nbf
In good hands

Your Guide to **Digital Safety**

Your Security is Our Shared Commitment

At National Bank of Fujairah, we believe the best security is built on a strong partnership—a partnership between you and your bank.

In a world that's more connected than ever, staying safe online is a shared responsibility. While digital tools make life easier, they also require us to be aware and prepared.

This guide is our commitment to that partnership. We are sharing our knowledge on the latest digital threats and the simple, effective steps we can take together to protect your financial well-being. Thank you for placing your trust in us.

Because with NBF, you're in good hands.

Table of Contents

nbf
In good hands

WHY IS DIGITAL SAFETY SO IMPORTANT?

We live in a digital age where our daily activities are deeply connected to the online world. While this technology brings incredible convenience, it also makes us vulnerable to new risks. Today, criminals can misuse advanced tools like Artificial Intelligence (AI) to create sophisticated scams, making it more important than ever to be vigilant.

Digital security means protecting your online identity, information, and devices from these evolving threats.

The Rise of Artificial Intelligence (AI) in Scams

Artificial Intelligence (AI) is a powerful technology that helps with many daily tasks, but criminals can misuse it to create convincing scams. They can generate false information or impersonate people with stunning accuracy. It's important to use your own judgment and double-check any information from AI before acting, especially if it involves money or security. Never share sensitive details like passwords or bank information with AI tools unless it's an official application from a company you trust.

- Always verify any information you receive from AI before acting on it, especially if it pertains to money, health, or security.
- Never share sensitive information, such as passwords, ID numbers, or bank details, with AI tools unless they are from official company applications.
- Be wary of AI applications that request excessive permissions, such as access to your camera, microphone, or contacts, especially if these features are not necessary for the service.
- Keep in mind that AI can seem convincing but may still provide incorrect or misleading answers. Use your judgment before making decisions based on its information.
- Teach children and family members that not everything an AI says, or shows is true.

Vishing

Vishing, short for "voice phishing," occurs when attackers call and pretend to be from your bank, a government office, or a company. Their goal is to pressure you into revealing personal or financial information over the phone. Vishing attacks are particularly dangerous because they exploit human trust and create a sense of urgency, often resulting in financial loss or identity theft.

- Do not share personal information such as PINs, passwords, or one-time codes over the phone.
- Be cautious of calls that use scare tactics, such as: "Your account will be blocked today," or "The police will come if you don't pay immediately."
- Remember: genuine banks, government agencies, or employers will never request confidential information over the phone.
- If you are unsure about a call, hang up and dial the official customer service number found on the back of your card or on the company's website.
- Avoid making financial transfers or purchases during a suspicious call, regardless of how urgent the caller seems.

Deepfake

Deepfakes are realistic-looking videos, audio, or images that are created using artificial intelligence. They can make it seem as though someone did or said something that never actually happened. While some deepfakes are created for fun, others are used by criminals for scams, spreading false information, blackmail, or impersonating trusted individuals.

- It's important to verify the authenticity of videos, voice notes, or images before believing or sharing them with others.
- Look for warning signs, such as unnatural facial expressions, lip movements that don't match the spoken words, or distorted lighting.
- If you receive a video or voice request from a boss, colleague, or family member asking for urgent money or information, be sure to double-check through another communication channel first.
- Avoid sharing suspicious content online, as it may contribute to scams or misinformation.
- Stay informed about new scams; understanding how deepfakes work can help you detect them more easily.

Securing Your Mobile Devices

Your smartphone is essential to your digital life, making it a target for criminals. Understanding these threats and taking a few simple precautions can help keep you safe.

Malicious Application Downloads

Malicious applications are disguised as legitimate apps but secretly contain harmful code. These apps can steal your personal information, track your activity, or even damage your device. Cybercriminals often present malicious apps as games, utilities, or free versions of popular applications.

- To stay safe, only download apps from trusted platforms such as the Apple App Store or Google Play Store.
- Avoid clicking on links in emails, messages, or websites that prompt you to “download this app quickly.”
- Before installing any app, check its reviews, ratings, and developer information. Be cautious if an app has poor reviews or very few downloads.
- Do not grant apps permissions they do not need, such as access to your camera, microphone, or location, unless it is necessary for the app’s functionality.
- Regularly update your apps and phone software to protect against vulnerabilities.
- Uninstall apps that you no longer use, as outdated apps can pose security risks

QR Code Safety

QR codes are widely used for payments, menus, and accessing websites due to their convenience. However, there is a risk of attackers replacing legitimate QR codes or creating fake ones that lead to malicious websites or initiate hidden downloads. Since QR codes obscure the destination link, they can be easily used to deceive users.

- Only scan QR codes from trusted sources, such as official businesses, banks, or event organizers. Be cautious of random QR codes found in public places, such as stickers on walls, posters, or ATMs.
- After scanning, always check the preview link before opening it. If the link appears suspicious, do not proceed.
- Never enter passwords, banking details, or personal information on websites accessed through unknown QR codes.
- Consider using a QR scanner that includes a security check and displays the link before you open it.
- If a QR code prompts you to download an app, ensure it redirects you to the official app store rather than a third-party website.

Android & iOS Safety Tips

Smartphones are powerful tools, but they are also common targets for cybercriminals. Both Android and iOS devices can be compromised if not properly secured. Taking a few precautions can significantly reduce your risk:

- Keep your device's software and apps updated regularly to fix security vulnerabilities.
- Only install apps from official app stores (such as Google Play and the Apple App Store). Avoid downloading APKs or using third-party app stores.
- Use strong passcodes, Face ID, or fingerprint authentication instead of simple PINs or swipe patterns.
- Enable "Find My iPhone" or "Find My Device to locate, lock, or wipe your phone if it gets lost.
- Do not jailbreak or root your phone, as this weakens built-in protections and makes it more vulnerable to malware.
- Review app permissions regularly and disable any unnecessary access to features like the camera, microphone, or location.
- Connect only to trusted Wi-Fi networks** and avoid using public Wi-Fi for sensitive activities.

Staying Safe on Social Media

Social media is a great way to connect, but it's also a common place for scams. Here's how you can protect your accounts on popular platforms

Social Media Safety Tips

Instagram

Instagram is a popular platform for sharing photos and videos, but it is also a hotspot for phishing and fake profiles. To stay safe:

- Set your profile to private so that only approved followers can see your posts.
- Be cautious of direct messages asking for personal details or links.
- Avoid logging in through links received via direct message; always use the official app.
- Turn on Two-Factor Authentication (2FA) in your account settings.
- Watch out for fake giveaway or prize messages.

TikTok

TikTok's short videos are entertaining, but attackers may exploit the platform to spread scams or harmful content. To enhance your security:

- Limit who can comment, duet, or message you through Privacy Settings.
- Be careful about oversharing personal details in your videos or profile.
- Report suspicious accounts, scams, or offensive content.
- Avoid clicking links in TikTok bios or messages unless they come from trusted, verified accounts.
- Regularly review which apps and websites are connected to your TikTok account.

Snapchat

- Snapchat is popular for sharing quick snaps, but it can be exploited through screenshots, fake profiles, or scams. To protect your account:
- Enable Login Verification (2FA) for added security.
- Be cautious about sending sensitive or private images, as screenshots can still be taken.
- Only add friends you know; avoid accepting random friend requests.
- Review your Snap Map settings to control who can see your location.
- Be wary of "Snapchat support" scams; official support will never ask for your password.

UNDERSTANDING TODAY'S DIGITAL THREATS

DATA THEFT

Data theft is the act of stealing private information of a user through computers, servers and devices. The intent behind this kind of activity is to gain personal and confidential information to help the commission of a crime such as theft of your money or stealing your identity to commit a fraud against someone else. Data theft is a rising problem for users and for businesses and corporations where employees have access to servers, laptops, external devices, and much more.

The most common form of data theft is hacking into personal computers to steal private information such as addresses, phone numbers and bank account details. Even with technological advancements, data thieves are able to find ways to hack into systems to steal the personal data of employees.

- Restrict access to your sensitive data through identity and access management.
- Set access permissions to control who can see what kind of data.
- Use encryption to protect data.
- Have a clear BYOD (Bring Your Own Device) policy.
- Establish and educate staff about confidential data policies.
- Staff needs to be diligent about email recipients and cc lists.

UNDERSTANDING TODAY'S DIGITAL THREATS

REMOTE ACCESS

Remote access is the ability to get access to a computer or a network from a remote distance. Fraudsters employ many tactics to persuade you to allow access to gain control of your computer by remote access.

HOW IT MAY HAPPEN

A random caller gets in touch with you, claiming to be a software company, a tech support provider or a telecom organisation. They state your computer is facing major technical issues and they need to access it remotely to fix the problem.

They might offer you to sell you software or request you to sign up for a service. And they ask for your personal details and bank/ credit card details.

They might call constantly.

We recommend that you never entertain such calls or allow remote access unless the service is one that you have pre-committed to.

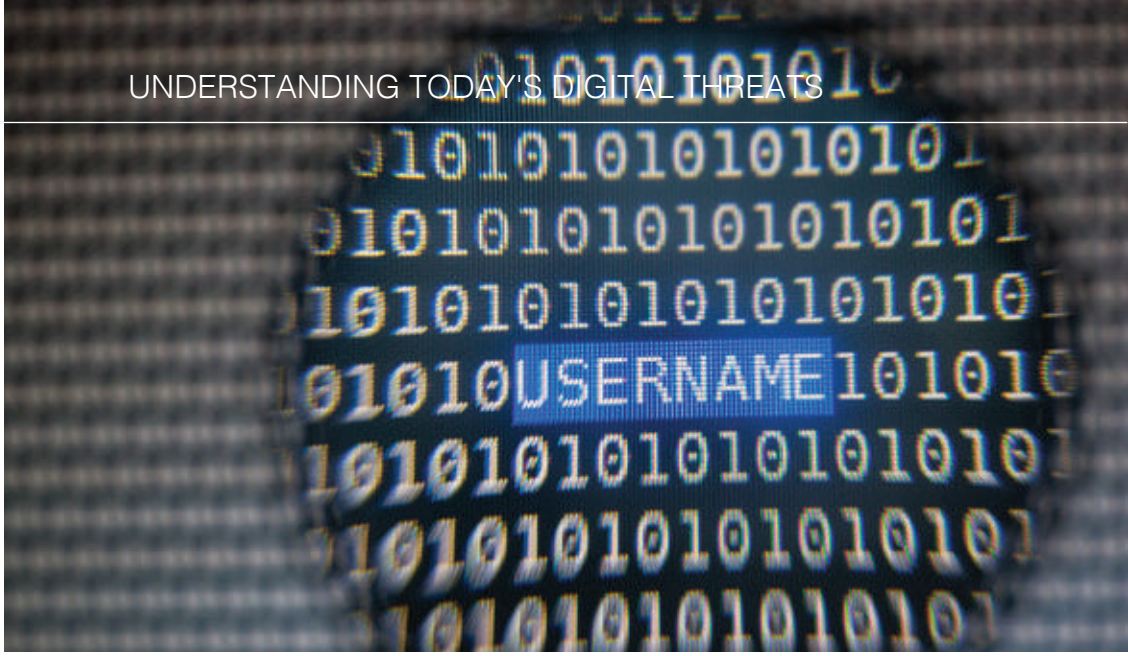
MALICIOUS SOFTWARE

Malicious software, commonly known as malware, is any software that harms your computer system. It is known by many names: viruses, trojans, worms, rootkits, spyware, adware, etc. They delete documents, steal protected data, add unwanted software... these are a few of the many problems they create. Once installed on your computer, these programs can seriously affect your privacy and your computer's security.

We recommend the installation of internet security software that should be updated constantly. There are a few other steps you can take to stay safe from malware.

- Update your operating systems, browsers and plugins. Switch on macro protection in Microsoft Office applications like Word and Excel.
- Switch on macro protection in Microsoft Office applications like Word and Excel.
- Don't open files from unknown/suspicious sources.
- Be alert when you use USB connected devices (memory sticks, external hard drives) since they are common carriers of viruses.
- Remove software you aren't using, specifically legacy programs (old Microsoft operating systems, Adobe Reader and media player systems).
- Purchase software from well-known trustworthy companies and download free software with caution.

UNDERSTANDING TODAY'S DIGITAL THREATS



PASSWORD CRACKING

Password cracking refers to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from a computer system. Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm. Numerous combinations are tried until the password is successfully discovered.

PASSWORD - DO'S

- Select a password with 10 characters or more (longer the password, the more difficult it will be to guess or crack). Make it a random combination of upper and lower case letters, numbers and symbols, e.g. Kdrt@3H*iyd^7
- Choose a song's line or a book title or a fact that wouldn't be associated with you. Alter it by employing the tips from the above sentence.
- Use different passwords for different sites.

PASSWORD - DON'TS

- Never use your username, actual name or business name.
- Family members or pet names.
- Birthday – yours or family members.
- Never type in keys in an order you find on your keyboard: For example, "qwerty" and "asdzxc" and "123456" are a bad idea, and easy to crack.
- Numerical sequences, either ascending or descending (12345 or 98765), duplicated numbers (33333) or keypad patterns they are easily recognised: 2480 or 78963), especially when choosing numerical passcodes or PINs.
- Don't store your password where it can be easily discovered.

PHISHING

Phishing is a cyber attack that uses disguised emails as a weapon. These emails pretend to come from a trusted organisation like a bank, credit card companies or e-commerce sites. The idea is to trick the email recipient into believing that the message is genuine and to click on a link, e.g. update password to prevent an account being suspended or a bank request to log into your internet banking account from a link in the email or a note from someone in their company or a known supplier — and to click a link or download an attachment.

HOW TO AVOID

- Prior to opening an attachment from an unknown source, verify the sender's email address.
- Do not click on emails from unknown sources. Hover the cursor over the sender's email address, which should bring up a "mouseover" box that will reveal its true destination.
- Don't unsubscribe to what might appear to you as a phishing email for it might take you to a hoax website.
- Don't reply to emails from unknown sources.
- Most internet security packages come with a spam blocking feature. Make sure yours is up to date and switched on.
- Most email clients (Microsoft, etc) have spam filtering as a standard feature. Ensure it is on.
- Check junk or spam mail folders because a legitimate email might be quarantined by mistake.

UNDERSTANDING TODAY'S DIGITAL THREATS

PUBLIC Wi-Fi

The very features that make free Wi-Fi hotspots so popular are the ones hackers exploit; namely, that it requires no authentication to establish a network connection. Hence Wi-Fi users are at risk from hackers so care must be taken when using free Wi-Fi. Please keep these points in mind.

- Wi-Fi spots are vulnerable places where cyber-criminals could intercept data that is transferred across the link.
- Your banking details, account passwords and other confidential data is at risk of being stolen.
- Never assume the Wi-Fi link is legitimate. It could be bogus, set up by criminals to capture valuable personal data.

RANSOMWARE

Criminals hijack your computer from a remote location with ransomware, a type of malicious software that encrypts and locks a victim's data. A pop-up window informs that the data will be unlocked only if a sum of money is paid. Only then will the attacker send a decryption key to release the data.

YOUR COMPUTER MAY GET ATTACKED BY RANSOMWARE UNDER THE FOLLOWING CIRCUMSTANCES WHEN YOU:

- Open a malicious attachment in an email.
- Click on a malicious link on a website, email, text message or social media site.
- Open corrupt macros in Word documents and Excel spreadsheets.
- Connect a corrupt USB connected device like a memory stick or an external hard drive, MP3 players.
- Open infected files from web-based digital file delivery sites like Dropbox, Hightail, etc.).
- Insert CDs/DVDs from untrustworthy sources like free music.
- Visit a corrupt website.

HOW TO AVOID

- Don't reply to or click on links in unknown or spam emails, especially from people or companies you do not know.
- Don't provide personal information when answering an email, unsolicited phone call, text message or instant message.
- Use reputable antivirus software and a firewall. Maintaining a strong firewall and keeping your security software up to date is critical.
- Employ content scanning and filtering on your mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
- Regularly back up your data to a remote USB connected device because some ransomware can affect even data stored on the Cloud.
- When travelling, make sure you use a trustworthy Wi-Fi source.

WHAT TO DO IF AFFECTED

- Ensure you are well prepared for such an attack by regularly backing up critical data
- Run a full scan with an up to date security solution to detect and remove any ransomware or malicious software.
- Restore any impacted files only from a known good backup. Restoration of your files from a backup is the fastest way to regain access to your data.
- If your computer gets locked, take advice from a trusted professional source.
- Do not pay the ransom since this only encourages and funds more attacks. Also, after payment, there is no guarantee that you will be able to regain access to your files.

UNDERSTANDING TODAY'S DIGITAL THREATS

SOCIAL ENGINEERING

Social engineering is the art of gaining access to systems or data by exploiting human psychology. A social engineer might pose as a work colleague from the IT department and try to trick you into revealing your password. Or you could be tricked into clicking on a malicious link that looks like it came from a Facebook friend or LinkedIn connection.

FOLLOW THESE STEPS TO AVOID SOCIAL ENGINEERING

- Never reveal confidential personal or professional information or customer data such as passwords, PINs, TINs or ID numbers.
- When you supply payment card information, ensure the person or company is genuine. Even then, never reveal passwords. Remember that a reputable bank or company will never ask for your password through an email or over the phone.
- If you're asked over the phone to reveal confidential information, request the caller/company's full and correct spelling. Hang up and find the company's official website, find a contact number, and ring back the person.
- Avoid opening email attachments from unknown or suspicious sources.
- Be aware of the information you are releasing on social media.

UNDERSTANDING TODAY'S DIGITAL THREATS

SMISHING

A form of phishing, smishing is when someone tries to trick you into giving them your private information via a text or SMS message. It is an emerging and growing threat, smishing is particularly alarming because sometimes people are more inclined to trust a text message than an email.

- Avoid clicking on any UNKNOWN messages with links. Furthermore, think about who sent you the message. Is it a person that you know?
- Don’t click on links in text messages unless you’re 100% certain they are genuine.
- Do not reply to text messages asking about your personal finances.
- Take time before replying to text messages. Think whether the sender, even a known one, would send you this kind of a text. Also, while the text message may be from a person you know, their number may be hacked or spoofed.
- Check the time when the unknown message was sent. If the text message was sent at an unusual time, then that is another sign of smishing.
- If unsure, call the person/organisation to authenticate the text message.
- If the text messages (along with the unknown number) calls for a quick reply then that is a clear sign of smishing. Do Not Reply!

SECURE YOUR DATA

ANTI-MALWARE PROTECTION
Anti-malware protection software is a given for most computer users. It has two main functions. First, providing advanced detection and prevention of malware. Second, early detection and preventing malware before it infects your system. The program can determine the infected area and will undertake the necessary steps to remove the infected file(s).

DATA BACKUP
Backing up your system on a routine basis is incredibly valuable since there is always a threat from new viruses that are being created on a daily basis across the world. Remote backups can be automated and updates can be created on a daily basis at set times. A full backup can create backups of all the data on the computer, including the operating system and installed applications in case a complete system restore is required.

DATA ENCRYPTION
Encryption is an ideal solution no matter where data is stored or how it is used. It should be standard for all data stored at all times, regardless of its importance.

FIREWALL
A firewall keeps hackers out of your network. Without its security, a hacker could get control of your computer, make it a part of a botnet, which is a large group of computers used to conduct an illicit activity, such as spreading viruses.
Internet Security
Always ensure your internet security systems are up to date in order to have maximum possible protection from cyber threats. Thousands of new viruses are created daily and software security manufacturers detected them and test them against their products. If there is an update, you will receive a notification. You have the choice of updating immediately or later but we recommend you download and install as soon as possible.

TWO-STEP AUTHENTICATION
A two-step authentication system, whether created by a passcode generator or a code sent via SMS, works by adding a second password to protected accounts. Both these authentication factors make for a stronger security model since it is more difficult to bypass or hack. This extra level of security lessens the risk of your online banking details, email or social media accounts being access by person/s seeking to exploit your online identity and data.

SECURE YOUR DATA

SMARTPHONE SECURITY
Smartphones are vulnerable to the same virus, spyware and phishing threats as your home computer.
- Always keep a screen lock activated on your phone.
- Use a password to unlock the screen.
- Only download apps from dedicated app stores to avoid exposure to malware, adware or ransomware.
- Avoid “jailbreaking” your device. It opens your phone up to malware and voids your warranty if a virus does occur.
- Activate an automatic cloud backup in case your phone is lost, stolen or destroyed.

SECURE PASSWORDS
Password security is of the utmost importance to reduce the likelihood of a hacker gaining access to your device. Make passwords long and complex. They should contain at least ten characters and have a combination of characters such as commas, percent signs, and parentheses, as well as upper case and lower case letters and numbers. Never write down your passwords since that makes it easier for them to be stolen and used by someone else. Also, never use the same password for two or more devices.

FRAUD AWARENESS AND PREVENTION

INVOICE FRAUD

Invoice fraud is a common occurrence in corporations and businesses. These kinds of fraudsters tend to choose companies based on their size in order to extract as much money as possible. With highly personal information about their target company, they create fake invoices and send it to the Accounts department.

Most of the time, if the department is overworked and lacks communication skills, these invoices get paid out without much research. Today, every business is vulnerable to invoice fraud and only the vigilance of staff members can help in preventing it.

- Match each invoice (3-Way Matching to a purchase order and receipt of goods. That way you're much less likely to pay a fraudulent invoice.
- Verify requests for amended payments by using established contact details, e.g. Call the sender on a telephone number previously used for communication.
- Track invoice activity to be able to notice when something changes, e.g. A sharp rise in invoices by a vendor.
- If you receive a call from an unknown number, refuse it. Then call the organisation using established contact details.
- Regularly check bank statements and report any suspicious activity to your bank.

FRAUD AWARENESS AND PREVENTION

CHEQUE FRAUD

Cheque fraud is a common form of financial crime where fake/manipulated cheques are deposited for payments. There are various types of cheque frauds and they include:

Cheque Theft: Stolen cheques, either in transit or from a victim, are fraudulently deposited for payments.

Cheque Washing: Manipulation of details related to the amount, date and beneficiary to cash the cheque.

Fake Cheques: Where genuine-looking cheques are created by copying details from original cheques including signatures.

Magic Ink Pen Usage: The cheque issuer is persuaded to fill up details with a pen provided by the 3rd party. The pen's 'magic ink' disappears after a while, allowing the fraudster to fill in a beneficiary name and amount, and fraudulently cash the cheque.

HOW TO PREVENT

- Keep cheque book under lock and key.
- Have different signatories for different amount thresholds.
- Regularly check SMS and email communication from your bank.
- Regularly check account statements and transactions to spot any unauthorized transaction.
- Always use your own pen when filling cheque details to avoid 'magic ink' pen fraud.
- Deliver goods/services to 3rd parties only after the cheque amount is credited to your account.
- Use electronic banking facilities offered by your bank instead of issuing cheques for payments as much as possible.
- If you find yourself a victim of cheque fraud, immediately notify the concerned bank and also consider filing a police complaint.

FUND TRANSFER FRAUD/ BUSINESS EMAIL COMPROMISE SCAM

Business Email Compromise (BEC) is a type of scam targeting companies who conduct wire transfers. So when you are transferring funds to a new account, make sure you validate the account details including bank name and account number. Use an alternate channel like making a phone call to the person/company using a phone number already known to you rather than relying on the phone number mentioned in the account's details.

Always be skeptical about any email that advises you that a supplier's banking details have changed.

Also, you could do a test transaction with a smaller amount. Once you get confirmation of receipt of funds, then transfer the remaining amount.

FRAUD AWARENESS AND PREVENTION

ADVANCE FEE SCAM

Advance fee fraud or upfront fee fraud is a scam where fraudsters charge processing fees in exchange of an opportunity to either participate in a special financial deal or by providing a share in an inheritance fund. There are many versions of this 'too good to be true' deal but the comment element is they all seek an advance fee.

Fraudsters pretend to be a bank employee/corporate executive or lawyer in relation to an inheritance fund where the customer has allegedly died with no surviving relatives. They get in touch via email or social media and sometimes even create fake social media profiles or use similar looking email addresses of genuine people to trick victims.

The victim is lured with the prospect of sharing in the inheritance. If the victim agrees to participate, fraudsters ask the victim to pay an 'advance fee' for taxes, legal charges, banking fees, notary charges, etc. thereby managing to extract money from the victim.

HOW TO AVOID

First and foremost, always remember that banks never send such emails or engage in social media communication with customers.

- These bank letters or financial documents are generally badly written and have spelling mistakes and poor grammar.
- To add credibility, the account holder's death is linked to a well-publicised incident such as a plane crash, earthquake, etc.
- Don't add unknown people to your chats and social media platforms and avoid opening emails from unknown senders.
- Keep in mind that something that appears 'too good to be true' is rarely true.
- If you are approached by people from a particular institution, report all the details to the institution using the email ID mentioned in the Contact Us or Report Fraud section of their actual website.

If you are a victim of advance fee fraud, follow these steps:

- Immediately stop contact with the fraudsters and don't send them any more money.
- Report the incident to relevant law enforcement authorities.
- If you have paid any money to fraudsters, report details to your bank in writing and provide a copy of the police complaint.
- A funds recall message can then be sent to the beneficiary bank by the remitting bank. If funds are available in the beneficiary account, they may get returned.

SIM REPLACEMENT FRAUD

Fraudsters obtain a duplicate SIM of the victim's mobile number. This allows them to receive calls/messages on behalf of the victim through which they can complete fraudulent fund transfer transactions.

They place fund transfer requests with the victim's bank by forging signatures or by using compromised login credentials. When the bank contacts the customer to validate the fund transfer transaction, the fraudster answers the call and provides the required details, and the transfer goes through.

The fraud is discovered when the victim realizes their mobile phone is not working and when they get a new SIM, they get the information about the unauthorized fund transfers or when they check their bank statement.

HOW TO AVOID

- Always update your contact details with your bank, especially new phone number/s.
- The moment you realize your phone is not working, call your bank and consider putting a debit freeze on your account.
- Get in touch with your telecom service provider and inquire whether any duplicate SIMs/Multi-SIM have been issued for your mobile number. If any are issued without your consent, get them deactivated.
- Install the latest anti-virus/malware software on your mobile phone, laptop or computer to prevent data compromise.

If you become a victim of SIM replacement fraud:

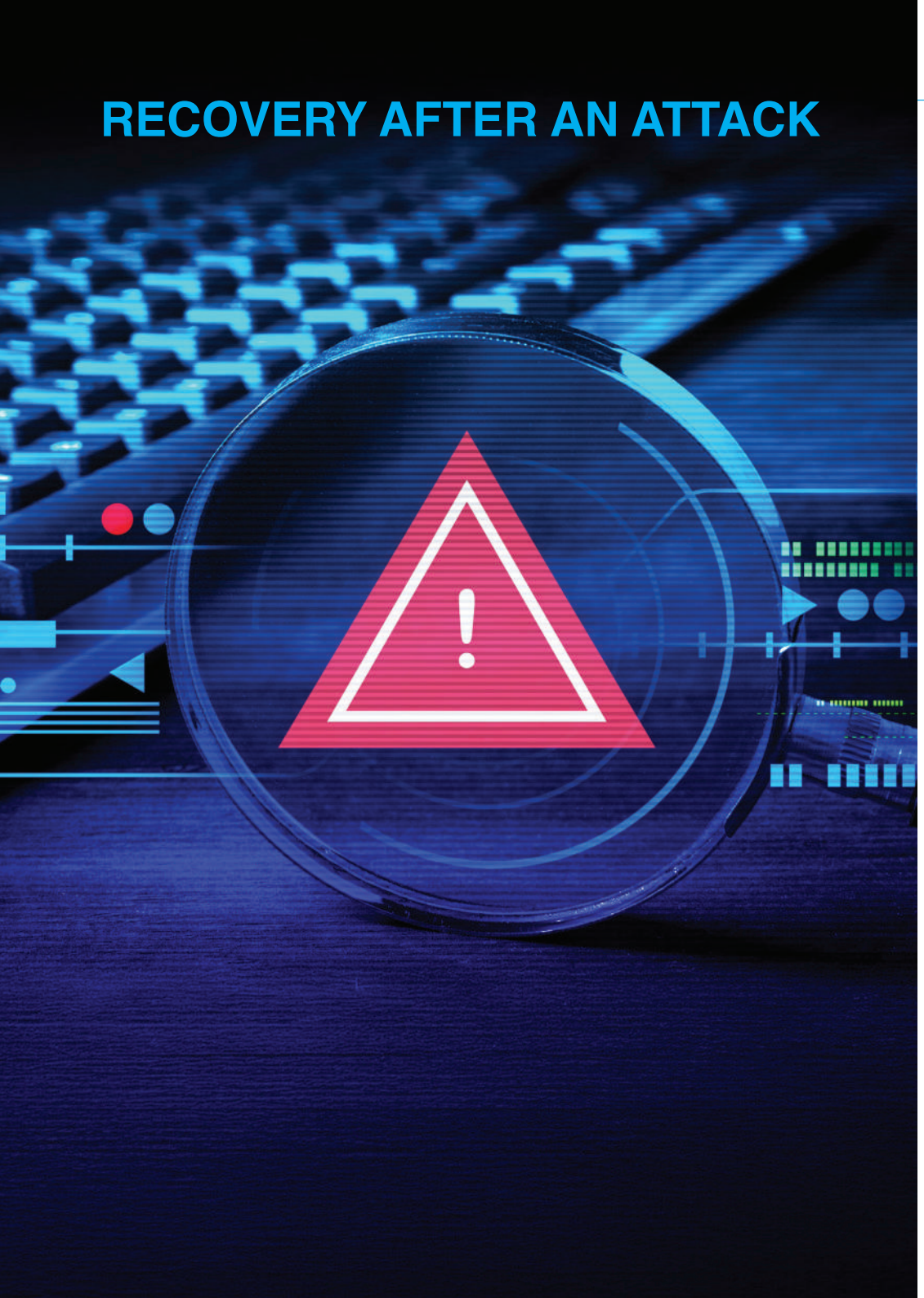
- Immediately notify your bank.
- Ask your telecom service provider for details about duplicate SIMs issued for your number.
- Consider filing a police complaint.
- A funds recall message can be sent to the beneficiary bank by the remitting bank. If funds are available in the beneficiary account, they may get returned.

FRAUD AWARENESS AND PREVENTION

ATM USAGE PRECAUTIONS

We use ATMs for the convenience of accessing our bank account/funds when we need it. While ATMs offer a secure way to conduct various types of banking transactions, you need to follow some basic precautions to ensure your account is never compromised.

- While entering your ATM PIN, keep one palm on top of the keyboard to ensure no one sees it.
- Ensure you remove your card and cash from the ATM. If you do not get either, immediately report it to your bank.
- If you opt for a transaction receipt, don't leave it behind in the ATM. If you don't need the receipt, then tear it before throwing it away.
- Subscribe for SMS alert and email alert service from your bank.
- Keep your phone number and email ID updated with your bank to ensure you always receive alerts.
- Regularly check your bank account statement and report any unknown transaction to your bank.
- Look for any loose ATM parts/devices. They could be placed there by fraudsters who want to steal your information.
- If you notice anybody behaving in a suspicious manner near the ATM, report it to concerned bank.



WHAT TO DO IF YOU SUSPECT A PROBLEM: WE'RE HERE TO HELP

If you think your account has been compromised or you've been targeted by a scam, please don't worry. Acting quickly is key, and we are ready to support you.

1. **Contact Us Immediately:** Call us on 600565551 at any time. The sooner we know, the faster we can help you secure your accounts and prevent any potential loss.
2. **Gather the Details:** Make a note of what happened, including the time, any websites you visited, or any numbers that contacted you.
3. **Report the Incident:** For your security and to help protect others, you can report the incident to the UAE Cybercrime authorities online at www.ecrime.ae.

Remember, you are not alone in this. As your banking partner, we are committed to helping you resolve the situation and restore your peace of mind.

ADWARE
A software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

BOTNET (INTERNET BOT)
A collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.

BREACH
An incident that results in the disclosure of potential exposure of data.

FIREWALL
A firewall is a network security system designed to prevent unauthorized access to public or private networks. Its purpose is to control incoming and outgoing communication based on a set of rules.

HACKING (COMPUTER HACKING)
To gain unauthorized access to data in a system or computer.

JAILBREAKING
Modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

MALWARE
Malicious software designed to infiltrate or damage a computer system without the owner's consent.

MOUSEOVER
A graphical control element that is activated when the user moves or "hovers" the pointer over its trigger area, usually with a mouse, but also possible using a digital pen.

PHISHING
Sending fraudulent emails requesting someone's personal and financial details.

GLOSSARY OF TERMS

ROOTKIT
A collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.

SPOOFING (EMAIL)
The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

SPYWARE
A computer software program or hardware device that enables an unauthorized person to secretly monitor and gather information about your computer use.

TROJAN
A type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.

TWO-STEP AUTHENTICATION
All techniques used to strengthen typical Username/password login session (e.g. single-factor authentication) by adding a second security challenge.

VIRUS (COMPUTER VIRUS)
A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

WORM (COMPUTER WORM)
A standalone malware computer program that replicates itself in order to spread to other computers.

We're Here For You

If you ever suspect any suspicious activity on your NBF account, alert us immediately.

Call Us 24/7
600565551

Email
InfoSec@nbf.ae

nbf
In good hands