Be Aware
Secure your On-line Experience

Table of Contents **Page #**

Introduction

The Internet is a universally accessible medium, which offers many benefits but admittedly, there are also risks. As a client of a financial institution, you may be seen as a potential target for fraudulent activities. By arming yourself with information and tools however, you can protect yourself from becoming a victim of fraud. Below we share many steps you can take to protect yourself online and make sure you don't fall prey to attempts to take your money. Our aim is to educate you generally, about online security.

Key Tips

1. Keep passwords, Personal Identification Number (PINs) and any other security information secret, including covering the key pad when entering your PIN at transaction machines such as our ETMs or at ATMs or Internet Banking in public places.

2. Create passwords that are hard-to-guess. The more complex and long, the better.

3. We will never ask you to provide your PIN to team members. Do not share with anyone.

4. Protect all your other personal information, including destroying your bank statements securely, collecting your mail promptly and not providing your details to anyone you do not know and trust.

5. Keep your computer safe by having up to date security software, check that you are only using trusted sites for purchasing items and not opening emails you're not sure about.

6. Never login to your bank website through a link in an email, even if the email appears to have come from your bank. Type the web address in yourself.

7. Keep your computer browser (e.g. Internet Explorer, Firefox), and product software (Microsoft Office/Adobe flash, etc) up to date. Software providers frequently develop updates and patches to address new and developing security threats.

8. When leaving your computer unattended, you should either shut it down or physically disconnect from the Internet connection. This lessens the chance that someone will be able to access your computer.

9. Treat all unsolicited emails with caution and never click on links from such emails and enter any personal information

10. Make sure your financial service provider has your up-to-date contact details.

11. Report anything you are suspicious of immediately, especially if you think your account has been compromised, a suspicious transaction is on your statement or your mail has been accessed by someone.

Passwords Tips

1. Do not choose a password that is easily identified with you (for example, your date of birth, telephone number or your name or any part of it). Use symbols as part of your password.

2. A password should have a minimum of eight characters, be as meaningless as possible and use uppercase letters, lowercase letters, numbers and special characters eg **xk28L$P97**.

3. Change passwords regularly, at least every 30 days.

4. Do not share your password with anyone! Be wary of unsolicited calls or emails requesting personal information or card numbers. JMMB will not ask you to disclose your PIN or password information.

5. Do not write your password down, even if it is disguised.

6. Do not use the same password in more than one place. If compromised, this limits unauthorized access to other places or your other systems.

If you believe your password has been compromised contact your service provider immediately.

Hoax Email or Phishing

Email is one of the prime movers for malicious viruses. Regardless of how enticing the 'subject' or attachment may look, be cautious. Any unexpected email, especially those with attachments (from someone you may or may not know), could contain a virus and may have been sent without that person's knowledge from an infected computer. Should you receive an email of this kind and you are doubtful of its legitimacy, delete it.

What is Phishing?

Phishing is the name given to the practice of sending emails at random, which claim to come from a reputable company such as your bank. The emails attempt to trick people into disclosing sensitive information at a bogus website 'phishing site' operated by fraudsters. These emails usually claim that it is necessary to "update" or "verify" your customer account information and they urge you to click on a link in the email which takes you to a phishing site. You may identify a real website by hovering (but don't click) your mouse pointer over the link. It should show you the real web address. Be very cautious if it looks nothing like the genuine company's web address and do not be fooled into thinking that just because the link uses your bank's name that it is genuine. It's possible to disguise the real destination of a link in an email. It may look like it is taking you to your bank's website but, in reality, you could be directed to a fraudster's bogus site.

An example is seen here where a link in an email appears to come from www.myonlinebank.com however hovering over the link it shows that it actually points to "www.malicioussite.com"

Sometimes the email won't contain a link; instead the recipient is asked to provide information on a form attached to the email. Any information entered on the phishing site or form will be used by the criminals for their own fraudulent purposes.

Phishing emails look like they come from a real email address from reputable organisations, such as your bank. However, it is relatively simple to create a fake entry in the "From:" box, so it should not be viewed as a guarantee that it has come from the person or organisation that it says it did.

Does a mail look "Phishy"?

- address you in vague terms, such as "Dear Sir / Madam or Dear Valued Customer"?
- ask for personal information, such as your online banking login details?
- ask you to click on a link in the email or download an attachment?
- come from an organisation you don't normally deal with?
- contain odd 'sp3lling', have poor grammar or use 'CaPiTals' in strange places (phishing emails do this in an attempt to avoid spam filter software).

If the answer is yes to more than one of these questions, the chances are that you've received a phishing email

If you receive a Hoax or Phishing Email

1. **Delete the email**
   If you receive a hoax email, delete the email immediately. Do not click on any links and do not open any attachments in a hoax email. JMMB will not ask you for your account details or financial or personal information via email or SMS.

2. **Report the incident**
   All hoax email incidents should be reported. These may be reported to cybersecurity@jmmb.com.

3. **Scan your computer for viruses**
   Many hoax emails contain viruses or Trojan Horses (key logger), which are downloaded to your computer when you open any attachments or select any included links. If you have clicked on any items within the email, run a complete virus check of your computer. If your computer still behaves in a suspicious manner after the virus scan, we recommend that you have a professional check your computer. We recommend that you perform virus scans on your computer regularly.

4. **Reset your Internet Banking password**
   After scanning your computer and ensuring it is free of viruses or Trojans, reset your Internet Banking password as per the procedures of your financial institution.

Protecting Your Identity

Identity theft is where your personal details are obtained to get some sort of financial or other benefit.

You can help protect your identity by following these tips:

- Report any loss or theft of documents such as driver license, credit card or passport immediately.
- If you have access to your personal credit file from a credit bureau, check on your status at least every six months.
- Keep tax records and other financial documents in a secure place.
- Cancel all unused or dormant accounts that you may have.
- Secure your mailbox with a padlock where possible.

Protecting Your Computer

Security is essential in protecting your information on the Internet. To do this, check your software vendors' web sites on a regular basis for new security upgrades, or use the automated patching features that some companies offer. The programs and operating system on your computer may have valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security on a regular basis.

Tips for General Computer Security

1. Have up-to-date virus protection on your computer.
2. Check for new Internet security protection software updates daily.
3. Scan all the files on your computer periodically including incoming and outgoing emails.

Virus Protection Software

A computer virus is a program that attaches itself to another program, but changes the action of that program so that the virus is able to spread. Viruses range from harmless pranks that merely show an annoying message, to programs that can destroy or disable a computer altogether.

Anti-virus software is designed to better protect you and your computer against known viruses, worms and Trojan Horses. A Trojan Horse is a malicious program disguised as something harmless, such as a game or a screen saver, but in fact contains hidden code that allows an intruder to take control of your machine without your knowledge.

There are malicious software that poses as Antivirus products. You should only use security software from reputable companies.

Internet Security Software

A firewall is a piece of software or hardware that filters all Internet traffic between your computer and the outside world. It works to either block or permit Internet traffic to and from your computer. You can use the Firewall to better protect your home or business computer and any personal information it holds from offensive websites, spam and unauthenticated logins from potential hackers.

A Firewall is seen to be essential for those who use their computers online, especially through the use of a cable modem. For more effective Internet protection, try using a firewall as a gatekeeper between your computer and the Internet.

Check your computer security on a regular basis and download the latest security upgrades.

Security Features on Websites

There are two ways you can generally verify that you are logging in to a secure web page:

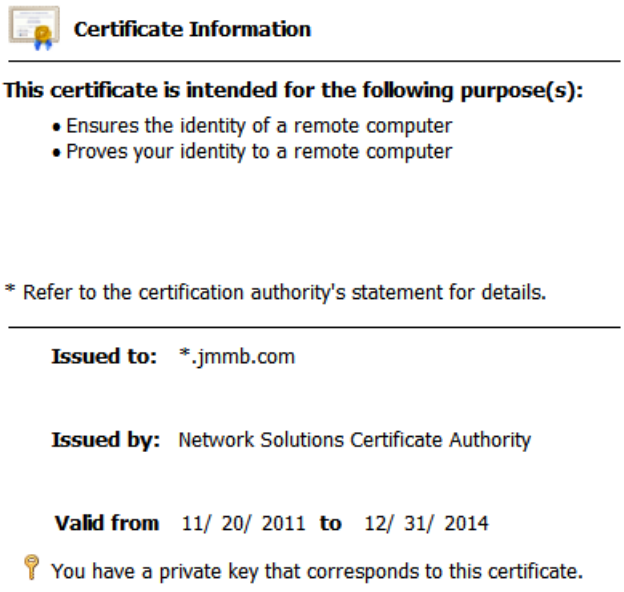
1. the website address changes from http:// to https:// when a secure connection is made.
2. a 'padlock' symbol appears on your web browser. The 'padlock' should be in the closed position and this symbol indicates that the page you are on has additional security. You can double-click the padlock symbol to view the security certificate's details.

   You can verify the authenticity of the 'padlock'.

   Double click on the 'padlock' symbol and ensure that the certificate:

   - is issued to the domain that you are interacting with
   - has a valid start and expiry date.

Certificate Example:



Beware of Fraudulent pop-up windows

Instead of displaying a completely fake website, the fraudsters may load the genuine website in the main browser window and then place their own fake pop-up window over the top of it. Displayed like this, you can see the address bar of the real website in the background, although any information you type into the pop-up window will be collected by the fraudsters for their own usage. To access your online banking account, type the address into a new window yourself. Use the security features of website mentioned above, to assess if website is legitimate and secure.

Using the Internet in public places

- Be wary of your surroundings and ensure no one is observing you when entering in your PIN or password.
- Ensure that there is a padlock symbol in the bottom right corner of your browser.
- Never click the 'save my password/details' option sometimes offered.
- Never change security details such as your password in a public place (ie libraries, Internet cafes).
- Do not leave your computer unattended or idle for long periods of time.
- Always log out from your online banking session when you have finished and close the browser.
- Try to use computers that have anti-virus software installed.

It is highly recommended that you never access internet banking or other sensitive systems in public places i.e. internet cafes

Scams and frauds

There are some individuals who could attempt to use your personal information to get access to your money. Scams are attempts to intentionally mislead a person, usually with the goal of financial or other gain. Many persons have fallen prey to various scams. It is therefore important for you to understand how to recognize and avoid scams. Below are a few tips and descriptions of some of the most common scams.

General tips to avoid scams

1. If it looks too good to be true—it probably is.
2. ALWAYS get independent advice if an offer involves significant money, time or commitment.
3. Remember there are no get-rich-quick schemes: the only people who make money are the scammers.
4. NEVER send money or give credit card or online account details to anyone you do not know and trust.
5. Check your bank account and credit card statements regularly. If you see a transaction you cannot explain on your account, contact your financial institution.
6. Keep your credit and any bank cards safe. Do not share your Personal Identity Number (PIN) with anyone. Do not keep any written copy of your PIN with the card.

Some Common Scams

Advance fee fraud: There are a number of variations on advance fee fraud, but they all ask people to pay an upfront fee to receive something of value. Once the fee is paid, the fraudster disappears.

Credit card fraud: This is another category that can include a variety of scams. It can include overcharging you for items you legitimately purchased as well as unauthorized credit card charges. Remember that as a consumer, you have more legal protections when using a credit card than a debit card. Also, review your credit card statements each month to ensure that they're accurate, and contact your credit card issuer immediately if you think you've been overcharged or if an unauthorized charge appears on your statement

The creation and/or alteration of a credit/debit card occurs when the information contained on the magnetic strip is reproduced. This type of crime is known as 'skimming'.

Computer crimes: This is a catch-all category that includes crimes targeting your computer or computer network, or crimes that attempt to use your computer or network to perpetrate other crimes. Take steps to secure your hardware, include password protection, firewalls and installation of spyware, anti-malware, anti-scamware and anti-virus software. If you're not comfortable installing these, ask a trusted friend or technology professional to safeguard your computers.

Identity theft: Email addresses are hijacked and the hijackers then contact people in the address books, claiming to have been mugged while on vacation overseas. The scammers or hijackers then request money, usually by wire money. Be vigilant about your email password and be skeptical if you receive email or IM requests from friends asking for money. Follow up with them offline to confirm the request

Nigerian Scams: You may receive an email/letter/fax that asks for your help to access a large sum of money in a foreign bank account. The message says that you will get a percentage of the funds in exchange for your help.

In all probability, the message is an example of the type of scam known as a Nigerian or "419" scam. The "large sum of money" does not exist. The messages are an opening gambit designed to draw potential victims deeper into the scam. Those who initiate a dialogue with the scammers by replying to the scam messages will eventually be asked for advance fees supposedly required to allow the deal to proceed. They may also become the victims of identity theft. The scammers use a variety of stories to explain why they need your help to access the funds.

For example:

- They may claim that political climate or legal issues preclude them from accessing funds in a foreign bank account.
- They may claim that your last name is the same as that of the deceased person who owned the account and suggest that you act as the Next of Kin of this person in order to gain access to the funds.
- They may claim that a rich merchant, who has a terminal illness, needs your help to distribute his or her wealth to charity.
- If you receive one of these scam emails, it is important that you do not respond to it in any way. The scammers are likely to act upon any response from those they see as potential victims.

Lottery Scams: You may receive an email/letter/fax that claims that you have won a great deal of money in an international lottery even though you have never bought a ticket. The email may claim that your email address was randomly chosen out of a large pool of addresses as a "winning entry". Such emails are almost certainly fraudulent. In some cases, the emails claim to be endorsed by well-known companies such as Microsoft or include links to legitimate lottery organization websites. Any relationships implied by these endorsements and links will be completely bogus.

There is no lottery and no prize. Those who initiate a dialogue with the scammers by replying to the messages will be first asked to provide a great deal of personal information. Eventually, they will be asked to send money, ostensibly to cover expenses associated with delivery of the supposed "winnings". They may also become the victims of identity theft. DO NOT respond to these messages. DO NOT supply any personal information what so ever to the scammers.

Online auction schemes: In an online auction scheme, a fraudster starts an auction on a site such as eBay or TradeMe with very low prices and no reserve price, especially for typically high priced items like watches, computers, or high value collectibles. The fraudster accepts payment from the auction winner, but either never delivers the promised goods, or delivers an item that is less valuable than the one offered—for example, a counterfeit, refurbished, or used item. According to data from law enforcement and consumer protection organizations, fraudulent schemes appearing on online auction websites are among the most frequently reported form of mass-marketing fraud.

Online retail schemes: involve complete online stores that appear to be legitimate. As with the auction scheme, when a victim places an order through such a site, their funds are taken but no goods are sent, or inferior goods are sent. In some cases, the stores or auctioneers were once legitimate, but eventually stopped shipping goods after accepting customer payments.

Do your research before purchasing items on the Internet, whether it is through an auction site or a general online retailer. Auction sites often have the seller's history include previous transactions, customer's reviews and ratings. If the user has poor ratings or comments, avoid buying anything from them. Also, if

they are a new user with little to no transactions, it is best to look for another user with more decent sales. Even if a user has good comments, look at a few of them to see if those customers purchased from other people on the same site; this is a good indication that they are not faking the review. For retail sites, look up the company on the Better Business Bureau and research the online store for customer reviews or feedback before making a purchase.

General Scam Indicators

The scams described above are some of the most common types of Internet fraud. However, these fraudsters are clever people who may use many variations of the above scams to achieve their nefarious ends.

In general, be wary of unsolicited emails or contacts that:

- Promise you money, jobs or prizes
- Ask for donations
- Propose lucrative business deals
- Ask you to provide sensitive personal information
- Ask you to follow a link to a website and log on to an account.

By taking the time to educate yourself about these common types of scam, and/or by sharing this information with others, you can make a valuable contribution to the war against Internet fraud

Mobile Banking Security

If you bank online and have a phone with an internet browser you may be able to access your bank's website just as you would if you were accessing it on a computer. Alternatively, if you use a smartphone you can usually download a dedicated app (application) provided by your bank. Apps provide a similar but alternative way of accessing your online bank account and are designed for ease of use and convenience. An app is a small piece of software designed for use on smartphones and tablet devices. However, you should always follow the advice below when downloading a piece of software onto your smartphone, especially if it is an app that requires internet access when you use it.

Here are some essential tips:

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

App stores: Only download apps from official app stores, such as Apple iTunes, Android Marketplace, Google, Play Store and BlackBerry App World. Free apps are great but downloading them from unknown sources could lead to your device becoming infected with a virus.

Update: Keep your smartphone's operating system updated with the latest security patches and upgrades.

Your smartphone: Think carefully before removing any security controls from your mobile device. This is known as 'jail-breaking' or 'rooting' your device. This will weaken the security of your device and expose you to additional risks. Some banks may restrict their service to a mobile device, if it's been jail-broken or rooted.

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

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

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

If you are a victim of fraud

- If you spot any unauthorised transactions on your online bank account, contact your financial institution immediately.
- If you think that you may have disclosed information to a fake website, or if you believe that any of your passwords have been captured by malware or otherwise, contact your financial institution immediately.