Cybercrime and Fraud Guide for Customers

Bank of St. Helena Ltd.

www.sainthelenabank.com

Contents

Introduction

Bank of St Helena Ltd takes our customer security very seriously and employ a wide range of measures to help keep you protected which includes multiple firewall solutions, data encryption, and fraud detection tools. With that in mind, we want to help you spot signs of fraud and cybercrimes to help protect yourself as well.

Both fraud and cyber scams are evolving and becoming more sophisticated which makes them harder to spot in their various forms. Our digital dependency provides fraudsters the opportunity to commit various types of financial fraud and we would urge customers to think before they click and learn more about being safe online.

Fraudsters use a variety of ways to trick victims including emails, text messages, social media, telephone and even in person. This guide describes the most common types of fraud and cybercrimes and how to spot them.

What are Cybercrimes

Cybercrimes are a type of criminal activity that either targets or uses a computer or mobile device (i.e. mobile phone, tablet) or a computer network. These crimes can be aimed at gaining money or to damage computers or networks for reasons other than profit. Cybercrime can be carried out by individuals or organisations. Some cybercriminals are organised, use advanced techniques and are highly technically skilled.

Social engineering scams are a common type of cybercrime where scammers use impersonation to try and con you. They attempt to win your trust and trick you into giving them money directly or disclosing confidential information voluntarily.

These attacks are common because scammers find it easier to take advantage of your natural instinct to trust than it is to break into your systems such as your email account. Common channels scammers use are fake phone calls, chat messages, emails, web pages and apps. They are more likely to impersonate your relatives or friends, officials of trusted organisations and government agencies. This tactic is intended to convince you to give them sensitive personal information voluntarily such as your account passwords.

What is Fraud

Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person. Personal and financial information obtained in a breach can be used to commit frauds affecting individuals, the private and public sectors alike. By harvesting personal and financial information through data breaches, criminals are able to commit fraud and damage people, businesses and services.

Victims of fraud range across vulnerable individuals, major corporations, smaller businesses, as well as the public sector. Fraud against individuals is typically targeted at elderly and other vulnerable people, for whom the consequences can often be devastating – psychologically as well as financially.

Fraud is increasingly being committed online. Where previously a fraud may have been committed by phone, post or in person, online access enables fraudsters to exploit victims remotely, often from another country. Some investment frauds, and most computer software service fraud, are known to be perpetrated from overseas.

Phishing

What is Phishing?

Phishing is an attack in which the scammer poses as a trusted person or organisation to trick potential victims into sharing sensitive information or sending them money. As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types (smishing and vishing are discussed later).

The Sender

In a phishing attack, the sender imitates (or "spoofs") someone trustworthy that the recipient would likely know. Depending on the type of phishing attack, it could be an individual, like a family member of the recipient, the CEO of the company they work for, or even someone famous who is supposedly giving something away. Often phishing messages mimic emails from large companies like PayPal, Amazon, or Microsoft, and also other banks or government offices.

The Message

Under the guise of someone trusted, the attacker will ask the recipient to click a link, download an attachment, or to send money. When the victim opens the message, they find a scary message meant to overcome their better judgement by filling them with fear. The message may demand that the victim go to a website and take immediate action or risk some sort of consequence.

The Destination

If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they comply, the sign-on information goes to the scammer, who uses it to steal identities, pilfer bank accounts, and sell personal information.

How do these attacks usually happen?

Phishing attacks begin with the scammer sending a communication, acting as someone trusted or familiar. The sender asks the recipient to take an action, often implying an urgent need to do so.

Email Phishing

Email phishing is one of the most common types of phishing and occurs when fraudsters masquerade as a trusted organisation to obtain confidential information such as personal information, bank details or passwords. The attacker sends an email claiming to be someone trustworthy and familiar (e.g. local retailer) and asks you to click a link to take an important action, or perhaps download an attachment. Often the email will link to a fake website which may appear almost identical to the legitimate website. This website will then entice the victim to enter log-on credentials or download malware. Additionally, the email communication will usually suggest that you must act urgently, maybe to prevent your online access from being blocked.

Remember, phishing emails can look extremely convincing by copying branding and spoofing email addresses to seem genuine.

Spear Phishing

Spear phishing is a targeted form of a phishing attack. Spear phishers generally disguise themselves as a legitimate, familiar sender, often from within the same organisation, to increase the chance the recipient will carry out the intended action.

This could include opening the attached file or visiting a website which would typically download malware, divulging sensitive personal or commercial information or being duped into completing a transaction. For instance, a fraudster might spear phish an employee whose responsibilities include the ability to authorise payments. The email implies to be from an executive in the organisation, commanding the employee to send a substantial payment either to the CEO or to a company vendor, but instead, the malicious payment link sends it to the attacker.

Whale Phishing

Whale phishing is for phishers looking to target high-profile victims. This can include Chief Executors and Directors. Typically, the attacker is trying to trick these well-known targets into giving their personal information and/or business credentials. Whaling attacks usually involve social engineering efforts to trick the victim into believing the deception.

Pop-Up Phishing

These cyberattacks use pop-up messages to trick users into sharing their financial details or downloading malicious software by pretending you have won a prize.

Recognising an attack

Recognising a phishing attempt isn't always easy. They often use fear to cloud your judgement. Here are a few common signs of a phishing attempt:

Bank of St Helena would not contact you requesting your Local Debit Card number, PIN or Online Banking Customer ID / password. To verify your identity, you will be asked for your Security Information which includes your Card Security Number (Local Debit Card) and memorable questions (Online Banking).

The Bank's official e-newsletters include link buttons, however, customers can search the official website directly for information on the newsletter topics or contact the Bank using info@sainthelenabank.com.

Requests for sensitive information

Always establish if the request for sensitive information is reasonable.

Attachment formats

Cybercriminals try to get you to unknowingly install malware. It would most likely be a .zip, .exe or .scr file.

Emotional appeals

They will try to elicit fear or urgency to convince you to act carelessly.

Link address

The hyperlink and actual linked page could differ and lead you to a malicious website.

Unsolicited emails

They will task something or offer you a reward that you didn't request or initiate.

Email sender domain

Even after evaluating the domain, you can never be 100% sure that the email is authentic.

Grammar or odd phrasing

Watch out for grammatical spelling errors and things that are technically correct, but nobody says.

Smishing

What is Smishing?

A fraud which targets the users of mobile phones using text messages is referred to as a 'SMiShing' scam. Scammers aim to obtain private and confidential information from individuals or encourage them to ring a number or click on a link for more information. Fraudsters may spoof the message onto a genuine message thread.

Each smishing attack uses similar methods, while the presentation may vary significantly. Attackers can use a wide variety of identities and premises to keep these SMS attacks fresh.

Typically, an attacker will claim there is an error with your account and give you steps to resolve it. The request can be as simple as using a fraudulent login page, while more complex schemes may ask you to provide a real account recovery code in an attempt to reset your password. Warnings of a support-based smishing scheme include an issue with billing, account access, unusual activity, or resolving your recent customer complaint.

How do these attacks usually happen?

SMS phishing attacks primarily spread uninterrupted and unnoticed due to their deceptive nature. Smishing deception is enhanced due to users having false confidence in text message safety.

Firstly, most people know about the risks of email fraud. You’ve probably learned to be suspicious of generic emails that say "Hi—check out this link." The exclusion of an authentic personal message tends to be a substantial red flag of email spam scams.

When people are on their phones, they are less wary. Many assume that their smartphones are more secure than computers. But smartphone security has limitations and cannot always directly protect against smishing.

Another risk factor is that when you’re on your smartphone and on the go, often you’re distracted or in a hurry. This means you’re more likely to get caught with your guard down and respond without thinking when you receive a message asking for bank information or to redeem a coupon.

Regardless of the means being used, these schemes ultimately require very little beyond your trust and a lapse in judgment to succeed. As a result, smishing can attack any mobile device with text messaging capabilities.

Gift Smishing

Gift smishing suggests the promise of free services or products, often from a reputable retailer or other company. These can be giveaway contests, shopping rewards, or any number of other free offers. When an attacker elevates your excitement by proposing the idea of “free,” this serves as a logic override to get you to act faster. Signs of this attack can include limited time offers or exclusive selection for a free gift card.

Invoice or Order Confirmation Smishing

Confirmation smishing involves a false confirmation of a recent purchase or billing invoice for a service. A link may be provided for a follow-up to manipulate your curiosity or prompt immediate action to trigger fear of unwanted charges. Evidence of this scam may involve strings of order confirmation texts or the absence of a business name.

Customer Support Smishing

Customer support smishing attackers pose as a trusted company’s support representative to help you resolve an issue.

Recognising an attack

As with phishing attacks, spotting smishing attacks isn’t always easy. Look for something that's off or unusual. Here is some advice when receiving a suspicious text:

At present, Bank of St Helena do not use SMS texting to contact customers.

An unexpected scary message

Sometimes, a hacker will try to scare you into clicking an infested link. They might say your bank account's been compromised or that you have minutes left to change a password. If you get a message like this, always question it - hesitating might just save you from being Smished.

A number you don't know

We've all been taught to be suspicious of strangers, and strange numbers are just an extension of that. If you don't recognise a number that's texting you, be cautious. It's possible the texter's not who they claim to be.

Ridiculous text

Not all hackers are sophisticated. Some might send a text that has nothing to do with you or that sounds too general to be legitimate.

Identity crisis

Does the person texting you sound off? As if they're not themselves? If that's the case, there's plausible reason, they aren't themselves at all.

Poor grammar

If the person texting can't spell your name right, chances are you don't actually know them. Weird punctuation, capitalisation and syntax are all warning signs.

Vishing

What is Vishing?

Vishing, or 'voice call phishing' involves phone-based phishing attempts to trick you into providing your personal information such as online banking passwords, confidential details or to persuade you to transfer money from your account.

Often, through the research carried out, the fraudsters will have your name, address, colleague names and bank details, essentially the kind of information that you would expect a genuine caller to have. The phisher may call claiming to represent your bank, the police, or the government. Next, they scare you with some sort of problem and insist you clear it up immediately by sharing your account information or paying a fine.

How do these attacks usually happen?

Vishing attacks can be as varied as phishing attacks. Some of the most common pretexts used in vishing include:

Account Issue

A visher may pretend to be from a service provider claiming that an issue exists with a customer's account. They will then ask for personal information to "verify the customer's identity."

Government Representative

A vishing attack may include an attacker masquerading as a representative of a government agency. These attacks are typically designed to steal personal information or trick the victim into sending money to the attacker.

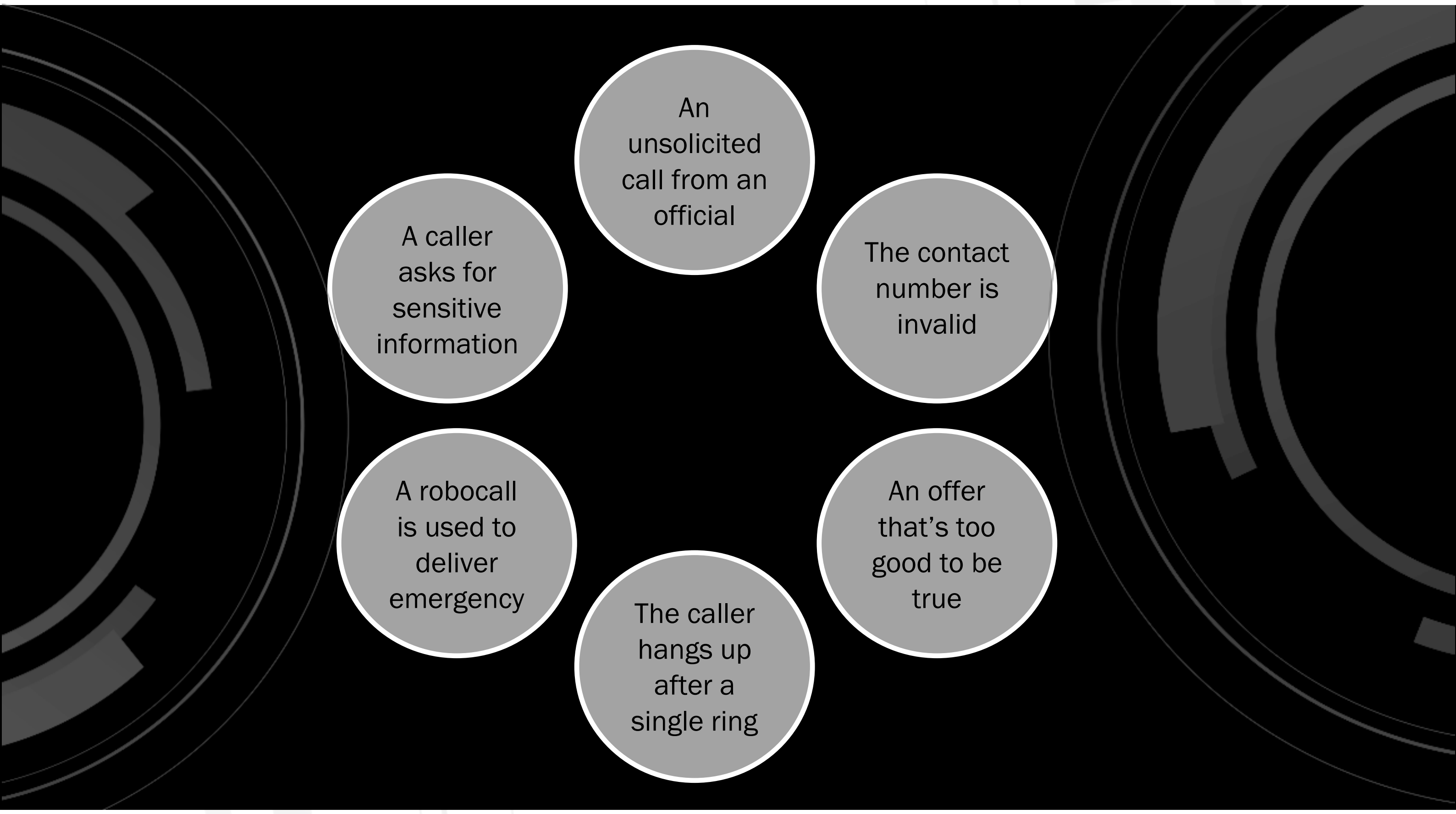
Tech Support

Social engineers may pretend to be tech support from large and well-known companies like Microsoft or Google. These attackers will pretend to help to fix an issue on the victim's computer or browser but actually install malware.

Recognising an attack

Here are some signs to look out for:

Bank of St Helena may contact you by telephone but would not request your Local Debit Card number, PIN or Online Banking Customer ID / password. To verify your identity, you will be asked for your Security Information which includes your Card Security Number (Local Debit Card) and memorable questions (Online Banking).



An unsolicited call from an official

The contact number is invalid

An offer that's too good to be true

The caller hangs up after a single ring

A robocall is used to deliver emergency

A caller asks for sensitive information

Social Media Scams

What are Social Media Scams?

Due to its wealth of personal information, social media has become a valuable tool for fraudsters to carry out their social engineering attacks. These scams are committed on social networking sites where scammers often create fake profiles, befriend innocent people, and send spam messages or links that lead to malicious websites.

How do these attacks usually happen?

Fraudsters will often use the information contained on various social media platforms and pretend to be a trusted person and encourage users to disclose their confidential information or to take specific action (e.g. send a payment).

Scammers can also make adverts or posts appear genuine by using official brand logos and made up terms and conditions. They often appear as special offers or contests, tricking you into entering your personal and financial information. Some common types of social scams are:

Email Notification Phishing

Social media revolves around notifications. Almost every aspect of these platforms can send an update to users to bring them back to the platform or inform them. The point of contact outside the platform is always email, and the template they use is similar and rarely questioned.

Users receiving these email messages often click on the button, taking them to the notification without paying too much attention to the rest of the design. This behaviour is what hackers rely on to get users to click on fraudulent links hidden in the buttons. The site it takes them to is then used to steal sensitive information via a fake password reset scam or malware download.

Facebook Quiz Phishing

Quizzes of all types started popping up all over Facebook, some using platform apps and some hosted on a different website. The titles range from “What type of childhood did you have” to “What kind of driver are you” and seem relatively harmless. However, the questions asked during the quiz are crafted to make the victim surrender information that are common answers to password security questions. This data is then used to reset the passwords of the victim’s account and take control of it.

While these quizzes may be entertaining, it’s best not to answer them since it’s too difficult to determine which ones are legitimate. It’s also ideal to keep your social media account private to strangers and never state identifying information in your image captions (make and model of your first car, address of your house growing up, etc.).

LinkedIn Fake Job Scam

In recent years, the job market has been on fire and employees are constantly on the lookout for qualified individuals. LinkedIn has allowed for the recruitment process to become highly streamlined. However, it’s also allowed scammers to create fraudulent company pages to run fake job scams.

They’ll create a job posting and collect applications or message users to share it with them. Some do this to gather sensitive information to launch phishing attacks later. Others will act as if the victim got the job and mail them a fraudulent check for their first pay, asking them to send back a portion to them for whatever reason.

The check later bounces, the scammer escapes with the money, and the victim is out for that amount. This type of practice is always a scam, and it’s the best way to spot a fake job scam. This scenario demonstrates why it’s paramount to research any employer before applying for a job to make sure they are legit.

The same thing applies to sharing personal information with an employer. Ensure it’s done over secure communication and you fully understand why the employer is asking you for this information.

In-App Phishing

All social media platforms include some form of direct messaging between users. This functionality has led many scammers to create fake profiles closely reminiscent of their victim's friends or family. They then ask users to send them money to cover a bill or share a password with them.

Fake social media profiles can be challenging to discern. Depending on the platform, scammers will have collected information such as jobs and city of birth to make profiles look incredibly realistic. Add recent photos, and you could quickly become the victim of a scam.

Fake Customer Support

One of the biggest tasks done on social media is getting direct support from a company. The instantaneous nature of online chats makes them more convenient than long phone calls, and consumers often prefer them. This consumer need has led many companies to start dedicated support accounts.

These accounts are only a stolen logo and description away from hackers scamming people. Using these accounts, criminals will contact people who have requested help, passing as the company. They'll then direct them to a fake login page to steal their login information. Particularly brazen scammers will even get their victims to pay for repair services.

Recognising an attack

Here is some advice when faced with possible social scams.

Bank of St Helena would not contact you via social media unless you have made first contact using the channels – Facebook and LinkedIn (links to social media channels can be found on the Bank's official website). The Bank does not use WhatsApp to contact customers.

Don't click on suspicious links

Be wary of any posts or messages that ask you to click on a link. Even if you know the person, pay close attention to the language and tone of the message. If something seems even the slightest bit off, ignore and delete the message.

Don't accept friend requests from strangers

If you accept a friend request from someone you're not familiar with, they can access all the personal details on your profile, your contact lists, and build a detailed picture of your online social activity.

Provide limited information

The amount of personal information you have to provide on social media profiles is optional, so avoid sharing sensitive information such as your home address and phone number.

Do your research

Check the person is genuine by looking up their name, profile picture or any other information they've provided you with.

Use enhanced privacy settings

Regularly check and adjust your privacy settings to restrict what people can and can't see on your profile. You should also restrict permissions for apps to access your personal information.

Enable 'Two-Factor Authentication'

Most social media sites offer Two-Factor Authentication. This provides an extra layer of security to your online accounts and means that even if someone steals or guesses your password, they won't be able to access your account without a second authenticating factor.

Use strong and unique passwords

Using the same password across multiple accounts greatly increases your chance of being hacked. You should use a unique password for each social media account and make it as strong and secure as possible.

Website Spoofing

What is Website Spoofing?

Website spoofing (or website scams) involves making a malicious website look like a legitimate one. The spoofed site will look like the login page for a website you frequent, down to the branding, user interface, and even a spoofed domain name that looks the same at first glance. Cybercriminals use these websites to capture your username and password or drop malware onto your computer. This is potentially more devastating because they could gain access to any information you save on that device. A scam site will generally be used in conjunction with a phishing email, in which the email will link to the website.

How do these attacks usually happen?

Registering a domain name requires little effort and has little oversight. There are some barriers in place to prevent near-identical domains from being created, but scammers are clever enough to find workarounds.

After a person has fallen for a spoofed website, they will likely carry on with their normal behaviour without a second thought. This could include typing in their username and password or entering in banking information, which is exactly what the scammer is hoping for.

Even though you think it's business as usual, the website is saving whatever information you enter. The scammer can then use your login information to gain access to the legitimate website, or any other website that uses the same username and password.

Recognising an attack

Web spoofers follow similar tactics and make common mistakes in their attempts to fool their victims. That makes it possible to identify them for what they are. Here are a few tips.

Bank of St Helena's official websites are: https://sainthelenabank.com, https://sainthelenabankonline.com and https://ibanktc.sainthelenabankonline.com.

Double-check the details

If a scammer executes the spoofed website well enough, it may be hard to distinguish it from the real thing. Before entering your login information or clicking on anything at all, take a moment to double-check these known red flags.

Phishing email makes suspicious requests

The body of the email often contains a shocking accusation that requires immediate action for you to lower your guard. Banks, governments, and retail businesses have standard practices for resolving issues. If an email claiming to be from a trusted source asks you to act out of the ordinary, contact the originator through the official channels.

Incorrect spelling and grammar

Spelling and grammar mistakes in an email or website are a red flag that it has not originated from a professional organisation. It is quite common for the text to have been sent through a language translator.

Avoid clicking mysterious links

With the tactics of cybercriminals continuously improving, not even your own eyes and judgment can be trusted 100% of the time. The best way to evade a malicious link is to avoid clicking it entirely. Manually type the domain name into your browser to increase the likelihood of reaching the legitimate destination.

The website URL is unsecure

The website lacks basic URL security protocols. Sometimes your browser will warn you when it detects that a website is not safe to visit. This shouldn't be ignored, nor should it be relied on. Your browser can be fooled, too.

Look at the URL

The most common tactic among website spoofers is creating a URL that is nearly identical to a legitimate website. The URL may only be off by one letter, even using the number "1" in place of a lowercase "l". People can easily direct themselves to the spoofed page by mistakenly typing the wrong key or by only glancing at the URL before clicking through.

Check for an SSL certificate

A Secure Sockets Layer (SSL) is an added level of security for every visitor on a website. It is an encrypted link that protects your sensitive information from being shared without your consent. It is usually represented by a lock or green icon next to the URL. An SSL is not a guarantee that a website is legitimate, but it is a solid piece of evidence in its favour.

Make sure the domain matches the SSL certificate

Since a third party produces the SSL for the website, double-check the certificate by comparing it to the URL. Click on the SSL icon to validate its security. If it was issued to a website that is different from the domain in the URL, then something fishy is going on and it shouldn't be trusted. That might be a URL spoof.

Malware

What is Malware?

Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge. Cyber attackers create, use and sell malware for many different reasons, but it is most frequently used to steal personal, financial or business information. While their motivations vary, cyber attackers nearly always focus their tactics, techniques and procedures (TTPs) on gaining access to privileged credentials and accounts to carry out their mission.

Exfiltrate Information

Stealing data, credentials, payment information, etc. is a recurring theme in the realm of cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

Disrupt Operations

Actively working to “cause problems” for a target’s operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of “disruption” can vary. And there’s also the scenario where infected systems are directed to carry out large-scale distributed denial of service (DDOS) attacks.

Demand Payment

Some malware is focused on directly extorting money from the target. Malware attempts to prevent a target from accessing their data (usually by encrypting files on the target) until the target “pays up.”

How do these attacks usually happen?

You may be tricked into clicking on a link or attachment or installing a program. When this happens, usually a virus installs itself on your computer and uses malicious code to do things like scan for personal information or capture keystrokes without you knowing

Most malware types can be classified into one of the following categories:

Virus

When a computer virus is executed, it can replicate itself by modifying other programs and inserting its malicious code. It is the only type of malware that can “infect” other files and is one of the most difficult types of malware to remove.

Worm

A worm has the power to self-replicate without end-user involvement and can infect entire networks quickly by moving from one machine to another.

Trojan

Trojan malware disguises itself as a legitimate program, making it one of the most difficult types of malware to detect. This type of malware contains malicious code and instructions that, once executed by the victim, can operate under the radar. It is often used to let other types of malware into the system.

Hybrid malware

Modern malware is often a “hybrid” or combination of malicious software types. For example, “bots” first appear as Trojans then, once executed, act as worms. They are frequently used to target individual users as part of a larger network-wide cyber-attack.

Adware

Adware serves unwanted and aggressive advertising (e.g., pop-up ads) to the end-user.

Malvertising

Malvertising uses unprotected online advertising to spread malware and involves injecting malicious or malware laden code into advertisements on legitimate online internet site advertising networks and web pages.

Spyware

Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.

Ransomware

Ransomware is a type of malware that severely restricts access to a computer, device or file until a ransom is paid by the user. It has the ability to lock a computer screen or encrypt files with a password, often using strong encryption.

Recognising an attack

Malware code is often hidden in attachments, links and free downloads. Here are some tips on recognising a malware attack.

Popup Ads pop up everywhere

While not as common as they used to be, adware programs bombard their victims with advertisements. Sometimes there are ads for legitimate products, netting an affiliate fee for the adware perpetrator any time someone clicks on the ad. Other times they contain links to malicious websites that will attempt to drop more malware on your PC.

Your browser keeps getting redirected

Not every site redirect is malicious, but if you find that trying to reach a website or Google takes you to an unfamiliar search site, you've got a problem.

An unknown app sends scary warnings

Creating and distributing fake antivirus programs (also called scareware) is a lucrative business. The perpetrators use drive-by downloads or other sneaky techniques to get the fake antivirus onto your system, then display alarming warnings about made-up security threats.

Mysterious posts appear on your social media

Malware focused on Facebook and other social media sites propagates by generating fake posts or direct messages. Typically, these posts include an inflammatory statement of some kind, like "OMG were you really that drunk? Look at this picture!"

You get ransom demands

Some malware programs literally hold your PC or data for ransom. Overt ransomware threats encrypt all your pictures and documents and demand that you pay to get them back. Even worse are the ones that encrypt your entire computer, rendering it useless unless you pay to have it unlocked. Others are all bluff and bluster.

Your system tools are disabled

A smart user, suspecting the presence of malware, might launch ‘Task Manager’ to investigate, or check settings using ‘Registry Editor’. If you suddenly find that trying to use these or other system tools triggers a message saying your Administrator has disabled them, it may well be an attempt at self-defence by malware on your system.

Identity Theft

What is Identity Theft?

Identity theft occurs when criminals access enough personal information about an individual to commit fraud. They use various techniques to steal these details, from outright theft and social engineering to harvesting data through cybercrime. With this information, criminals can impersonate the victim in order to access bank accounts, fraudulently claim benefits or obtain genuine documents in the victim's name.

How do these attacks usually happen?

Criminals are increasingly stealing identity data online, for example persuading individuals to disclose personal details and passwords through 'phishing' emails, and then trading the data. Common ways fraudsters can steal your identity are through the following.

Vishing

Fraudsters call you pretending to be a genuine business and mislead you into giving away personal and financial information. They will attempt to make the call appear convincing by faking background noises so you believe it's a call centre environment.

Hacking / Malware

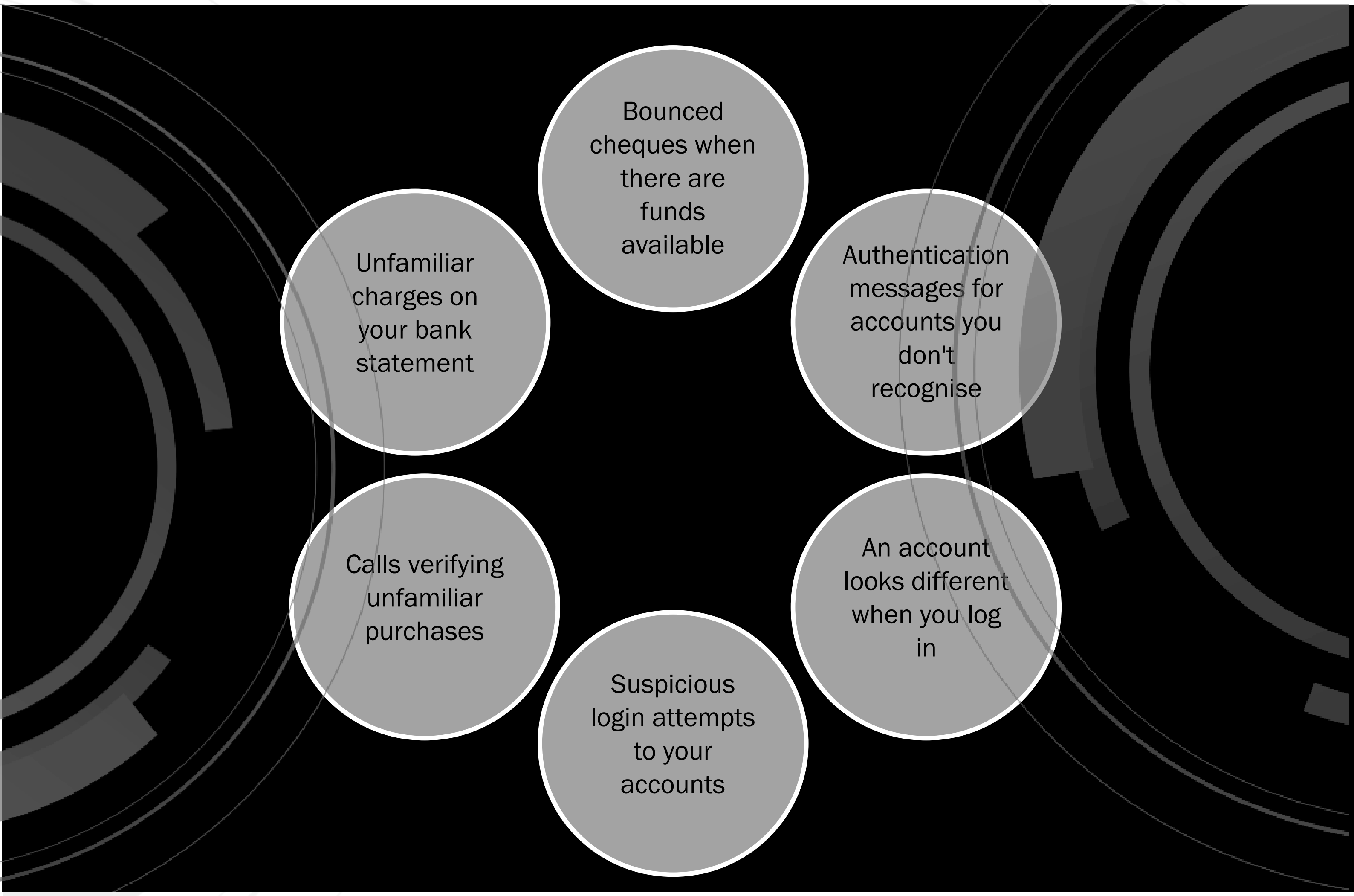
Software's used to hack into your computer, or information's taken from your smartphone.

Phishing

Fraudsters send an email that appears to be from a trusted company, getting you to click a link or download an attachment which would deliver a virus to your computer, allowing them to access your details.

Warning signs of Identity Theft

Here are some of the common warning signs that someone has stolen your identity.



Bounced cheques when there are funds available

Unfamiliar charges on your bank statement

Authentication messages for accounts you don't recognise

Calls verifying unfamiliar purchases

An account looks different when you log in

Suspicious login attempts to your accounts

Investment Scams

What are Investment Scams?

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Criminals will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

How do these attacks usually happen?

Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and returns are lost.

Fraudsters are organised and they may have details of previous investments you have made, or shares you have purchased. Knowing this information does not mean they are genuine.

Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

The fraudster may put pressure on you by offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit. If could be a scam if you're pressured to act quickly. Common types of scams are:

Cryptocurrency Scams

Cryptocurrencies are digital currencies and cryptocurrency investment scammers are convincing. Bitcoin is the most well-known form of digital currency. Scammers may advertise or post on social media offering great returns from cryptocurrency trading. If you click on the advertisement or post, the scammer will contact you or you will be directed to a fake website. The scammer will offer to make an investment on your behalf, or provide details of an app or website through which you can invest.

The scammers will encourage you to buy cryptocurrency through an exchange or request you send money to a company for them to do so on your behalf. They will then claim to either trade on your behalf, or coach you through making trades yourself. You will be able to see the profits you have made on a webpage, app or custom MetaTrader platform.

The data you can see will be fake and will show you profiting (or losing as a way to get you to invest more money). Eventually you will be unable to withdraw any money. The scammers will make excuses for delays in withdrawals, you are banned from the platform or the trading platform is closed. When you try and find out what has happened, the scammers cannot be contacted and your money is gone.

Romance Baiting

The scammer sets up a fake dating profile and will connect with you on a dating website, dating app or social media. The scammer will ask to continue chatting to you off the dating website or app, typically on a free but encrypted chat site such as WhatsApp, Google Hangouts or WeChat. They may say they want to do this as these chat sites are 'more private'.

Scammers will try to build your trust and will often do things like express strong emotions for you in a short period of time and share lots of 'personal' things with you.

Once they have gained your trust the scammer will tell you about an investment opportunity. Often, they say they have invested a small amount of and made a lot of money very quickly. They will encourage you to initially transfer a small amount of your own money to show how easy the investment is. You may see a quick return. The scammer then encourages you to invest larger amounts.

The scammer will tell you to top up your accounts to increase your profits. If or when you run out of money to transfer or want to withdraw all your funds, the scammer will cease all communication. You will then be unable to obtain your investments from the platform or be told the investment has gone wrong.

Celebrity Endorsement Scams

Scammers use the image, name and personal characteristics of well-known celebrities without their permission, to entice you into investing. Fake celebrity endorsements are often used to advertise scam cryptocurrency schemes.

The way the celebrities' image is used can take two forms:

An advert might pop up on social media or even YouTube using a celebrity's image and claiming they endorse or have made a large amount of money from an investment opportunity.

You may see a fake news story about an investment opportunity which appears to be from a well-known media using a celebrity's image.

The investment adverts or news stories make claims about investment opportunities with huge returns and will typically link to a scam website, often involving a cryptocurrency investment 'opportunity'.

Ponzi Schemes

Ponzi schemes are scams that use funds collected from new investors to pay existing investors. No real investment exists and eventually these schemes collapse. Scammers contact people on social media asking them to download or invest through apps. They promise you will see high returns very quickly and you will think you do, but the scammer uses money other people have invested to pay you some return.

Once you have seen a return, the scammer will persuade you to encourage your friends, family and colleagues to invest in the same scheme. They will pay them 'returns' and ask them to recruit people they know into the scheme as well. Eventually, when the scammer runs out of money or the pool of people being recruited dries up, the scammer will disappear and no one will be able to recover their money.

Recognising an attack

Here are some tips for recognising investment scams.

Bank of St Helena would not contact you to discuss investment schemes outside the available Savings Accounts.

Promise of low risks with high returns

Always remember, if something seems too good to be true it probably is. If you are promised 'guaranteed returns' this is a warning sign.

You are contacted out of the blue

You receive a call, email or message on social media from someone offering unsolicited advice on investments.

Someone you haven't met in person offers you investment advice

Never take investment advice from someone you meet on social media or any communication platform.

Use of celebrity endorsements or images

These are usually fake. Celebrities rarely discuss their investments or financial decisions in public.

You are asked to deposit funds into different accounts for each transaction

Scammers may claim this is for security reasons, or because they are an international company.

How you can help protect yourself from becoming a victim of a Cybercrime or Fraud

Always remember: if something seems too good to be true, it probably is.

1. *Do not disclose your personal information easily*

Scammers will do everything possible to trick you into providing them with your personal information. Remember that a Bank of St Helena representative will never ask you to disclose your passwords or PIN Number. Never provide this confidential information over the phone, text or via email to anyone claiming to be from the Bank of St Helena, or any other organisation. If you are not certain, please check with us or report it to us directly. Do not use the contacts provided by the suspicious email, text or phone call.

2. *Avoid sharing too much personal information on Social Media*

Be cautious about sharing personal information on social media, which might be used by fraudsters to trick you, relatives or friends.

3. *If you suspect a scam, please report it to the relevant party immediately*

If you think you might have encountered fraud with your Bank of St Helena Account, please report it to us using the Bank's published contact information or online forms. This is also applicable to someone pretending to be from another organisation, you should report it to the relevant person within the organisation, or to the police.

4. *Don't assume an email or phone call is authentic*

Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Be mindful of who you trust – criminals may try and trick you into their confidence by telling you that you've been a victim of fraud. Criminals often use this to draw you into the conversation, to scare you into acting and revealing security details. Remember, criminals can also make any telephone number appear on your phone handset so even if you recognise it or it seems authentic, do not use it as verification they are genuine.

5. *Don't be rushed or pressured into making a decision*

Under no circumstances would a genuine trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons. Remember to stop and take time to carefully consider your actions.

6. *Listen to your instincts*

If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

7. *Stay in control*

Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's okay to stop the discussion if you do not feel in control of it.

8. *Update your devices, apps, antivirus software and use a spam feature*

Computers and devices are regularly threatened by new viruses, so software updates can help combat these and protect your devices. It is recommended to download software from verified and trusted sites. Updated apps can also provide additional security as they are constantly updated by the creator. By having a spam feature the spoofed emails will be sent directly to your spam folder to reduce the risk of accidentally opening one. The spam filter is not guaranteed to catch everything, however, so stay aware.

9. *Think before you click*

Only click on links if you know and trust the sender, the same goes for downloading any files.

10. *Choose strong passwords*

Ensure unique, strong and secure passwords are used and it is best to change them often and not use the same details for your main accounts. Accessing reputable password managers can also assist in creating strong passwords that provide additional protection.

11. *Use bookmarks for frequently visited pages*

Since random links will be left unclicked, it's convenient to bookmark websites you regularly visit. This speeds up the process of visiting the page while reducing the chance of human error in typing it by hand.

12. *Manually search URLs*

If you must visit a page that is not already bookmarked, manually search for the URL. This avoids the risk of a malicious link planting a virus on your device. Take care that the URL is spelled correctly, otherwise, you will not reach the intended page.

Do you suspect you have been a victim of Cybercrime or Fraud?

Your first point of contact should be the Police to report the crime.

If you need help blocking your Bank Cards or changing your Online Banking Details please contact us on customerservices@sainthelenabank.com or (+290) 22390.

Glossary

Account Issue Vishing

A visher may pretend to be from a service provider claiming that an issue exists with a customer's account. They will then ask for personal information to "verify the customer's identity."

Adware

Adware serves unwanted and aggressive advertising (e.g., pop-up ads) to the end-user.

Celebrity Endorsement Scams

Scammers use the image, name and personal characteristics of well-known celebrities without their permission, to entice you into investing.

Cryptocurrency Scams

Scammers impersonate new or established businesses offering fraudulent crypto coins or tokens. If you click on the advertisement or post, the scammer will contact you or you will be directed to a fake website. The scammer will offer to make an investment on your behalf, or provide details of an app or website through which you can invest.

Customer Support Smishing

Customer support smishing attackers pose as a trusted company's support representative to help you resolve an issue.

Cybercrimes

Cybercrimes are a type of criminal activity that either targets or uses a computer, a computer network or a networked device. These crimes can be aimed at gaining money or to damage computers or networks for reasons other than profit.

Email Notification Phishing

For sites such as social media, an email message is common for updates. Users often click on the button, taking them to the notification without paying too much attention to the rest of the design. This behaviour is what hackers rely on to get users to click on fraudulent links hidden in the buttons.

Email Phishing

Email phishing is one of the most common types of phishing and occurs when fraudsters masquerade as a trusted organisation to obtain confidential information such as personal information, bank details or passwords.

Facebook Quiz Phishing

Questions asked during the quiz on Facebook (such as "What type of childhood did you have" to "What kind of driver are you") are crafted to make the victim surrender information that are common answers to password security questions.

Fraud

Fraud is when trickery is used to gain a dishonest advantage, which is often financial, over another person. Personal and financial information obtained in a breach can be used to commit frauds affecting individuals, the private and public sectors alike.

Gift Smishing

Gift smishing suggests the promise of free services or products, often from a reputable retailer or other company. These can be giveaway contests, shopping rewards, or any number of other free offers.

Government Representative Vishing

A vishing attacker masquerading as a representative of a government agency. These attacks are typically designed to steal personal information or trick the victim into sending money to the attacker.

Hybrid Malware

Modern malware is often a “hybrid” or combination of malicious software types. They are frequently used to target individual users as part of a larger network-wide cyber-attack.

Identity Theft

Identity theft occurs when criminals access enough personal information about an individual to commit fraud. They use various techniques to steal these details, from outright theft and social engineering to harvesting data through cybercrime.

In-App Phishing

All social media platforms include some form of direct messaging between users. This functionality has led many scammers to create fake profiles closely reminiscent of their victim’s friends or family. They then ask users to send them money to cover a bill or share a password with them.

Investment Scams

Criminals will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Invoice or Order Confirmation Smishing

Confirmation smishing involves a false confirmation of a recent purchase or billing invoice for a service. A link may be provided for a follow-up to manipulate your curiosity or prompt immediate action to trigger fear of unwanted charges.

Malware

Malware is a collective term used to refer to a multitude of malicious software, including viruses, Trojans and ransomware. It is created for nefarious purposes, typically to damage, disrupt or exploit vulnerabilities in computers.

Malvertising

Malvertising uses unprotected online advertising to spread malware and involves injecting malicious or malware laden code into advertisements on legitimate online internet site advertising networks and web pages.

Phishing

Phishing is an attempt to obtain sensitive information from a victim by email. The sender will claim to be emailing from a trusted source, such as a colleague, the victim's bank or similar. The email will typically direct the victim to a website which will ask them to share their passwords or credit card details, or install malware on the victim's device.

Ponzi Schemes

Ponzi schemes are scams that use funds collected from new investors to pay existing investors. No real investment exists and eventually these schemes collapse. They promise you will see high returns very quickly and you will think you do, but the scammer uses money other people have invested to pay you some return.

Pop-up Phishing

These cyberattacks use pop-up messages to trick users into sharing their financial details or downloading malicious software by pretending you have won a prize.

Ransomware

Ransomware is a type of malware designed to coerce victims into paying a ransom, often by restricting access to a computer, device or files until the user pays a fee. Other times, messages purporting to be from law enforcement agencies are displayed claiming the user has been involved in illegal online activities, and providing instructions to pay a fine.

Romance Baiting

Romance Baiting involves a scammer setting up a fake dating profile and will connect with you on a dating website, dating app or social media. The scammer will ask to continue chatting to you off the dating website or app, typically on a free but encrypted chat site such as WhatsApp, Google Hangouts or WeChat.

Smishing (SMiShing)

A social engineering technique which targets users of mobile phones/devices. Smishing is a type of phishing attack that uses SMS messages, instead of email (phishing), to obtain private and confidential information from individuals. The messages are typically designed to trick the recipient into downloading malware onto their mobile phone/device.

Social Engineering

The manipulation of people into performing actions or divulging sensitive or confidential information that can be used to gain physical access to areas or unauthorised access to computer systems, usually for fraudulent or other criminal purposes.

Social Media Scams

Social media scams are committed on social networking sites where scammers often create fake profiles, befriend innocent people, and send spam messages or links that lead to malicious websites.

Spam

Spam is unsolicited bulk email, the electronic equivalent of junk mail, that comes to your inbox. Spammers often disguise their email in an attempt to evade anti-spam software. Increasingly spam arrives via legitimate email addresses whose user credentials have been compromised. Spammers can send millions of emails in a single campaign at very little cost. Spam is frequently used to distribute malware. Spammers are now also exploiting the popularity of instant messaging and social networking sites such as Facebook and Twitter to avoid spam filters and to trick users into revealing sensitive and financial information.

Spear Phishing

A carefully crafted phishing attack directed at specific individuals or companies. The email is often made to look like it has arrived from a recognised source, to lull the recipient into a sense of trust. Although often intended to steal data for malicious purposes, cyber-criminals may also intend to install malware on a targeted user's computer.

Spyware

Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.

Tech Support Vishing

Social engineers may pretend to be tech support from large and well-known companies like Microsoft or Google. These attackers will pretend to help to fix an issue on the victim's computer or browser but actually install malware.

Trojan

A Trojan horse or Trojan is a program that appears harmless but is, in fact, malicious software. Typically, the malware would be hidden within an innocent-looking email attachment or a free computer program/application.

Virus

Viruses are malicious computer programs that can spread to other files. Viruses can have harmful effects such as displaying irritating messages, stealing data, or giving hackers control over your computer. Viruses can attach themselves to other programs or hide in code that runs automatically when you open certain types of files. Sometimes they can exploit security flaws in your computer's operating system to run and spread automatically. You might receive an infected file in a variety of ways, including via an email attachment, in a download from the Internet, or on a USB drive.

Vishing

Vishing uses the telephone in an attempt to scam users into divulging private or confidential information.

Website Spoofing

Website spoofing involves making a malicious website look like a legitimate one. The spoofed site will look like the login page for a website you frequent, down to the branding, user interface, and even a spoofed domain name that looks the same at first glance.

Whale Phishing

Whale phishing is for phishers looking to target high-profile victims. This can include Chief Executors and Directors.

Worm

A worm has the power to self-replicate without end-user involvement and can infect entire networks quickly by moving from one machine to another.

Bank of St. Helena Ltd.

www.sainthelenabank.com