal details is not the only harm that you may be subjected to. If you help transfer money for a stranger you be involved in illegal money laundering and may be subjected to criminal liability. If you are asked to receive money from a stranger and transfer money to another stranger, Consumer Affairs advises that you contact the Bermuda Police Service immediately.

# 4. The Golden Rules for Protecting Yourself

Having identified the types of scams consumers are often subjected to, and the stages of a scam, the following section outlines the "golden rules" to protecting yourself from being involved in and harmed from a scam.

**Rule #1: Remain Alert**

Consumer Affairs advises that you remain alert of the fact that **scams do exist**. When dealing with uninvited communication (i.e. phone, e-mail, mail, in-person, social media), always consider the possibility that the reason why the communication is unusual is because you are the target of a scam. If it looks too good to be true then it probably is.

**Rule #2: Inform Yourself**

Consumer Affairs advises that you verify the validity and authenticity of any person or business that contacts you unexpectedly. If you have only ever met someone online, or are unsure of the legitimacy of a business, Consumer Affairs advises that you conduct some research (i.e. do a Google image search on photos, search the Internet for testimonials of other customers who have dealt with the person that has contacted you).

**Rule: #3: Exercise Caution**

If you receive an e-mail, phone call or publications from a suspicious source, Consumer Affairs advises that you exercise caution when opening the communication. Do not open suspicious texts, pop-up windows or emails and **delete the suspicious communication**.

If you are unsure whether an unexpected communication is suspicious, Consumer Affairs advises that you verify the identity of the contact and **do not** use the contact details provided in the message sent to you (i.e. conduct a Google search of the company and use the contact details on their official website).

It cannot be overstated how important it is to exercise caution when sharing your personal information on the internet and on social media platforms. Scammers can use your information and pictures to create a fake identity or target you with a scam.

**Rule #4: Secure Yourself**

Consumer Affairs advises that you keep your personal information secure at all times. As part of securing your personal information, it is suggested that you shred your monthly bills and other important documents before throwing them out in the trash. It is advised that you keep your passwords and banking details (i.e. pin number) in a safe, secure location.

As part of securing your personal information, keep your mobile devices and computers secure by using password protection. Furthermore, it is advised that you do not share your passwords with others, update your security software regularly and that you back up your digital content consistently.

With regards to your home Wi-Fi it is recommended that you utilize a password and avoid using public computers or Wi-Fi spots to access online banking or to provide personal information to a known source. Publicly available Wi-Fi is **not considered** secure and may expose you to having your personal information being stolen as scammers may hack public Wi-Fi spots.

Additionally, as part of securing your personal information it is recommended that you **choose your passwords carefully** (i.e. difficult for others to guess, a mix of upper and lower class letters, numbers and symbols), that you **update your passwords regularly** and that you **do not use the same password across numerous platforms.**

**Rule #5: Beware Unusual Payment Methods**

Scammers often ask their targets to make a payment (i.e. wire transfers, credit/debit card payment, cryptocurrency transfer). If you are asked to make an upfront payment for goods and/or services from an unknown source you are likely being targeted by a scammer.

**Rule #6: Beware Requests for Personal Details or Money**

Consumer Affairs recommends that you never send money to, or provide your credit card details, banking details or copies of personal documents to unknown sources. Additionally, never agree to receive money from an unknown source as part of a transfer to an unknown 3rd party. Money laundering is a criminal offence.

**Rule #7: Exercise Caution Shopping Online**

When shopping online beware of offers that seem too good to be true and always use an online shopping service that you know and trust.

Think twice before using cryptocurrencies to purchase goods or services online. Cryptocurrencies do not have the same protections as other transaction methods. If you transfer cryptocurrency to a scammer you are not likely to get your money back after you have sent it.

# 5. If You Think You Have Been Scammed

If you've given away money or personal information because of a scam, Consumer Affairs advises that you consider the following steps:

- Protect yourself from further risks
- Check if you can get your money back
- Report the scam to Consumer Affairs

If you've been scammed there are steps you can take to protect yourself from things getting worse. What you need to do depends on what has happened.

If the scammer visited your residential address, called you, or sent you a message, Consumer Affairs advises that you ignore them but keep a record of what has happened so you can report it.

## 5.1 Phone Calls

If the scammer **called you** there are steps you can take to stop getting nuisance calls that you don't want. You shouldn't receive nuisance calls if you didn't give the caller your number, for example:

- cold calls trying to sell you something you don't want or need, like double glazing
- recorded or automated messages telling you that you're due compensation, perhaps for a mis-sold insurance policy such as PPI

If you think a caller has used your contact details without your permission in an attempt to run a scam, you should report it to your phone service provider and the Information Commissioner's Office of Bermuda.

If you are unsatisfied with your phone service provider's response to your reported scam, Consumer Affairs advises that you file a complaint with your phone service provider. If you remain unsatisfied with your phone service provider's response to your complaint, it is advised that you submit a formal complaint with the Regulatory Authority of Bermuda.

There are products to block some calls (like international calls or withheld numbers) but be careful that they don't also block calls you want. Consumer Affairs advises that you contact your phone service provider and ask if they they have a service to block some numbers. Alternatively, you can install a call blocking device on your phone yourself.

## 5.2 Computer Hacked

Sometimes scammers ask to access your computer so they can control it remotely. For example, they might pretend to be from your internet service provider and say they need to deal with a technical problem.

The scammer might have infected your computer with a virus and/or stolen passwords and financial information. To stay safe you should:

- Reset your passwords
- Let your bank know your financial information might have been stolen
- Make sure you update your antivirus software

You could also get an IT professional to check your computer.

## 5.3 Funds Transferred or Personal Details Stolen

If you suspect that you have transferred money to a scammer, that your bank account reflects suspicious activity (i.e. 'unauthorized transaction') or you have mistakenly provided personal details to a suspected scammer (i.e. account details, PIN number, etc.) Consumer Affairs advises that you contact the Financial Crime Unit with the Bermuda Police Service and your personal bank immediately.

After you've told your bank about the scam keep an eye on your bank statements and look out for any unusual transactions. If you think your password has been stolen Consumer Affairs advises that you change your password as soon as possible. If you've used the same password on any other accounts you should change it there too.

You might be able to get your money back after you've been scammed. What you should do, and whether you will get a refund, depends on what happened. When contacting your bank Consumer Affairs advises that you clearly explain what has happened and ask if you can get the transaction reversed and receive a refund.

If you have used a debit or credit card or PayPal to pay for something, and you haven't received the goods or service you purchased, you might be able to get your money back. Upon filing a scam report your bank can ask the seller's bank to refund the money. This is known as a 'chargeback scheme'.

If you have to pay for something using a bank transfer or direct debit, and haven't received the goods or service you purchased, Consumer Affairs advises that you contact your bank immediately to let them know what has happened and ask if you can get a refund. Most banks should reimburse you if you've transferred money to someone because of a scam. This type of scam is known as an 'authorised push payment'.

If you are not happy with how your bank deals with your scam report, Consumer Affairs advises that you submit a formal complaint. If you are unsatisfied with your bank's response to your complaint, it is advised that you submit a complaint with the Bermuda Monetary Authority. If the Bermuda Monetary Authority decides that you have been treated unfairly, the Bermuda Monetary Authority has legal authority to comply your bank to operated fairly.

If you have used a money transfer service (i.e. Western Union) it is unlikely you will be able to get your money back. There are things you can do to protect yourself if you ever need to use a money transfer service again.

You should:

- only send money to someone you know
- choose a password that's hard to guess and don't share it with others

# 6. How to Protect Yourself Online

There are things you can do to protect yourself from being scammed online. If you are buying something on a site you have not used before, Consumer Affairs advises that you spend a few minutes checking the website; starting with the company's contract terms and conditions. The company's address should have a street name, not just a post office box.

Following a review of the company's website, Consumer Affairs advises that you check to see what people have said about the company. It is worth looking for reviews on different websites and do not rely on reviews the company has put on its own website. Also, do not rely on seeing a padlock in the address bar of your internet browser. The existence of a padlock in the address bar does not guarantee you are buying from a real company.

Do not click on or download anything you don't trust (e.g. if you get an email from a company with a strange email address). Downloading suspicious content could infect your computer with a virus. Additionally, Consumer Affairs advises that you make sure your antivirus software is up to date to give you more protection.

Some online scams try to get you to provide your personal information (e.g. the name of your primary school or your social security number). Scammers can use this information to hack your bank accounts. If you come across sites that ask for this type of information, without an obvious reason, first check that the company is legitimate.

Make sure you have a strong password for your email accounts that you don't use anywhere else. Some websites let you add a second step when you log in to your account (i.e. "two-factor authentication"). Two-factor authentication makes it harder for scammers to access your accounts.

Additionally, Consumer Affairs advises that you familiarize yourself with how your service providers will contact you (i.e. your bank, electricity and electronic communications service providers). Check your service provider's website to see how your they will and won't communicate with you (e.g. find out what type of security questions they'll ask if they phone you).

## How to contact Consumer Affairs

**Mailing address:**
D. Rego Building, 3rd Floor
75 Reid Street
Hamilton HM 12

**Telephone:**
Consumer Affairs (441) 297-7627
Rental Unit (441) 297-7700
**Fax**: (441) 295-6892
**E-mail:** consumers@gov.bm
**FB** – Consumer Affairs Bermuda

Published by the Ministry of Legal Affairs and Constitutional Reform
Design and pre-press production: Department of Communication & Information
Printed in Bermuda by the Bermuda Press Ltd